Geometría Algebraica

(Álgebra Conmutativa I)

Carlos Sancho de Salas y Pedro Sancho de Salas

28-11-2022

Índice general

Parte I

Álgebra Conmutativa I

Introducción

El presente manual está concebido como texto de referencia para los estudiantes del Grado de Matemáticas de la UEX, en las asignaturas de Álgebra: Álgebra Conmutativa, Álgebra I, Álgebra II y Teoría de Números. Incluye diversos temas de Álgebra y Geometría Algebraica para alumnos de máster y doctorado, y sirve también como manual de apoyo a los profesores del área de Álgebra. Ha sido redactado a partir de los cursos que recibieron los autores en la Universidad de Salamanca, impartidos por nuestro padre Juan Bautista Sancho Guimerá y su discípulo el profesor Cristóbal García-Loygorri y Urzaiz, y a partir de la experiencia docente e investigadora en la Licenciatura y Grado en Matemáticas de las universidades de Extremadura y Salamanca. En las secciones sobre la descomposición primaria de ideales y sobre los teoremas fundamentales de la Teoría de Números hemos seguido unas notas del profesor Juan A. Navarro, en el capítulo sobre la desingularización de superficies he seguido unas notas del profesor Juan B. Sancho.

El objetivo del manual es desarrollar de modo autocontenido los conocimientos básicos en Álgebra de todo graduado en Matemáticas y, junto con un segunda partel, los conocimientos básicos de un profesor en el área de Geometría Algebraica.

En toda disciplina matemática concurren entrelazadamente diversos aspectos. En primer lugar se desarrolla una teoría general, para la cual se introducen ciertas técnicas o herramientas y los cálculos necesarios para que la teoría sea efectiva. En segundo lugar, por razones intelectuales y pedadógicas, la disciplina ha de desarrollarse de modo justificado, natural, gradual, sugerente, etc. He tratado que el texto no sea simplemente una acumulación de resultados sino que en él advierta el lector una unidad de fondo, un solo discurso.

Un lugar común para los legos en Matemáticas consiste en entender las Matemáticas como una mera herramienta para la resolución por cálculo de ciertos problemas "reales" de otras disciplinas científicas. De modo parejo, dentro del mundo matemático se entiende el Álgebra como una herramienta para resolver problemas de otras áreas de la Matemática con una "significación real". Una misión primordial de la Matemática y dentro de ella del Álgebra es hacer un análisis profundo de los conceptos y teorías conocidos, análisis que supone una refundación e iluminación de éstos. En este texto

queremos también mostrar cómo la Geometría Algebraica, el cálculo diferencial tensorial de la Geometría Diferencial y la Física, la Teoría de Números, etc., hunden sus raíces en el Álgebra.

Intentemos dar una idea de lo que se estudia en este manual, idea que será imprecisa, parcial y oscura porque las Matemáticas se explican en su propio desarrollo, en su propio devenir. Hablemos con concisión. Podemos decir que este manual es un texto de Geometría Algebraica. Se estudian las variedades algebraicas, es decir, las soluciones de los sistemas de ecuaciones algebraicas. Se comienza con el estudio de las soluciones (raíces) de una ecuación polinómica $p(x) = 0$. Se calculan de modo aproximado las raíces y cuándo pueden obtenerse mediante raíces cuadradas, cúbicas, etc., (capítulos 1. y 2.). A continuación se estudia la variedad de soluciones de los sistemas algebraicos en varias variables y aparecen los conceptos de dimensión, el concepto de multiplicidad de un punto, función de Hilbert, de punto singular, y el problema de desingularización (capítulos 3.,4.,5. y 7.). Estamos hablando, pues, de invariantes asociados a las variedades algebraicas, necesarios para su clasificación. Para el cálculo de las soluciones de los sistemas de ecuaciones, se introduce la teoría de la eliminación de variables (la teoría de la resultante) y la teoría de Gröbner (capítulos 1. y 8.); para la separación de las raíces de un polinomio y el cálculo de las vueltas alrededor del origen de una curva, la teoría del exceso y los polinomios de Sturm; para el cálculo de las raíces de un polinomio por radicales, la resolvente de Lagrange; para la determinación de los puntos singulares, el cálculo diferencial; para la desingularización de curvas, la explosión en puntos; para la desingularización de superficies, la explosión en puntos y curvas, etc.

Hasta ahora hemos hablado solo desde el punto de vista geométrico. ¿Dónde aparece el Álgebra Conmutativa? Cada variedad algebraica X está determinada por su anillo de funciones complejas continuas algebraicas A_X: la variedad algebraica X se identifica esencialmente con el conjunto de los ideales primos de su anillo de funciones, $\mathrm{Spec} A_X$. Cada concepto geométrico tiene su correspondiente concepto en Álgebra Conmutativa: la dimensión de una variedad es igual a la dimensión de Krull de su anillo de funciones, la multiplicidad de un punto es igual a la multiplicidad del anillo de gérmenes de funciones en el punto, etc. Cada proceso geométrico tiene su correspondiente proceso algebraico: cada morfismo entre variedades se corresponde con un morfismo de anillos entre los anillos de funciones algebraicas; la restricción a un abierto $U \subset X$ con el morfismo de anillos de localización $A_X \to A_U := \{f/g,\ f, g \in A_X \text{ y } g \text{ no se anula en ningún punto de } U\}$, $f \mapsto f/1$; la restricción a un cerrado $Y \subset X$ con el morfismo de anillos de paso al cociente $A_X \to A_Y = \{\bar{f},\ f \in A_X : \bar{f} = \bar{g} \text{ si y solo si } f - g \text{ se anula en } Y\}$, $f \mapsto \bar{f}$; el producto directo de dos variedades se corresponde con el producto tensorial de sus respectivos anillos de funciones, etc.

Geometría Algebraica	**Álgebra Conmutativa**
Spec A, espectro	A, anillo conmutativo
$p_1(x_1,\ldots,x_n)=\cdots=p_r(x_1,\ldots,x_n)=0$	$\mathbb{C}[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$
$\phi\colon X\to Y$	$\phi^*\colon A_Y\to A_X$, $\phi^*(f)=f\circ\phi$
Dimensión de X	Dimensión de Krull de A_X
Punto no singular, $x\in X$	Anillo local regular, $A_{X,x}$
Cono tangente a X en x	Graduado de A_X por el ideal $\mathfrak{m}_x$
Explosión en un punto $x\in X$	Dilatado de A_X por el ideal $\mathfrak{m}_x$

Por otra parte, múltiples conceptos del Análisis y de la Geometría Diferencial, son algebraicos: la diferencial de una función, su derivada, se tratará con el módulo de las diferenciales de Kähler, los desarrollos de Taylor de una función con la compleción del anillo de funciones.

En el capítulo 6. introducimos la técnica o herramienta fundamental para el estudio y clasificación de distinto tipo de anillos y morfismos de anillos: el Álgebra Homológica.

Vía el Álgebra Conmutativa, la Teoría de Números puede entenderse desde un punta de vista geométrico. Definiciones y teoremas del Álgebra Conmutativa dan simultáneamente definiciones y teoremas en Geometría Algebraica y la Teoría de Números. El anillo de los números enteros $\mathbb{Z}$ está estrechamente relacionado con el anillo de funciones algebraicas de la recta afín, el anillo de polinomios $\mathbb{C}[x]$: ambos son anillos euclídeos. Los anillos de enteros están relacionados con los anillos de funciones de curvas, ambos son anillos de dimensión de Krull 1 y el proceso de desingularización en ambos consiste en obtener un anillo regular. Los números primos pueden entenderse como puntos de una curva.

Capítulo 0

Grupos, anillos y módulos

0.1. Grupos

La estructura más básica y fundamental en Álgebra es la estructura de grupo (y semigrupo). Los anillos, los espacios vectoriales, los módulos, etc. necesitan para su definición de la noción de grupo.

Demos una justificación de carácter muy general para la introducción de la teoría de grupos, siguiendo a Felix Klein en su Erlanger Programm. Dar una teoría (geométrica) es dar una estructura, un espacio con cierta estructura. En esta teoría es fundamental el estudio del grupo de automorfismos de la estructura, es decir, de aquellas biyecciones del espacio que respetan la estructura del espacio. Las nociones y objetos de este espacio, o de la teoría, serán aquéllos que queden invariantes por el grupo de automorfismos recién mencionado. El estudio de las funciones, campos diferenciables, etc., que quedan invariantes por el grupo y el estudio de las relaciones que verifican éstos, son todos los teoremas de la teoría. Es pues el estudio de los grupos (y la teoría de invariantes) un tópico fundamental en Matemáticas.

En el cálculo de las raíces de un polinomio, es conveniente conocer el grupo de aquellas permutaciones de las raíces, que respetan las relaciones algebraicas que verifican éstas. Ya veremos que las raíces de un polinomio se pueden obtener mediante radicales si y solo si el grupo de permutaciones mencionado es resoluble (noción que más adelante explicaremos).

1. Definición: Sea G un conjunto. Diremos que una aplicación $m : G \times G \to G$ (seguiremos las notaciones $m(g,g') = g \cdot g' = gg'$ y diremos que m ó $\cdot$ es una operación) dota a G de estructura de grupo si cumple las siguientes condiciones:

1. Propiedad asociativa: $g \cdot (g' \cdot g'') = (g \cdot g') \cdot g''$, para todo $g, g', g'' \in G$.

2. Existencia de elemento neutro: Existe un elemento de G, que denotamos por 1 y denominamos elemento neutro, tal que $1 \cdot g = g \cdot 1 = g$, para todo $g \in G$.

3. Existencia de inversos: Para cada $g \in G$ existe un elemento de G, que denotamos por g^{-1} y denominamos inverso de g, tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Si además se cumple que $g \cdot g' = g' \cdot g$, para todo $g, g' \in G$, diremos que G es un grupo abeliano o conmutativo; en cuyo caso, a menudo denotaremos la operación del grupo por $+$, al elemento neutro por 0 y al inverso de cada g por $-g$ (y lo denominaremos opuesto de g).,

2. Ejemplos: El conjunto de los números enteros con la suma, $(\mathbb{Z}, +)$, es un ejemplo básico de grupo conmutativo. El conjunto de todas las biyecciones de un conjunto X en sí mismo, con la operación composición de aplicaciones, $(Biy X, \circ)$, es un grupo no conmutativo (cuando X contenga más de dos elementos).

Si 1 y $1'$ son elementos neutros del grupo G entonces $1 = 1'$: $1 = 1 \cdot 1' = 1'$. Si h y h' son inversos de $g \in G$, entonces $h = h'$: $h = h \cdot 1 = hgh' = 1 \cdot h' = h'$.

3. Definición: Sea $(G, \cdot)$ un grupo. Diremos que un subconjunto $H \subseteq G$ es un subgrupo de G si cumple las siguientes condiciones:

1. Si $h, h' \in H$ entonces $h \cdot h' \in H$.

2. $1 \in H$.

3. Si $h \in H$ entonces $h^{-1} \in H$.

Si H es un subgrupo de G, entonces la operación de G define en H una estructura de grupo. Recíprocamente, si H es un subconjunto de un grupo G y la operación de G define en H una estructura de grupo entonces H es un subgrupo.

4. Proposición: *La intersección de cualquier familia de subgrupos de un grupo es un subgrupo.*

5. Definición: Dado un subconjunto X de un grupo G, llamaremos subgrupo generado por X y lo denotaremos $\langle X \rangle$, al mínimo subgrupo de G que contiene a X, es decir, a la intersección de todos los subgrupos de G que contienen a X.

Por ejemplo, el subgrupo de $\mathbb{Z}$ generado por $n \in \mathbb{Z}$, es igual a $\langle n \rangle = \{m \cdot n, m \in \mathbb{Z}\} =: n\mathbb{Z}$. El subgrupo de $\mathbb{Z}$ generado por $n, n' \in \mathbb{Z}$, es $\langle n, n' \rangle = \{mn + m'n', m, m' \in \mathbb{Z}\}$.

Dado un número entero $z \in \mathbb{Z}$, llamaremos valor absoluto de z y denotaremos $|z|$, al máximo entre z y $-z$.

6. Teorema de división de números enteros: *Sean n y $d \neq 0$ dos números enteros. Existe una única pareja de números enteros c y r (denominados cociente y resto de dividir n por d), tales que $0 \leq r < |d|$ y*

$$n = c \cdot d + r$$

Demostración. Procedamos por inducción sobre $|n|$, para probar la existencia de c y r.

Si $|n| = 0$, entonces $c = 0$ y $r = 0$. Podemos suponer que $|n| > 0$. El teorema es cierto para d si y solo si lo es para $-d$ (solo hay que cambiar c por $-c$), luego podemos suponer que $d > 0$.

Supongamos $n > 0$. Si $n < d$, entonces $c = 0$ y $r = n$. Si $n \geq d$. Sea $n' = n - d$, luego $|n'| = n - d < n = |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' + 1)d + r'$ y hemos concluido.

Supongamos, ahora, $n < 0$. Sea $n' = n + d$, luego $|n'| < |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' - 1)d + r'$ y hemos concluido.

Veamos la unicidad de c y r. Sea $n = cd + r = c'd + r'$, cumpliendo c, c', r, r' lo exigido. Podemos suponer $r \geq r'$. Entonces, $(c - c')d + (r - r') = 0$ y $|c - c'| \cdot |d| = |(c - c')d| = r - r' \leq r < |d|$, luego $c - c' = 0$. Por tanto, $c = c'$ y $r = n - cd = r'$.

□

7. Teorema: *Si H es un subgrupo del grupo (aditivo) de los números enteros $\mathbb{Z}$, entonces existe un único número natural n tal que $H = n\mathbb{Z}$.*

Demostración. Si $H = \{0\}$ entonces $H = 0 \cdot \mathbb{Z}$.

Supongamos $H \neq \{0\}$. Existen naturales positivos en H, porque el opuesto de cada número entero de H pertenece a H. Sea $n \in H$ el mínimo número natural no nulo contenido en H. Veamos que $H = n\mathbb{Z}$: Obviamente, $n\mathbb{Z} \subseteq H$. Dado $m \in H \subset \mathbb{Z}$, existen números enteros c y r tales que

$$m = cn + r, \quad 0 \leq r < n$$

Luego, $r = m - cn \in H$, porque $m, -cn \in H$. Por la definición de n, se tiene que $r = 0$. Luego, $m \in n\mathbb{Z}$, $H \subseteq n\mathbb{Z}$ y $H = n\mathbb{Z}$.

Por último, demostremos la unicidad: observemos que si un número natural m pertenece a $n\mathbb{Z}$, entonces $m \geq n$. Por tanto, si $m\mathbb{Z} = n\mathbb{Z}$, $m \geq n$ y $n \geq m$, luego $m = n$.

□

Si $m \in n\mathbb{Z}$ diremos que m es un múltiplo de n y que n es un divisor de m.

Sea $(G, +)$ un grupo abeliano y $G_1, G_2 \subseteq G$ dos subgrupos. Denotamos $\langle G_1, G_2 \rangle = G_1 + G_2$ y el lector puede comprobar que $G_1 + G_2 = \{g_1 + g_2,\ g_1 \in G_1\ g_2 \in G_2\}$.

Por la proposición anterior, dados $n, n' \in \mathbb{Z}$, existe $m \in \mathbb{N}$ tal que $n\mathbb{Z} + n'\mathbb{Z} = m\mathbb{Z}$. Observemos que $n, n' \in m\mathbb{Z}$, luego m es divisor de n y n'. Si $m' \in \mathbb{N}$ es divisor de n y n' entonces $m \in n\mathbb{Z} + n'\mathbb{Z} \subseteq m'\mathbb{Z}$, y m' divide a m. Por tanto, m es el máximo común divisor de n y n'.

Por la proposición anterior, dados $n, n' \in \mathbb{Z}$, existe $m \in \mathbb{N}$ tal que $n\mathbb{Z} \cap n'\mathbb{Z} = m\mathbb{Z}$. El lector, puede comprobar que m es el mínimo común múltiplo de n y n'.

8. Definición: Diremos que una aplicación $f : G \to G'$ entre dos grupos es un morfismo de grupos si para todo $g, g' \in G$ se cumple que

$$f(g \cdot g') = f(g) \cdot f(g').$$

Diremos que f es un isomorfismo de grupos si f es biyectiva (en tal caso la aplicación inversa f^{-1} es un isomorfismo de grupos). Diremos que es un epimorfismo (resp. monomorfismo) de grupos si f es epiyectiva (resp. inyectiva).

Si $f : G \to G'$ es un morfismo de grupos entonces $f(1) = 1$: $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ y multiplicando por $f(1)^{-1}$ obtenemos $1 = f(1)$. Además, $f(g^{-1}) = f(g)^{-1}$: $1 = f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$ y multiplicando por $f(g)^{-1}$ obtenemos $f(g)^{-1} = f(g^{-1})$.

Denotaremos $\mathrm{Hom}_{grp}(G, G')$ al conjunto de todos los morfismos de grupos de G en G'.

9. Definición: Sea $f : G \to G'$ un morfismo de grupos. Llamaremos núcleo de f y lo denotaremos $\mathrm{Ker}\, f$, al subconjunto de G

$$\mathrm{Ker}\, f := f^{-1}(1) = \{g \in G : f(g) = 1\}$$

Llamaremos imagen de f, que denotaremos $\mathrm{Im}\, f$, a la imagen de la aplicación f, es decir,

$$\mathrm{Im}\, f := \{f(g) \in G', g \in G\}$$

10. Proposición: *$\mathrm{Ker}\, f$ es un subgrupo de G e $\mathrm{Im}\, f$ es un subgrupo de G'. En general, la antimagen por un morfismo de grupos de un subgrupo es subgrupo y la imagen de un subgrupo es subgrupo.*

Dado un morfismo de grupos $f : G \to G'$ y $g \in G$, calculemos el conjunto de elementos $g' \in G$ tales que $f(g') = f(g)$: $f(g') = f(g)$ si y solo si $1 = f(g)^{-1} \cdot f(g') = f(g^{-1} \cdot g')$, es decir, si y solo si $g^{-1} \cdot g' \in \mathrm{Ker}\, f$, que equivale a decir que $g' \in g \cdot \mathrm{Ker}\, f := \{g \cdot h, h \in \mathrm{Ker}\, f\}$.

11. Proposición: *Un morfismo de grupos $f : G \to G'$ es inyectivo si y solo si* $\mathrm{Ker}\, f = \{1\}$.

Si identificamos los elementos de G cuando tengan la misma imagen, obtenemos un conjunto biyectivo con la imagen. Es decir, si identificamos cada $g \in G$ con los elementos de $g \cdot \mathrm{Ker}\, f$ obtenemos un conjunto que es biyectivo con $\mathrm{Im}\, f$.

Sea $H \subseteq G$ un subgrupo. Dado $g \in G$, denotamos $gH := \{gh \in G,\ h \in H\}$. Sean $g, g' \in G$.

Si $g' \in gH$ entonces $g'H = gH$: Sea $h \in H$, tal que $g' = gh$. Entonces, $g'H = ghH = gH$.

Si $g' \notin gH$, entonces $g'H \cap gH = \emptyset$, pues si $z \in g'H \cap gH$, entonces $g'H = zH = gH$.

Luego, dados $g, g' \in G$, o $gH = g'H$ o bien $g'H \cap gH = \emptyset$.

12. Definición: Sea $H \subseteq G$ un subgrupo. Llamaremos conjunto cociente de G por H, que denotaremos G/H, al conjunto

$$G/H := \{gH \mid g \in G\} \underset{\text{Not}}{=} \{\bar{g},\ g \in G : \bar{g'} = \bar{g} \text{ si y solo si } g' \in g \cdot H \text{ (o equiv. } g'H = gH)\}$$

Es decir, si en G identificamos cada $g \in G$ con todos los elementos de $gH \subseteq G$, obtenemos el conjunto G/H.

13. Notación: Se dice que g es congruente con g' módulo H y se denota $g \equiv g' \, mod \, H$, cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g'H$ (o $g'^{-1}g \in H$). Dado $p \in \mathbb{Z}$ y $n, m \in \mathbb{Z}$, escribiremos $n \equiv m \, mod \, p$ si $n \equiv m \, mod \, p\mathbb{Z}$, (es decir, si $n - m \in p\mathbb{Z}$).

La aplicación $G \to G/H$, $g \mapsto \bar{g}$, se denomina el morfismo de paso al cociente (por H).

14. Definición: Llamaremos orden de un conjunto X, que denotaremos $|X|$, al número de elementos del conjunto. Si el conjunto tiene un número infinito de elementos diremos que es de cardinal infinito.

15. Ejemplo: Si $n > 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un conjunto de orden n, explícitamente $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \ldots, \overline{n-1}\}$: Dado $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$, por el teorema de división de números enteros, existen números enteros únicos c y r, con $0 \leq r < n$, de modo que $m = cn + r$. Por tanto, $\bar{m}$ es igual a un único $\bar{r} \in \{\bar{0}, \ldots, \overline{n-1}\}$.

16. Teorema de Lagrange: *Sea G un grupo de orden finito. Si H es un subgrupo de G entonces*

$$|G| = |G/H| \cdot |H|$$

Demostración. $G = \coprod_{\bar{g} \in G/H} g \cdot H$ y $|gH| = |H|$ (porque la aplicación $H \to gH$, $h \mapsto gh$ es biyectiva). Por tanto, $|G| = |G/H| \cdot |H|$.

□

17. Observación: Subrayemos que el teorema de Lagrange nos dice que el orden de todo subgrupo de un grupo finito divide al orden del grupo.

18. Definición: Se dice que un subgrupo $H \subseteq G$ es normal (en G) cuando $gHg^{-1} \subseteq H$, para todo $g \in G$, es decir, si $ghg^{-1} \in H$, para todo $g \in G$ y $h \in H$.

Si G es un grupo conmutativo, todo subgrupo de G es normal en G.

Si H es normal y tomamos $g^{-1} \in G$, tendremos $g^{-1}Hg \subseteq H$, luego $H \subseteq gHg^{-1}$. Como $g^{-1}Hg \subseteq H$ entonces $gHg^{-1} = H$ (para todo $g \in G$). Por tanto, $gH = Hg$, para todo $g \in G$, y recíprocamente si un subgrupo cumple esta condición el subgrupo es normal.

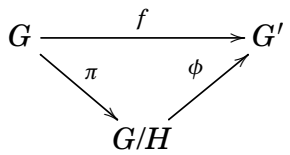
19. Teorema: *Sea $H \subseteq G$ un subgrupo y $\pi : G \to G/H$ la aplicación de paso al cociente. H es un subgrupo normal de G si y solo si existe en G/H una (única) estructura de grupo, de modo que π sea un morfismo de grupos.*

Demostración. Supongamos que H es normal en G. Definamos en G/H la operación $\bar{g} \cdot \bar{g'} := \overline{gg'}$, que está bien definida porque $gHg'H = gg'HH = \underline{gg'}H$. La propiedad asociativa se cumple de modo obvio, $\bar{1}$ es el elemento neutro y $\overline{g^{-1}}$ es el inverso de $\bar{g} \in G/H$. Luego, G/H es grupo. Además, $\pi : G \to G/H$ es morfismo de grupos, pues $\pi(g \cdot g') = \overline{gg'} = \bar{g} \cdot \bar{g'} = \pi(g) \cdot \pi(g')$.

Recíprocamente, si π es un morfismo de grupos, entonces $\bar{g} \cdot \bar{g'} = \pi(g) \cdot \pi(g') = \pi(gg') = \overline{gg'}$. Por tanto, la operación en G/H está determinada. Además, dados $h \in H$ y $g \in G$, tenemos que $\bar{h} \cdot \bar{g} = \bar{1} \cdot \bar{g} = \bar{g}$, luego $hg \in gH$, para todo $h \in H$, es decir, $Hg \subseteq gH$. Por tanto, $g^{-1}Hg \subseteq H$, para todo $g \in G$. Tomando $g^{-1} \in G$, $gHg^{-1} \subseteq H$ y H es normal en G.

□

20. Propiedad universal del grupo cociente: *Sea $H \subseteq G$ un subgrupo normal y $\pi : G \to G/H$ el morfismo de paso al cociente. Un morfismo de grupos $f : G \to G'$ factoriza a través de π si y solo si $H \subseteq \operatorname{Ker} f$, es decir, existe un (único) morfismo de grupos $\phi : G/H \to G'$ de modo que el diagrama*



es conmutativo si y solo si $H \subseteq \operatorname{Ker} f$.

Demostración. Si existe ϕ (cumpliendo lo exigido), entonces $1 = \phi(\bar{1}) = \phi(\bar{h}) = f(h)$, para todo $h \in H$, luego $H \subseteq \operatorname{Ker} f$. Además, $\phi(\bar{g}) = \phi(\pi(g)) = f(g)$, luego está determinado.

Recíprocamente, supongamos $H \subseteq \operatorname{Ker} f$. Definamos $\phi(\bar{g}) := f(g)$, que está bien definida porque $f(gH) = f(g)f(H) = f(g)$. Además, $\phi(\pi(g)) = \phi(\bar{g}) = f(g)$.

□

21. Teorema de isomorfía: *Sea $f: G \to G'$ un morfismo de grupos. La aplicación, $\phi: G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$, $\phi(\bar{g}) := f(g)$, es un isomorfismo de grupos.*

Demostración. Por la propiedad universal del grupo cociente, sabemos que $\phi \circ \pi = f$ e $\mathrm{Im}\, f = \mathrm{Im}(\phi \circ \pi) = \mathrm{Im}\, \phi$, porque π es epiyectiva. Veamos que ϕ es inyectiva: si $1 = \phi(\bar{g}) = f(g)$, entonces $g \in \mathrm{Ker}\, f$ y $\bar{g} = \bar{1}$, luego $\mathrm{Ker}\, \phi = \{\bar{1}\}$. □

0.1.1. Grupos cíclicos

22. Definición: Diremos que un grupo G es cíclico si está generado por uno de sus elementos, es decir, existe $g \in G$ de modo que $G = \langle g \rangle$.

23. Proposición: *Si G es un grupo de orden un número primo, entonces G es cíclico.*

Demostración. Por el teorema de Lagrange no puede haber más subgrupos de G que G y el trivial $\{1\}$. Por tanto, el subgrupo generado por cualquier elemento distinto de 1 es igual a G. □

24. Notación: Sea G un grupo y $g \in G$. Si $n > 0$, se define $g^n := g \overset{n}{\cdots} g$; si $n < 0$, se define $g^n := g^{-1} \overset{-n}{\cdots} g^{-1}$; y $g^0 := 1$.

Si escribimos el grupo G con notaciones aditivas (en vez de $\cdot$ escribimos $+$), escribiremos $n \cdot g$, en vez de g^n (como es natural).

25. Proposición: *Un grupo G es cíclico si y solo si es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, para algún un número natural n.*

Demostración. $\mathbb{Z}/n\mathbb{Z}$ es un grupo (aditivo) cíclico, generado por $\bar{1}$.

Supongamos que $G = \langle g \rangle$ es cíclico. Sea $f: \mathbb{Z} \to G$, el morfismo definido por $f(n) = g^n$. Es fácil comprobar que f es un morfismo de grupos. $\mathrm{Im}\, f$ es un subgrupo de G, que contiene a g, luego $\mathrm{Im}\, f = G$ y f es epiyectivo. $\mathrm{Ker}\, f$ es un subgrupo de $\mathbb{Z}$, luego existe $n \in \mathbb{N}$ tal que $\mathrm{Ker}\, f = n\mathbb{Z}$. Por el teorema de isomorfía $\mathbb{Z}/n\mathbb{Z} \simeq G$. □

$\mathbb{Z}/n\mathbb{Z}$ es un grupo conmutativo, pues es cociente de $\mathbb{Z}$ que es conmutativo. Por tanto, todo grupo cíclico es conmutativo.

26. Definición: Llamaremos orden de un elemento $g \in G$ de un grupo, al orden del subgrupo $\langle g \rangle$ de G que genera.

En la proposición anterior hemos dado el isomorfismo $\mathbb{Z}/n\mathbb{Z} \simeq \langle g\rangle$, $\bar{m} \mapsto g^m$. Por tanto, si $n > 0$, el orden de g es igual a $|\langle g\rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$, $\langle g\rangle = \{1, g^1, \ldots, g^{n-1}\}$ y n es el mínimo número natural positivo tal que $g^n = 1$, además, si $g^m = 1$, entonces m es un múltiplo del orden de g. Si $n = 0$, entonces el orden de g es $|\langle g\rangle| = |\mathbb{Z}| = \infty$ y $\langle g\rangle = \{\ldots, g^{-m}, \ldots, 1, g^1, \ldots, g^m, \ldots\}$ (cumpliendo $g^i \neq g^j$, para todo $i, j \in \mathbb{Z}$, $i \neq j$).

27. Si G es un grupo de orden $m < \infty$, entonces el orden de todo elemento $g \in G$ divide a m, ya que el orden de todo subgrupo $\langle g\rangle$ divide al orden del grupo G, por el teorema de Lagrange. En particular, $g^{|G|} = 1$.

28. Proposición: *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sea $G = \langle g\rangle$ un grupo cíclico y $\pi\colon \mathbb{Z} \to G$, $\pi(n) := g^n$, que es un epimorfismo de grupos. Dado un subgrupo $H \subseteq G$, se cumple que $H = \pi(\pi^{-1}(H))$. Ahora bien, $\pi^{-1}(H)$ es un subgrupo de $\mathbb{Z}$, luego es cíclico (es decir, generado por un elemento z). Por tanto, $H = \pi(\pi^{-1}(H))$ está generado por $\pi(z)$ y es cíclico. □

29. Proposición: *Sea $0 \neq n \in \mathbb{Z}$. Entonces, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es un generador si y solo si el máximo común divisor de m y n es 1 ("m y n son primos entre sí").*

Demostración. Consideremos el epimorfismo natural $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(z) = \bar{z}$. Es claro que $\pi^{-1}(\langle\bar{m}\rangle) = m\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$, donde r es el máximo común divisor de m y n. Por otra parte, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$, es decir, $\langle\bar{m}\rangle = \mathbb{Z}/n\mathbb{Z}$, si y solo $\pi^{-1}(\langle\bar{m}\rangle) = \mathbb{Z}$. Por tanto, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $r = 1$. □

Así pues, si $G = \langle g\rangle$ es un grupo cíclico de orden $n > 0$, entonces g^m es un generador de G si y solo si m y n son primos entre sí.

0.1.2. Grupo simétrico

El grupo simétrico S_n es el grupo de todas las biyecciones (o "permutaciones") de un conjunto de n elementos en sí mismo, con la operación composición de aplicaciones.

Comentario: Una biyección entre dos conjuntos $\tau\colon X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f\colon X \to X$, que aplica x en $f(x)$, tenemos la correspondiente aplicación en Y: "la que aplica $\tau(x)$ en $\tau(f(x))$, es decir, la aplicación $\tau \circ f \circ \tau^{-1}\colon Y \to Y$". Así el grupo de las permutaciones de X se identifica con el grupo de las permutaciones de Y (vía la identificación de X con Y). Con mayor precisión, el morfismo

$$Biy X \to Biy Y, \quad \sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$$

es un isomorfismo de grupos (como el lector puede comprobar).

Si Y es un conjunto de orden n, entonces Y es biyectivo con $\{1,\dots,n\} =: X$ y $Biy Y = Biy X =: S_n$. El número de permutaciones de n elementos es $n!$, luego $|S_n| = n!$.

30. Definición: Dados r puntos distintos $x_1,\dots,x_r \in X$, con $r > 1$, la permutación definida por $\sigma(x_i) := x_{i+1}$, para todo $i < r$; $\sigma(x_r) := x_1$; y $\sigma(x) := x$, para todo $x \notin \{x_1,\dots,x_r\}$, la denotaremos $(x_1,\dots,x_r) := \sigma \in Biy X$. Diremos que $(x_1,\dots,x_r)$ es un ciclo y observemos que es de orden r. Si $r = 2$, diremos que el ciclo es una transposición. Diremos que dos ciclos $(x_1,\dots,x_r),(x'_1,\dots,x'_{r'})$ de $Biy X$ son disjuntos si $x_i \neq x'_j$ para todo i, j.

31. Lema: *Si $\sigma = (x_1,\dots,x_r)$ y $\sigma' = (x'_1,\dots,x'_{r'})$ son disjuntos, entonces conmutan, es decir, $\sigma \circ \sigma' = \sigma' \circ \sigma$.*

Demostración. Para $x \in \{x_1,\dots,x_r\}$, $(\sigma \circ \sigma')(x) = \sigma(x) = (\sigma' \circ \sigma)(x)$. Para $x \in \{x'_1,\dots,x'_r\}$, $(\sigma \circ \sigma')(x) = \sigma'(x) = (\sigma' \circ \sigma)(x)$. Para $x \notin \{x_i, x'_j\}_{i,j}$, $(\sigma \circ \sigma')(x) = x = (\sigma' \circ \sigma)(x)$.

De otro modo (siguiendo el comentario anterior): $\sigma' \circ \sigma \circ \sigma'^{-1} = (\sigma'(x_1),\dots,\sigma'(x_r)) = (x_1,\dots,x_r) = \sigma$ y hemos concluido.

□

32. Teorema: *Toda permutación $\sigma \in S_n$, distinta de la identidad, es igual a un producto de ciclos disjuntos, de modo único salvo el orden de los factores.*

Demostración. Sea $x \in X$, tal que $\sigma(x) \neq x$. Sea r el mínimo número natural positivo tal que $\sigma^r(x) = x$ (tal número existe porque el orden de σ, que divide al orden de S_n, es finito). Para todo $0 \leq s < s' < r$, se cumple que $\sigma^{s'}(x) \neq \sigma^s(x)$: pues componiendo con σ^{-s} son distintos, pues $\sigma^{s'-s}(x) \neq x$, porque $0 < s' - s < r$. Sea $\sigma_1 = (x, \sigma(x),\dots,\sigma^{r-1}(x))$. Entonces, como σ_1 y σ coinciden sobre $\{x, \sigma(x),\dots,\sigma^{r-1}(x)\}$ y σ_1 es la identidad sobre $X \setminus \{x, \sigma(x),\dots,\sigma^{r-1}(x)\}$, se cumple que $\sigma_1^{-1} \circ \sigma$ deja fijos a $\{x, \sigma(x),\dots,\sigma^{r-1}(x)\}$ y a los que dejaba fijos σ. Reiterando el proceso obtenemos ciclos disjuntos $\sigma_1,\dots,\sigma_s$ tales que $\sigma_s^{-1} \circ \cdots \circ \sigma_1^{-1} \circ \sigma = \mathrm{Id}$. Luego, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$.

Sea otra descomposición $\sigma = \tau_1 \circ \cdots \circ \tau_t$ en producto de ciclos disjuntos. Reordenando, podemos suponer que $\tau_1(x) \neq x$. Es decir, x "aparece" en el ciclo τ_1 (y en σ_1). Luego, $\tau_1(x) = \sigma(x) = \sigma_1(x)$. Obviamente, $\tau_1(x) = \sigma(x) = \sigma_1(x)$ "aparece" en ciclo de τ_1 y en el de σ_1. Luego, $\tau_1^2(x) = \sigma^2(x) = \sigma_1^2(x)$. Así sucesivamente, $\tau_1^i(x) = \sigma^i(x) = \sigma_i^2(x)$, para todo i. Por tanto, $\tau_1 = \sigma_1$ y $\sigma_2 \circ \cdots \circ \sigma_s = \tau_2 \circ \cdots \circ \tau_t$. Reiterando el argumento concluimos que, después de reordenar los factores, $\sigma_2,\dots,\sigma_s$ coinciden con $\tau_2,\dots,\tau_t$.

□

33. Definición: Sea $\sigma \in S_n$ una permutación distinta de la identidad. Sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ una descomposición en producto de ciclos disjuntos y d_i el orden de σ_i. Reordenando podemos suponer que $d_1 \geq d_2 \geq \cdots \geq d_s$. Diremos que $d_1, \ldots, d_s$ es la forma de σ .

34. Definición: Dado $g \in G$, diremos que el morfismo $\tau_g \colon G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h, h' \in G$ son conjugados si y solo si existe $g \in G$, de modo que $\tau_g(h) = h'$.

35. Teorema: *La condición necesaria y suficiente para que $\sigma, \sigma' \in S_n$ sean conjugadas es que tengan la misma forma.*

Demostración. Sea $\sigma = (x_{11}, \ldots, x_{1d_1}) \circ \cdots \circ (x_{s1}, \cdots, x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_{11}), \ldots, \tau(x_{1d_1})) \circ \cdots \circ (\tau(x_{s1}), \cdots, \tau(x_{sd_s}))$$

que tiene la misma forma. Sea $\sigma' = (x'_{11}, \ldots, x'_{1d_1}) \circ \cdots \circ (x'_{s1}, \cdots, x'_{sd_s})$. Si τ es cualquier permutación que cumpla $\tau(x_{ij}) = x'_{ij}$, para todo i, j, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

36. Proposición: *Si $d_1, \ldots, d_s$ es la forma de $\sigma \in S_n$, entonces el orden de σ es el mínimo común múltiplo de $d_1, \ldots, d_s$.*

Demostración. Escribamos $\sigma = \sigma_1 \cdots \sigma_s$ como producto de ciclos disjuntos. Entonces, $\sigma^n = \sigma_1^n \cdots \sigma_s^n$ y σ_i^n es "disjunta" con σ_j^n, para $i \neq j$. Luego, $\sigma^n = \mathrm{Id}$ si y solo si $\sigma_1^n = \cdots = \sigma_s^n = \mathrm{Id}$. Por tanto, el orden de σ es el mínimo común múltiplo de los órdenes de σ_i (que son d_i). □

37. Proposición: *Todo permutación $\sigma \in S_n$ es producto de transposiciones.*

Demostración. Como toda permutación es producto de ciclos, basta probar que todo ciclo es producto de transposiciones. Sea, pues, un ciclo $(x_1, \ldots, x_r) \in S_n$. Obviamente, $(x_1, x_2)(x_1, \ldots, x_r) = (x_2, \ldots, x_r)$, luego

$$(x_1, \ldots, x_r) = (x_1, x_2)(x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3)(x_3, \ldots, x_r) = \cdots = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r)$$

□

Signo de una permutación.

Cada permutación $\sigma \in S_n = Biy(\{1, 2, \ldots, n\})$ define una biyección del anillo de polinomios en n variables con coeficientes números racionales, $\mathbb{Q}[x_1, \ldots, x_n]$:

$$\mathbb{Q}[x_1, \ldots, x_n] \to \mathbb{Q}[x_1, \ldots, x_n],\ p(x_1, \ldots, x_n) \mapsto p(x_1, \ldots, x_n)^\sigma := p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Sea $\delta(x_1,\dots,x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1,\dots,x_n]$. Sea $\sigma \in S_n = Biy(\{1,2,\dots,n\})$. Es fácil comprobar que $\delta(x_1,\dots,x_n)^\sigma = \delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \pm\delta(x_1,\dots,x_n)$.

38. Definición: Llamaremos signo de una permutación $\sigma \in S_n$, que denotaremos $\operatorname{sign}(\sigma)$, al número entero 1 ó -1 tal que $\delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \operatorname{sign}(\sigma)\cdot\delta(x_1,\dots,x_n)$.

39. Proposición: *Consideremos el grupo (multiplicativo)* $\{1,-1\}$. *El morfismo natural*

$$\operatorname{sign}\colon S_n \to \{1,-1\},\ \sigma \mapsto \operatorname{sign}(\sigma)$$

es un morfismo de grupos.

Demostración. $\operatorname{sign}(\sigma'\sigma)\cdot\delta = \delta^{\sigma'\sigma} = (\delta^\sigma)^{\sigma'} = (\operatorname{sign}(\sigma)\delta)^{\sigma'} = \operatorname{sign}(\sigma')\cdot\operatorname{sign}(\sigma)\cdot\delta$. Luego, $\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\sigma') = \operatorname{sign}(\sigma\cdot\sigma')$. □

Es fácil ver que $\operatorname{sign}(\mathrm{Id}) = 1$ y que $\operatorname{sign}((1,2)) = -1$.

Evidentemente, sign es un epimorfismo (para $n > 1$).

40. Definición: Llamaremos subgrupo alternado de S_n, que denotaremos A_n, al núcleo del morfismo sign, es decir, al subgrupo (normal) de S_n formado por las permutaciones de signo positivo.

Por el teorema de isomorfía $S_n/A_n \simeq \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Por el teorema de Lagrange, $|A_n| = |S_n|/2 = n!/2$ $(n > 1)$.

Observemos que el signo es invariante por conjugaciones, es decir,

$$\operatorname{sign}(\tau\sigma\tau^{-1}) = \operatorname{sign}(\tau)\cdot\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\tau)^{-1} = \operatorname{sign}(\sigma)$$

En particular, el signo de toda transposición es -1, porque todas son conjugadas de la transposición $(1,2)$.

41. Proposición: *Si la forma de una permutación* $\sigma \in S_n$ *es* $d_1,\dots,d_r$, *entonces*

$$\operatorname{sign}(\sigma) = (-1)^{d_1-1}\cdots(-1)^{d_r-1} = (-1)^{d_1+\cdots+d_r-r}.$$

Demostración. Si $\sigma = (x_1,\dots,x_r)$, entonces $(x_1,\dots,x_r) = (x_1,x_2)(x_2,x_3)\cdots(x_{r-1},x_r)$ es producto de $r-1$ transposiciones. Como sign es un morfismo de grupos, $\operatorname{sign}(\sigma) = (-1)^{r-1}$.

En general, $\sigma = \sigma_1\cdots\sigma_r$, donde σ_i es un ciclo de orden d_i. Por tanto, $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma_1)\cdots\operatorname{sign}(\sigma_r) = (-1)^{d_1-1}\cdots(-1)^{d_r-1}$. □

0.1.3. Producto directo y semidirecto de grupos

42. Definición: Dados dos grupos G_1, G_2 se define el producto directo de ellos al conjunto producto cartesiano de ambos, $G_1 \times G_2$, con la operación de grupo definida por la fórmula:

$$(g_1, g_2) \cdot (g_1', g_2') := (g_1 g_1', g_2 g_2')$$

43. Ejemplo: Más adelante (subsección 0.6.5), probaremos que los grupos abelianos generados por un número finito de elementos son isomorfos a un producto directo de grupos cíclicos.

44. Notación: Dados dos subgrupos $H, H' \subseteq G$, denotamos $H \cdot H' := \{hh' \in G, \text{ con } h \in H \text{ y } h' \in H'\}$.

45. Proposición: *Sean $H, H' \subseteq G$ dos subgrupos normales. Supongamos $H \cap H' = \{1\}$. Entonces, los elementos de H conmutan con los de H' y HH' es un subgrupo de G isomorfo a $H \times H'$.*

Demostración. Para todo $h \in H$ y $h' \in H'$, $(hh'h^{-1})h'^{-1} = h(h'h^{-1}h'^{-1}) \in H \cap H' = \{1\}$, luego $hh' = h'h$. Ahora ya, la aplicación

$$m : H \times H' \to G,\ m((h, h')) := hh'$$

es un morfismo de grupos inyectivo. Luego, $H \times H' \simeq \operatorname{Im} m = HH'$. □

46. Definición: Sea $H \subseteq G$ un subgrupo. Llamaremos normalizador de H en G, que denotaremos $N(H)$ (o $N_G(H)$), al subgrupo de G definido por

$$N(H) := \{g \in G : gHg^{-1} = H\}$$

El normalizador de H en G es el máximo subgrupo de G en el que H es normal.

47. Proposición: *Sean $H, H' \subseteq G$ dos subgrupos. Supongamos $H \cap H' = \{1\}$ y que $H' \subseteq N(H)$. Entonces, HH' es un subgrupo de G y la aplicación*

$$m : H \times H' \to H \cdot H', \quad m(h, h') := hh'$$

es biyectiva. Denotaremos, $H \rtimes H' = HH'$.

Demostración. Dados $h_1h_1' \in HH'$ y $h_2h_2' \in HH'$, $h_1h_1'h_2h_2' = (h_1(h_1'h_2{h_1'}^{-1}))\cdot(h_1'h_2') \in HH'$. Dado $hh' \in HH'$ $(hh')^{-1} = ({h'}^{-1}h^{-1}h')\cdot {h'}^{-1} \in HH'$. Además, $1 \in HH'$. Por tanto, HH' es un subgrupo de G.

Veamos que m es inyectiva: Si $m((h_1,h_1')) = m((h_2,h_2'))$, entonces $h_1h_1' = h_2h_2'$. Por lo tanto, $h_2^{-1}h_1 = h_2'{h_1'}^{-1} \in H \cap H' = \{1\}$, y $h_1 = h_2$ y $h_1' = h_2'$. Obviamente, m es epiyectiva.

□

Observemos en la proposición anterior que aunque $H \times H'$ es biyectivo con $H \rtimes H'$, no es isomorfo como grupo, pues $(h_1h_1')\cdot(h_2h_2') = (h_1(h_1'h_2{h_1'}^{-1}))\cdot(h_1'h_2')$, que no coincide en general con $(h_1h_2)\cdot(h_1'h_2')$.

48. Ejercicio: Sean G y G' dos grupos y $\phi\colon G' \to \mathrm{Aut}_{grp}(G)$ un morfismo de grupos. Consideremos las aplicaciones $i_1\colon G \to \mathrm{Biy}(G\times G')$, donde $i_1(g)$ está definida por $i_1(g)(g_1,g') := (gg_1,g')$ y $i_2\colon G' \to \mathrm{Biy}(G\times G')$, $i_2(g')$ está definida por $i_2(g')(g,g_1') := (\phi(g')(g), g'g_1')$. Prueba que i_1 e i_2 son morfismos inyectivos de grupos. Si identificamos G y G' con sus imágenes por i_1 e i_2 respectivamente, prueba que $G \cap G' = \{1\}$ y que $G' \subseteq N(G)$. Prueba que $g'g{g'}^{-1} = \phi(g')(g)$ y que por tanto $(g_1g_1')\cdot(g_2g_2') = (g_1\phi(g_1')(g_2))\cdot(g_1'g_2')$. Se dice que $G \rtimes G'$ es el producto semidirecto de los grupos G y G'.

49. Ejercicio: Sea $G' \to \mathrm{Aut}_{gr}(G)$, $g' \mapsto \mathrm{Id}$, para todo $g' \in G'$, el morfismo trivial. Prueba que $G \rtimes G' = G \times G'$.

50. Grupo de afinidades de $\mathbb{R}^n$: *Sea $G = \mathbb{R}^n$ (con la operación +) y $G' = Gl_n(\mathbb{R})$ el grupo de las matrices de orden n invertibles (con la operación componer matrices). Consideremos G como subgrupo de* $\mathrm{Biy}(\mathbb{R}^n)$ *vía el morfismo inyectivo $G \to \mathrm{Biy}(\mathbb{R}^n)$, $e \mapsto T_e$, donde $T_e(e') := e + e'$. Consideremos G' como subgrupo de* $\mathrm{Biy}(\mathbb{R}^n)$ *vía la inclusión obvia. Entonces, $G \cap G' = \{\mathrm{Id}\}$ y $G' \subset N(G)$. Al producto semidirecto $\mathbb{R}^n \rtimes Gl_n(\mathbb{R})$, se le denomina grupo de afinidades de $\mathbb{R}^n$.*

51. El grupo diédrico D_n: *Se denomina grupo diédrico D_n ($n > 2$) al grupo formado por todas las isometrías del plano que dejan estable el polígono regular de n-lados (la operación de D_n es la composición de isometrías).*

Puede demostrarse que D_n está generado por el giro g de $2\pi/n$ radianes y una simetría τ (del polígono). Además, se tiene que $\langle g\rangle \cap \langle\tau\rangle = \{\mathrm{Id}\}$ y $\tau g\tau^{-1} = g^{-1}$. Por tanto, $\langle g\rangle$ es normal en D_n, y por la proposición 0.1.47, $D_n = \langle g\rangle \rtimes \langle\tau\rangle = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, explícitamente

$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_n,\ (\bar r, \bar s) \mapsto g^r\cdot\tau^s$$

Las isometrías del plano que dejan estable un polígono regular de n-lados están determinadas por cómo permutan los vértices. Por tanto, si numeramos consecutivamente

los vértices del polígono regular con los números $1,\dots,n$*, tenemos un morfismo inyectivo* $D_n \hookrightarrow S_n$*, de modo que* g *se corresponde con la permutación* $(1,2,\dots,n)$ *y* τ *con la permutación que asigna* $i \mapsto n-i$*, para todo* $1 \leq i < n$*.*

52. Ejercicio: Sea $n \geq 2$, $A_n \subseteq S_n$ y $\mathbb{Z}/2\mathbb{Z} = \langle (1,2) \rangle \subseteq S_n$. Prueba que $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

0.1.4. G-conjuntos. Teoremas de Sylow

Sea G un grupo.

53. Definición: Llamaremos G-conjunto a cada pareja (X,τ) constituida por un conjunto X y una representación τ de G como transformaciones de X, es decir, un morfismo de grupos $\tau : G \to Biy X$.

Para no abusar de la notación, cuando no haya posibilidad de confusión, escribiremos X en vez de (X,τ) y para cada $g \in G$ y $x \in X$ escribiremos $g \cdot x$, o simplemente gx, en vez de $\tau(g)(x)$, que denominaremos transformado de x por g.

Observemos que para todo G-conjunto X se cumple

1. $1 \cdot x = x$, para todo $x \in X$.
2. $g \cdot (g' \cdot x) = (g \cdot g') \cdot x$, para todo $x \in X$ y $g, g' \in G$.

Es fácil ver que dotar a un conjunto X de estructura de G-conjunto, equivale a dar una aplicación $\phi : G \times X \to X$, tal que si denotamos $\phi((g,x)) = g \cdot x$, entonces se cumplen las dos condiciones 1. y 2. anteriores.

54. Ejemplos: G es naturalmente G-conjunto de los siguientes modos:

1. Operando por la izquierda: Se define $g * x := g \cdot x$, para cada $g, x \in G$, donde $*$ indica la operación de G en G como G-conjunto.
2. Operando por la derecha: Se define $g * x := x \cdot g^{-1}$, para cada $g, x \in G$.
3. Operando por conjugación: Se define $g * x := g \cdot x \cdot g^{-1}$, para cada $g, x \in G$.

Sea $H \subset G$ un subgrupo. El cociente G/H es un G-conjunto con la acción $g \cdot \bar{g}' := \overline{gg'}$, para cada $g \in G$ y $\bar{g}' \in G/H$.

Si X es un G-conjunto y tenemos una biyección $\sigma : X \to Y$ (es decir, "identificamos X con Y"), entonces Y es de modo natural un G-conjunto: $g \cdot y := \sigma(g \cdot \sigma^{-1}(y))$ (es decir, si g transforma x en gx, entonces g transforma $\sigma(x)$ en $\sigma(gx)$).

55. Teorema de Cayley: *Todo grupo es de modo canónico un grupo de transformaciones de un conjunto. Con precisión, el morfismo*

$$\tau : G \to Biy G$$

definido por $\tau(g)(g') := gg'$*, es un morfismo de grupos inyectivo.*

Demostración. $\tau(g_1 \cdot g_2)(g) = g_1 g_2 g = \tau(g_1)(\tau(g_2)(g))$, para todo $g \in G$ y $g_1, g_2 \in G$. Luego, $\tau(g_1 \cdot g_2) = \tau(g_1) \circ \tau(g_2)$ y τ es un morfismo de grupos. Además, si $\tau(g) = \mathrm{Id}$, entonces $g = \tau(g)(1) = 1$, luego τ es inyectivo. □

56. Definición: Sea X un G-conjunto. Diremos que G opera transitivamente sobre X si para toda pareja $x, x' \in X$ existe un $g \in G$ de modo que $x' = gx$. Diremos que un subgrupo de permutaciones $G \subset S_n = Biy\{1, \ldots, n\}$ es transitivo si opera transitivamente en $\{1, \ldots, n\}$.

Por tanto, si G es un grupo finito de orden n, entonces G es isomorfo a un subgrupo transitivo de S_n.

57. Definiciones: Dados dos G-conjuntos X, Y diremos que una aplicación $f : X \to Y$ es un *morfismo de G-conjuntos*, cuando conmute con la acción de G, es decir,

$$f(g \cdot x) = g \cdot f(x)$$

para todo $g \in G$ y $x \in X$. Al conjunto de los morfismos de G-conjuntos de X en Y lo denotaremos:

$$\mathrm{Hom}_G(X, Y)$$

(en el caso de que haya alguna ambigüedad escribiremos $\mathrm{Hom}_{G-conj}(X, Y)$).

Diremos que f es *isomorfismo* de G-conjuntos, cuando sea un morfismo biyectivo. Si $f : X \to X$ es un isomorfismo de G-conjuntos, entonces diremos que es un *automorfismo* de X como G-conjunto.

58. Observación: Se comprueba fácilmente las siguientes propiedades:

1. La *composición de morfismos* de G-conjuntos *es morfismo* de G-conjuntos, es decir: si X, Y, Z son G-conjuntos y $f : X \to Y$ y $h : Y \to Z$ son morfismos de G-conjuntos, entonces la composición $h \circ f : X \to Z$ es morfismo de G-conjuntos.

2. *La identidad es morfismo* de G-conjuntos: si X es un G-conjunto, entonces la aplicación $Id_X : X \to X$ definida por la fórmula $Id_X(x) = x$, es morfismo de G-conjuntos.

3. *La aplicación inversa de un isomorfismos* de G-conjuntos *es morfismo* de G-conjuntos: si $f: X \to Y$ es un isomorfismo de G-conjuntos, entonces $f^{-1}: Y \to X$ es morfismo de G-conjuntos.

De aquí se obtiene inmediatamente el siguiente teorema.

59. Proposición: *Si X es un G-conjunto y denotamos* $\mathrm{Aut}_G(X)$ *al conjunto de los isomorfismos de G-conjuntos, entonces* $\mathrm{Aut}_G(X)$ *es grupo con la composición de aplicaciones.*

60. Ejercicio: Sea G un grupo y consideremos G como G-conjunto operando por la izquierda. Prueba que $G \to \mathrm{Aut}_G(G)$, $g \mapsto R_g$, $R_g(g') := g' \cdot g^{-1}$, es una biyección.

Sean X e Y dos G-conjuntos. Entonces, $X \times Y$ es G-conjunto: $g \cdot (x,y) := (gx, gy)$. Obviamente, $X \coprod Y$ es G-conjunto. $\mathrm{Hom}(X,Y)$ es G-conjunto: $(g \cdot f)(x) := g \cdot f(g^{-1} \cdot x)$, para todo $f \in \mathrm{Hom}(X,Y)$.

61. Definición: Sea X un G-conjunto y $x \in X$. Llamaremos órbita de x, que denotaremos O_x o $G \cdot x$, al conjunto

$$G \cdot x := \{g \cdot x, g \in G\} \subseteq X$$

Llamaremos subgrupo de isotropía de x, que denotaremos I_x, al subgrupo de G definido por

$$I_x := \{g \in G : g \cdot x = x\}$$

62. Proposición: *La órbita de x es un G-conjunto isomorfo a G/I_x. Explícitamente, la aplicación*

$$G/I_x \to G \cdot x, \quad \bar{g} \mapsto g \cdot x$$

es un isomorfismo de G-conjuntos.

Demostración. Al lector. □

63. Proposición: *Sea X un G-conjunto, $x \in X$ y $x' = g \cdot x$. Entonces,*

$$I_{x'} = g \cdot I_x \cdot g^{-1}$$

Demostración. Al lector. □

Si $x' \in G \cdot x$ entonces $G \cdot x' = G \cdot x$: Obviamente, $G \cdot x' \subseteq G \cdot G \cdot x = G \cdot x$. Por otra parte, $x' = g \cdot x$, para cierto $g \in G$, luego, $x = g^{-1} \cdot x' \in G \cdot x'$. Por tanto, $G \cdot x \subseteq G \cdot x'$ y $G \cdot x' = G \cdot x$.

Si $x' \notin G \cdot x$, entonces $(G \cdot x') \cap (G \cdot x) = \emptyset$: Si $z \in (G \cdot x') \cap (G \cdot x)$, entonces $G \cdot x' = G \cdot z = G \cdot x$. Luego, $x' \in G \cdot x$ y llegamos a contradicción.

Por tanto, las órbitas de dos puntos o son iguales o disjuntas.

64. Definición: Sea X un G-conjunto. Llamaremos conjunto cociente de X por la acción de G en X, que denotaremos X/G, al al conjunto de las órbitas de X. Si denotamos $\bar{x} = G \cdot x$, entonces

$$X/G := \{\bar{x}, x \in X\}$$

y $\bar{x'} = \bar{x}$ si y solo si $x' \in G \cdot x$ (o equivalentemente $G \cdot x' = G \cdot x$).

Es decir, si en X identificamos todos los puntos de cada órbita obtenemos el conjunto cociente.

Con mayor generalidad, sea un conjunto X con una relación de equivalencia $\sim$ (por ejemplo, si X es un G-conjunto, podemos definir $x \sim x'$ si $G \cdot x = G \cdot x'$). Se llama conjunto cociente de X por la relación de equivalencia $\sim$, que denotaremos $X/\sim$, al conjunto de sus clases de equivalencia. Si denotamos $\bar{x}$ a la clase de equivalencia de x, entonces

$$X/\sim := \{\bar{x}, x \in X\}$$

y $\bar{x'} = \bar{x}$ si y solo si $x' \sim x$. Es decir, si en X identificamos cada $x \in X$ con sus equivalentes, obtenemos $X/\sim$.

65. Definición: Sea X un G-conjunto. Diremos que $x \in X$ es invariante por G (o G-invariante) si $g \cdot x = x$, para todo $g \in G$. Denotaremos X^G al subconjunto de X formado por todos los invariantes por G, es decir,

$$X^G = \{x \in X : g \cdot x = x \text{ para todo } g \in G\}.$$

66. Definición: Sea $p \in \mathbb{N}$ un número primo y G un grupo finito. Diremos que G es un p-grupo cuando $|G| = p^n$, con $n > 0$.

67. Fórmula de clases: *Sea G un grupo finito y X un G-conjunto finito. Entonces,*

$$|X| = |X^G| + \sum_{\bar{x} \in X/G, x \notin X^G} |G|/|I_x|$$

Además, si G es un p-grupo, entonces

$$|X| \equiv |X^G| \, mod \, p$$

Demostración. $X = \coprod_{\bar{x} \in X/G} G \cdot x = X^G \coprod_{\bar{x} \in X/G, x \notin X^G} G \cdot x$. Como $G \cdot x \simeq G/I_x$, entonces, por el teorema de Lagrange

$$|X| = |X^G| + \sum_{\bar{x} \in X/G, x \notin X^G} |G|/|I_x|$$

Si G es un p-grupo, por el teorema de Lagrange $|G/I_x| = p^i$ (e $i = 0$ si y solo si $x \in X^G$). Luego,

$$|X| \equiv |X^G| \, mod \, p$$

□

68. Definición: Dado un grupo G, llamaremos *centro* $Z(G)$ *de* G al subconjunto de G formado por los elementos $z \in G$ que conmutan con todos los de G, es decir, $zg = gz$ (para todo $g \in G$). De otro modo $Z(G)$ es el núcleo del morfismo $c : G \to Biy(G)$ definido por la acción de G en G por conjugación (i.e. $c(g)(g') := gg'g^{-1}$).

69. Proposición: *Si G es un p-grupo, entonces su centro es no trivial (i.e. $|Z(G)| > 1$).*

Demostración. Por la fórmula de clases $|Z(G)| = |G^G| = |G| \, mod \, p = 0 \, mod \, p$, como $1 \in Z(G)$ se concluye que $|Z(G)| \geq p > 1$. □

70. Proposición: *Si G es un grupo tal que $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Sea $G/Z(G) =< \overline{g} >$, siendo $\overline{g}$ la clase de $g \in G$. Obviamente, se tiene que $G =< g > \cdot Z(G)$, luego $g \in Z(G)$ (pues conmuta con $< g >$ y con $Z(G)$), luego $< g > \subseteq Z(G)$ y $G = Z(G)$. □

71. Corolario: *Todo grupo de orden p^2 (con p primo) es abeliano.*

Demostración. $Z(G) \subset G$ es no trivial, luego $G/Z(G)$ es de orden 1 o p. En cualquier caso es cíclico y, por la proposición anterior G es abeliano. □

72. Teorema de Cauchy: *Si G es un grupo de orden múltiplo de un número primo p, entonces contiene un subgrupo de orden p.*

Demostración. Tenemos que probar que existe un morfismo de grupos no trivial de $\mathbb{Z}/p\mathbb{Z}$ en G.

Sean G y G' dos grupos y $X = \mathrm{Hom}_1(G', G)$ el conjunto de las aplicaciones f de G' en G, tales que $f(1) = 1$. Definamos la operación de G' en X, $(g_1 * f)(g_2) := f(g_2 g_1) \cdot f(g_1)^{-1}$, para $f \in X$ y $g_1, g_2 \in G'$, que dota a X de estructura de G'-conjunto. Se tiene que

$$\mathrm{Hom}_1(G', G)^{G'} = \mathrm{Hom}_{grp}(G', G).$$

Observemos que $|X| = |G|^{|G'|-1}$. Si p es un número primo, G es un grupo de orden múltiplo de p y $G' = \mathbb{Z}/p\mathbb{Z}$, entonces por la fórmula de clases

$$|\mathrm{Hom}_{grp}(\mathbb{Z}/p\mathbb{Z}, G)| = |X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| \mod p \equiv 0 \mod p.$$

Luego, $|\mathrm{Hom}_{grp}(\mathbb{Z}/p\mathbb{Z}, G)| > 1$.

□

73. Proposición: *Sea X un G-conjunto, $H \subseteq G$ un subgrupo y consideremos G/H como G-conjunto de modo natural: $g \cdot \bar{g'} = \overline{gg'}$. Entonces,*

$$\mathrm{Hom}_G(G/H, X) = X^H,\ f \mapsto f(\bar{1}).$$

74. Proposición: *Sea $H \subseteq G$ un subgrupo finito. Consideremos G/H como H-conjunto con la operación $h \cdot \bar{g'} := \overline{hg'}$. Entonces se cumple que*

$$\begin{aligned}(G/H)^H &= \{\bar{g} \in G/H : H \cdot \bar{g} = \bar{g}\} = \{\bar{g} \in G/H : Hg \subseteq gH\} = \{\bar{g} \in G/H : H \subseteq gHg^{-1}\} \\ &= \{\bar{g} \in G/H : H = gHg^{-1}\} = \{\bar{g} \in G/H : g \in N_G(H)\} \\ &= N_G(H)/H.\end{aligned}$$

75. Definición: Sea G un grupo de orden $p^n \cdot m$, p primo, $n > 0$ y $(p,m) = (1)$. A los subgrupos de G de orden p^n se les denomina p-subgrupos de Sylow.

76. Primer teorema de Sylow: *Si G es un grupo de orden múltiplo de un número primo p, entonces contiene p-subgrupos de Sylow.*

Demostración. Escribamos $|G| = p^n \cdot m$, $n > 0$ y $(p,m) = 1$ Sabemos por el teorema de Cauchy que G contiene subgrupos de orden p. Basta probar que si G contiene un subgrupo H de orden p^i, con $i < n$, entonces H está incluido un subgrupo H' de G (y es normal en H') de orden p^{i+1}. Consideremos la acción de H en G/H: $h \cdot \bar{g'} = \overline{hg'}$. Entonces, $(G/H)^H = N_G(H)/H$ y por la fórmula de clases $|N_G(H)/H| = |(G/H)^H| \equiv |G/H| \, mod\, p = 0 \, mod\, p$. Luego, $|N_G(H)/H|$ es un p-grupo y por el teorema de Cauchy existe un subgrupo $Z \subseteq N_G(H)/H$ de orden p. Sea $\pi : N_G(H) \to N_G(H)/H$ el morfismo de paso al cociente. Entonces, $H' := \pi^{-1}(Z) \subseteq N_G(H)$ es un subgrupo que contiene a $\pi^{-1}(1) = H$ (y H es normal en él) y tal que $H'/H = Z$. Luego, H' es el subgrupo de orden p^{i+1} buscado. □

77. Segundo teorema de Sylow: *Sea G un grupo de orden múltiplo de un número primo p. Entonces, todos los p-subgrupos de Sylow de G son conjugados entre sí.*

Demostración. Sean H, H' dos subgrupos de un grupo G. Observemos que $H' \subseteq gHg^{-1}$ $\iff H'g \subseteq gH \iff H'gH \subseteq gH \iff \bar{g} \in (G/H)^{H'}$.

Sean $H, H' \subseteq G$ dos p-subgrupos de Sylow. Basta probar que $(G/H)^{H'} \neq \emptyset$. Por la fórmula de clases $|(G/H)^{H'}| \equiv |G/H| \, mod\, p \neq 0 \, mod\, p$ y hemos terminado.

□

78. Corolario: *Sea G un grupo de orden finito múltiplo de un número primo p y H un p-subgrupo de Sylow. G contiene un único p-subgrupo de Sylow si y solo si H es un subgrupo normal.*

79. Tercer teorema de Sylow: *Sea G un grupo de orden $p^n \cdot m$, con p primo, $n > 0$ y $(p,m) = (1)$. Entonces, el número de p-subgrupos de Sylow de G es divisor de m y congruente con 1 módulo p.*

Demostración. Sea H un p-subgrupo de Sylow y X el conjunto de los conjugados de H. Por el segundo teorema de Sylow, el número de p-subgrupos de Sylow de G es igual a $|X|$. Consideremos la acción de G en X, $g * H' = gH'g^{-1}$, para $g \in G$ y $H' \in X$. El subgrupo de isotropía de $H \in X$, es igual $N_G(H)$ y X es igual a la órbita de H, luego $X = G/N_G(H)$. Por lo tanto,

$$m = |G/H| = |G|/|H| = (|G|/|N_G(H)|) \cdot (|N_G(H)|/|H|) = |X| \cdot |N_G(H)/H|$$

y $|X|$ divide a m.

H opera en X porque es un subgrupo de G. Por la fórmula de clases $|X| \equiv |X^H| \, mod \, p$. Ya solo nos falta probar que $|X^H| = 1$. Si $H' \in X^H$ entonces $h \cdot H' \cdot h^{-1} = H'$, para todo $h \in H$, luego $hH' = H'h$, para todo $h \in H$ y $H \cdot H' = H' \cdot H$. Por tanto, $H \cdot H'$ es un subgrupo de G, H' es normal en $H \cdot H'$ y $(H \cdot H')/H' \simeq H/(H \cap H')$. Entonces, $|H \cdot H'| = |H'| \cdot |H/(H \cap H')|$ y $H \cdot H'$ es un p-grupo, que ha de coincidir con H. En conclusión, $H' = H$ y $|X^H| = 1$.

□

0.2. Anillos

Desde un punto de vista aritmético, los anillos son las estructuras que recogen las operaciones de suma y producto, como las que tenemos en $\mathbb{Z}$. Ahora bien, los anillos pueden entenderse geométricamente como anillos de funciones continuas de un espacio.

Intentemos justificar la introducción de los anillos desde un punto de vista geométrico.

Un físico estudia el universo con unos instrumentos, que le van dando información, números. Del mismo modo opera todo ser vivo. Es decir, el físico cuenta con unas funciones, con el álgebra definida por estas funciones. Desde un punto de vista kantiano y positivista, el punto de partida del conocimiento es este álgebra de funciones. El espacio se obtiene del anillo o álgebra de funciones.

Desde Descartes, imaginamos tres ejes de coordenadas y todo punto del espacio viene definido por tres coordenadas. Los puntos vienen determinados por los valores de las funciones coordenadas en ellos. Además los objetos del espacio, por ejemplo un paraboloide, los solemos definir en implícitas. Dos objetos serán iguales si no los sabemos distinguir, es decir, con nuestra terminología, si no existe una función que

valore distintamente en los dos objetos. Gauss, con la introducción de las coordenadas curvilíneas, permitió independizarnos de la elección arbitraria de las coordenadas cartesianas.

Dependiendo de las funciones que consideremos como "admisibles", el espacio será de una forma u otra. Por ejemplo, dado $\mathbb{R}^3$, si consideramos que cualquier aplicación de conjuntos de $\mathbb{R}^3$ en $\mathbb{R}$ es una observación o función admisible, estaremos considerando nuestro espacio como un conjunto discreto. Si consideramos solo las funciones continuas, lo estaremos considerando como espacio topológico. Si consideramos el anillo generado algebraicamente por las tres coordenadas, lo consideraremos como espacio algebraico.

En este último caso, los objetos vienen definidos por el lugar geométrico definido por ecuaciones (compatibles) del tipo

$$p_1(x_1,x_2,x_3)=0,\dots,p_r(x_1,x_2,x_3)=0 \qquad (*)$$

Objetos que denominaremos subvariedades algebraicas. Como es obvio, si al sistema anterior le añadimos una ecuación del tipo $\sum_i f_i \cdot p_i(x_1,x_2,x_3)=0$, ésta es redundante. El sistema de ecuaciones definido por los polinomios $p_1(x_1,x_2,x_3),\dots,p_r(x_1,x_2,x_3)$ tiene las misma soluciones que el sistema de ecuaciones definido por los polinomios del ideal $(p_1(x_1,x_2,x_3),\dots,p_r(x_1,x_2,x_3))$. Tenemos, pues, una correspondencia biunívoca entre los ideales y las subvariedades. Los puntos son las subvariedades más pequeñas, luego se corresponderán con los ideales maximales de $\mathbb{C}[x_1,x_2,x_3]$ (nuestro anillo de funciones "admisibles"). Como veremos, las subvariedades irreducibles (es decir, las que no son unión de dos subvariedades propias) se corresponden con los ideales primos. Así pues, el conjunto de los ideales primos de $\mathbb{C}[x_1,x_2,x_3]$ se corresponde con el conjunto de las subvariedades irreducibles de $\mathbb{C}^3$.

Diremos que un polinomio $p(x_1,x_2,x_3)$ se anula en el lugar geométrico definido por el sistema $(*)$ cuando $p(x_1,x_2,x_3)\in I=(p_1(x_1,x_2,x_3),\dots,p_r(x_1,x_2,x_3))$, es decir, cuando $p(x_1,x_2,x_3)$ pertenezca al ideal definido por el sistema de ecuaciones. Además, dos polinomios cualesquiera definirán la misma función algebraica sobre el lugar geométrico cuando difieran en un polinomio perteneciente al ideal. Es decir, el anillo de funciones algebraicas de la subvariedad algebraica definida por el sistema $(*)$ es $\mathbb{C}[x_1,x_2,x_3]/I$.

El lugar geométrico de un sistema de ecuaciones, como conjunto de soluciones del sistema, no recoge toda la información geométrica deseable, pero que sin embargo, sí que está en el anillo de funciones. Por ejemplo, si consideramos el sistema

$$x_1^2+x_2^2-1=0, x_1-1=0$$

podríamos decir que el lugar geométrico definido es el punto $(1,0)$. Sin embargo, diríamos que el punto $(1,0)$ está "contado" dos veces. Concepto, por ahora, impreciso. Ya veremos que este hecho está relacionado con la igualdad $\dim_{\mathbb{C}}\mathbb{C}[x_1,x_2]/(x_1^2+x_2^2-1,x_1-1)=2$.

Aunque el anillo de funciones algebraicas reales del lugar geométrico definido por un sistema de ecuaciones

$$p_1(x_1,x_2,x_3)=0,\dots,p_r(x_1,x_2,x_3)=0 \qquad (*)$$

es un concepto del todo claro, paradójicamente el propio lugar geométrico no es un concepto claro. Por ejemplo, si consideramos en el plano la ecuación

$$x_1^2+x_2^2+1=0, \qquad \text{“elipse imaginaria”}$$

podemos decir que el lugar geométrico definido es el vacío, si consideramos las soluciones sobre $\mathbb{R}$ (y no $\mathbb{C}$). Sin embargo, podemos hablar del anillo de funciones algebraicas reales de la subvariedad definida por esta ecuación, que es $\mathbb{R}[x_1,x_2]/(x_1^2+x_2^2+1)$. Además, los ideales primos maximales de $\mathbb{R}[x_1,x_2]/(x_1^2+x_2^2+1)$ cumplen que al hacer cociente por ellos obtenemos $\mathbb{C}$, y se corresponden con las soluciones imaginarias de la ecuación, módulo conjugación (ya se verá).

La intersección de variedades algebraicas es variedad algebraica. La Geometría Algebraica, con los anillos, es el marco adecuado para el desarrollo de la Teoría de la Intersección.

En general, sea k un cuerpo, $\bar{k}$ el cierre algebraico de k y $\mathrm{Aut}_{k-alg}(\bar{k})$ el conjunto de las “conjugaciones” de $\bar{k}$ (es decir, el conjunto de automorfismos de cuerpos $\tau:\bar{k}\to\bar{k}$ tales que $\tau(\lambda)=\lambda$, para todo $\lambda\in k$). Sea $I=(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))\subseteq k[x_1,\dots,x_n]$ y $A=k[x_1,\dots,x_n]/I$. Entonces, el lugar geométrico de las soluciones, sobre $\bar{k}$, del sistema de ecuaciones

$$\begin{aligned} p_1(x_1,\dots,x_n) &= 0\\ \cdots &\quad \cdots\\ p_r(x_1,\dots,x_n) &= 0 \end{aligned}$$

módulo conjugaciones, se corresponde biunívocamente con el conjunto de ideales maximales del anillo A. Explícitamente, a cada solución $(\alpha_1,\dots,\alpha_n)\in\bar{k}^n$ (y sus conjugadas) del sistema de ecuaciones le hacemos corresponder el ideal maximal $\mathfrak{m}:=\{\overline{p(x_1,\dots,x_n)}\in A$, tales que $p(\alpha_1,\dots,\alpha_n)=0\}$.

Con mayor generalidad, si K es un cuerpo algebraicamente cerrado que contiene a $\bar{k}$, “suficientemente grande”, entonces el lugar geométrico de las soluciones del sistema de ecuaciones anterior sobre K (módulo conjugaciones de K), se corresponde biunívocamente con el conjunto de ideales primos de A.

En este capítulo iniciaremos la comprensión geométrica de cualquier anillo conmutativo A, asociándole un espacio cuyos puntos se corresponden con los ideales primos de A. Espacio que denotaremos por $\mathrm{Spec}\,A$ y denominaremos espectro primo de A.

La teoría de ideales inicia el cumplimiento del sueño de Kronecker: la unificación de la Aritmética y la Geometría. Desde esta perspectiva los elementos de cualquier

anillo conmutativo pueden entenderse como funciones sobre el espectro primo del anillo. Así, por ejemplo, los números enteros, los enteros de Gauss, etc., son verdaderas funciones y les podemos aplicar intuiciones y recursos geométricos. Los números primos podrán ser interpretados geométricamente como los puntos o subvariedades irreducibles de un espacio, etc.

Las dos operaciones o procesos básicos estudiados en este capítulo, serán la localización y paso al cociente en anillos y módulos. Estos dos procesos pueden ser entendidos geométricamente como los dos procesos de restricción a abiertos y restricción a cerrados. También estudiaremos el producto tensorial, que geométricamente representa el producto directo de variedades algebraicas.

Comencemos con una revisión rápida de la definición y propiedades elementales de los anillos.

1. Definición: Un anillo A es un conjunto dotado con dos operaciones

$$A \times A \xrightarrow{+} A,\ (a,a') \mapsto a+a', \quad A \times A \xrightarrow{\cdot} A,\ (a,a') \mapsto a \cdot a',$$

que denominamos suma y producto[1], tales que

1. A es un grupo abeliano con respecto a la suma (luego tiene un elemento neutro, que se denota por 0, y cada $a \in A$ tiene un opuesto que se denota por $-a$).
2. La multiplicación es asociativa ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$) y distributiva ($a \cdot (b+c) = a \cdot b + a \cdot c$).

   Además, solo consideraremos anillos conmutativos con unidad, es decir, cumpliendo:

3. $ab = ba$, para todo $a, b \in A$.
4. Existe un elemento $1 \in A$ tal que $a1 = 1a = a$, para todo $a \in A$.

A lo largo del libro entenderemos anillo por anillo conmutativo con unidad.

Observemos que $a \cdot 0 = 0$, porque $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Observemos también que $-1 \cdot a = -a$, porque $0 = 0 \cdot a = (1+(-1)) \cdot a = a + (-1 \cdot a)$.

2. Ejemplos: 1. El anillo de los números enteros, $\mathbb{Z}$. El anillo de los números racionales $\mathbb{Q}$. El anillo de los números reales $\mathbb{R}$. El anillo de los números complejos, $\mathbb{C}$.

2. El anillo de funciones reales continuas, $C(X)$ de un espacio topológico X, con la suma y producto de funciones.

[1] Será usual utilizar la notación $a \cdot a' = aa'$.

3. Los anillos de polinomios $\mathbb{C}[x_1,\ldots,x_n]$.

4. Dado $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n$, denotamos $x^\alpha := x_1^{\alpha_1}\cdots x_n^{\alpha_n}$. Sea A un anillo, se define el "anillo de series formales en las variables $x_1,\ldots,x_n$ con coeficientes en A", que denotamos $A[[x_1,\ldots,x_n]]$, como

$$A[[x_1,\ldots,x_n]] := \{\sum_{\alpha\in\mathbb{N}^n} a_\alpha\cdot x^\alpha,\ a_\alpha\in A\},$$

donde dadas $s(x)=\sum_{\alpha\in\mathbb{N}^n} a_\alpha\cdot x^\alpha$, $t(x)=\sum_{\alpha\in\mathbb{N}^n} b_\alpha\cdot x^\alpha\in A[[x_1,\ldots,x_n]]$, se define

$$\begin{aligned} s(x)+t(x) &:= \sum_{\alpha\in\mathbb{N}^n}(a_\alpha+b_\alpha)\cdot x^\alpha \\ s(x)\cdot t(x) &:= \sum_{\alpha\in\mathbb{N}^n}(\sum_{\beta+\beta'=\alpha} a_\beta\cdot b_{\beta'})\cdot x^\alpha \end{aligned}$$

3. Definición: Un elemento $a\in A$, diremos que es un divisor de cero, si existe $b\in A$, no nulo tal que $ab=0$. Diremos que un anillo es íntegro si el único divisor de cero es el cero.

4. Ejemplos: $\mathbb{Z}$ es un anillo íntegro. Si A es un anillo íntegro entonces el anillo de polinomios con coeficientes en A, $A[x]$ es un anillo íntegro.

5. Definición: Diremos que un elemento de un anillo es invertible si tiene inverso (en el anillo con la multiplicación).

6. Definición: Diremos que un anillo es un cuerpo si todo elemento no nulo es invertible.

Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

Los cuerpos son anillos íntegros: si $a\cdot b=0$ y $b\neq 0$, entonces $0=a\cdot b\cdot b^{-1}=a$.

Anillos euclídeos

7. Definición: Un anillo íntegro A se dice que es euclídeo si existe una aplicación $\delta\colon A\setminus\{0\}\to\mathbb{N}$, que cumple

1. $\delta(a)\leq\delta(ab)$, para todo $a,b\in A\setminus\{0\}$.

2. Para cada $a\in A$ y $b\in A$ no nulo, existen $c,r\in A$, de modo que $a=bc+r$, y r es nulo ó $\delta(r)<\delta(b)$.

8. Ejercicio: Sea (A,δ) un anillo euclídeo. Pruébese que $a \in A\setminus\{0\}$ es invertible si y solo si $\delta(a) = \delta(1)$. Pruébese que si $a \in A\setminus\{0\}$ no es invertible entonces $\delta(a) > \delta(1)$. Sea $\delta' \colon A\setminus\{0\} \to \mathbb{N}$, $\delta'(a) := \delta(a) - \delta(1)$. Pruébese que (A,δ') es un anillo euclídeo y que $a \in A\setminus\{0\}$ es invertible si y solo si $\delta'(a) = 0$.

Veamos algunos ejemplos de anillos euclídeos.

9. El anillo de los números enteros: *Definimos $\delta \colon \mathbb{Z}\setminus\{0\} \to \mathbb{N}$, $\delta(n) := |n|$, donde $|n| = n$ si n es positivo y $|n| = -n$ si n es negativo. Por el teorema* **??**, *es fácil comprobar que $(\mathbb{Z},\delta)$ es un anillo euclídeo.*

10. Los anillos de polinomios: *Sea A un anillo. Diremos que el grado de un polinomio con coeficientes en A*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x], \text{ con } a_n \neq 0$$

es n y denotaremos $gr(p(x)) = n$.

Si A es un anillo íntegro, entonces el grado es una función aditiva, es decir, se cumple la fórmula

$$gr(p(x)q(x)) = gr(p(x)) + gr(q(x)) \ .$$

para cada par de polinomios $p(x), q(x) \in A[x]$ (seguimos la convención: $gr(0) = -\infty$). Por tanto, si $p(x) \neq 0$ es múltiplo de $q(x)$, entonces $gr\, p(x) \geq gr\, q(x)$.

Algoritmo de división *en el anillo de polinomios: Sea $A = k$ un cuerpo. Para cada par de polinomios no nulos $p(x), q(x) \in k[x]$, existen otros dos, $c(x), r(x)$, que denominaremos* cociente *y* resto *de dividir $p(x)$ por $q(x)$, únicos con las condiciones:*

1. $p(x) = c(x)\cdot q(x) + r(x)$.
2. $gr(r(x)) < gr(q(x))$.

Demostración. Existencia: Si $\mathrm{gr}\, q(x) > \mathrm{gr}\, p(x)$ entonces $c(x) = 0$ y $r(x) = p(x)$. Supongamos $\mathrm{gr}\, q(x) = m \leq n = \mathrm{gr}\, p(x)$ y escribamos $p(x) = a_0 x^n + \ldots + a_n$ y $q(x) = b_0 x^m + \cdots + b_m$. Procedemos por inducción sobre $\mathrm{gr}\, p(x)$. Si $\mathrm{gr}\, p(x) = 0$, entonces $\mathrm{gr}\, q(x) = 0$ y $c(x) = \frac{a_0}{b_0}$ y $r(x) = 0$. Sea, pues, $\mathrm{gr}(p(x)) > 0$. El polinomio $p'(x) := p(x) - \frac{a_0}{b_0}\cdot x^{n-m}\cdot q(x)$ es de grado menor que el de $p(x)$, luego por hipótesis de inducción, existen $c'(x)$ y $r'(x)$ tales que $p'(x) = c'(x)\cdot q(x) + r'(x)$ y $gr(r'(x)) < gr(q(x))$. Entonces, $c(x) := c'(x) + \frac{a_0}{b_0}\cdot x^{n-m}$ y $r(x) := r'(x)$ cumplen lo exigido.

Unicidad: Al lector. □

Por lo tanto, $(k[x], \mathrm{gr})$ es un anillo euclídeo.

11. El anillo de los enteros de Gauss: *Sea* $\mathbb{Z}[i] := \{a+bi \in \mathbb{C} : a,b \in \mathbb{Z}\}$. $\mathbb{Z}[i]$ *es un anillo (subanillo de* $\mathbb{C}$*) y se denomina el anillo de los enteros de Gauss.* $\mathbb{Z}[i]$ *con la aplicación*

$$\delta : \mathbb{Z}[i] \to \mathbb{N}, \quad \delta(a+bi) := (a+bi)\cdot(a-bi) = a^2+b^2$$

es un anillo euclídeo:

Dados $z, z' \in \mathbb{Z}[i]$ no nulos se cumple que $\delta(zz') = \delta(z)\delta(z') \geq \delta(z)$. Dado un número complejo $a+bi \in \mathbb{C}$, denotemos $|a+bi| = a^2+b^2 \in \mathbb{R}$. Consideremos el número complejo $z/z' \in \mathbb{C}$ y consideremos un entero de Gauss $c \in \mathbb{Z}[i]$ lo más cercano posible a z/z'. Tenemos que $|z/z' - c| < 1$. Sea $r := z - z'c$, si $r \neq 0$ entonces

$$\delta(r) = \delta(z - z'c) = |z'(z/z' - c)| = |z'||z/z' - c| < |z'|$$

Tenemos, pues, que $z = z'c + r$ con $r = 0$ ó $\delta(r) < \delta(z')$.

0.2.1. Ideales de un anillo. Cociente por un ideal

12. Definición: Un subconjunto $I \subseteq A$ diremos que es un ideal de A si es un subgrupo para la suma y cumple que $a \cdot i \in I$, para todo $a \in A$ y todo $i \in I$.

Los subconjuntos $\{0\}$ y A son ideales del anillo A.

Dado $a \in A$, el conjunto $a \cdot A := \{a \cdot b \in A, \forall b \in A\}$ es un ideal de A. Si $I \subseteq \mathbb{Z}$ es un ideal, entonces existe un $n \in \mathbb{Z}$ tal que $I = n \cdot \mathbb{Z}$ (por el teorema **??**).

Un anillo es un cuerpo si y solo si los únicos ideales del anillo son el (0) y todo el anillo: Si A es un cuerpo e $I \subset A$ es un ideal no nulo, entonces existe $a \in I$ no nulo; como $a \cdot A = A$ tendremos que $I = A$. Recíprocamente, si A no contiene más ideales que $\{0\}$ y A, dado $a \in A$ no nulo tendremos que $a \cdot A = A$, lo que implica que $1 \in a \cdot A$, luego a es invertible.

13. Ejercicio: Sea X un conjunto y $\mathrm{Aplic}(X,\mathbb{R})$ el conjunto de las aplicaciones de X en $\mathbb{R}$. Con la suma y producto ordinarios de funciones $\mathrm{Aplic}(X,\mathbb{R})$ es un anillo. Sea $Y \subset X$ un subconjunto, prueba que $\{f \in \mathrm{Aplic}(X,\mathbb{R}) : f(y) = 0,\ \forall y \in Y\}$ es un ideal de $\mathrm{Aplic}(X,\mathbb{R})$.

La intersección de ideales es un ideal. Dado un subconjunto $F \subseteq A$, denotaremos por (F) al ideal mínimo de A que contiene a F (que es la intersección de todos los ideales que contienen a F). Diremos que el ideal (F) está generado por F. Explícitamente $(F) = \{a \in A : a = \sum_{i=0}^{n} a_i f_i$ con $f_i \in F, a_i \in A$ y $n \in \mathbb{N}$ cualesquiera$\}$. Dado $a \in A$, tenemos que $(a) = aA$. Dados dos ideales I_1 e I_2 de A, llamaremos suma de los dos ideales, que denotaremos por $I_1 + I_2$, al ideal de A definido por $I_1 + I_2 := \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$, que es el mínimo ideal de A que contiene a I_1 y I_2.

14. Definición: Sea A un anillo. Diremos que un ideal $I \subseteq A$ es principal si existe $a \in A$ tal que $I = aA$. Diremos que un anillo es un dominio de ideales principales si es un anillo íntegro cuyos ideales son principales.

$\mathbb{Z}$ es un dominio de ideales principales.

15. Proposición: *Los anillos euclídeos son dominios de ideales principales.*

Demostración. Sea (A,δ) un anillo euclídeo e $I \subset A$ un ideal no nulo. Sea $i \in I$ un elemento no nulo tal que $\delta(i) = \min\{\delta(j)\}_{j\in I\setminus\{0\}}$. Veamos que $I = i\cdot A$: Dado $j \in I$ no nulo, existen $c,r \in A$ de modo que $j = c\cdot i + r$ y $r = 0$ ó $\delta(r) < \delta(i)$. Observemos que $r \in I$, luego no es posible que $\delta(r) < \delta(i)$. En conclusión, $j = c\cdot i$. Por tanto, $I = i\cdot A$.

□

El ideal $\mathfrak{p} = (2, x_1)$ del anillo $\mathbb{Z}[x_1,\dots x_n]$ no es principal: un generador de $\mathfrak{p}$ sería un divisor de 2 y éstos son ± 1 y ± 2, y $1\cdot\mathbb{Z}[x_1,\dots,x_n]$ y $2\cdot\mathbb{Z}[x_1,\dots,x_n]$ son ideales distintos de $\mathfrak{p}$. En consecuencia, los anillos $\mathbb{Z}[x_1,\dots,x_n]$ no son dominios de ideales principales.

Análogamente, si k es un cuerpo, el ideal (x_1,x_2) del anillo $k[x_1,\dots,x_n]$ no es principal, así que los anillos $k[x_1,\dots,x_n]$ no son dominios de ideales principales (para $n > 1$).

Sea $I \subseteq A$ un ideal. Como I es un subgrupo (aditivo) de A, podemos considerar el grupo cociente A/I, donde

$$A/I := \{\bar{a} \text{ (donde } \bar{a} := a + I),\ \forall\, a \in A\},$$

y $\bar{a} + \bar{b} := \overline{a+b}$. Recordemos que $\bar{a} = \bar{b}$ si y solo si $a - b \in I$. Podemos definir en A/I la operación "producto", $\bar{a}\cdot\bar{a'} := \overline{a\cdot a'}$, que dota a A/I de estructura de anillo (compruébese).

16. Ejemplo: Consideremos el ideal $9\cdot\mathbb{Z} \subseteq \mathbb{Z}$. En $\mathbb{Z}/9\cdot\mathbb{Z}$ tenemos que $\overline{10^n} = \overline{10}^n = \bar{1}^n = \bar{1}$. Por tanto, dado un número natural cualquiera, por ejemplo $7836 \in \mathbb{N}$, tenemos que

$$\overline{7836} = \overline{7\cdot 10^3 + 8\cdot 10^2 + 3\cdot 10 + 6} = \overline{7}\cdot\overline{10^3} + \overline{8}\cdot\overline{10^2} + \overline{3}\cdot\overline{10} + \overline{6} = \bar{7} + \bar{8} + \bar{3} + \bar{6} = \overline{7+8+3+6}$$

Por tanto, 7836 es divisible por 9 (es decir, $\overline{7836} = \bar{0}$) si y solo si $7+8+3+6$ es divisible por 9 (es decir, $\overline{7+8+3+6} = \bar{0}$). En general, un número natural $n = n_1 n_2 \dots n_r$, escrito en base decimal, es divisible por nueve si y solo si la suma de sus cifras, $n_1 + \dots + n_r$ es divisible por nueve.

0.2.2. Morfismo de anillos

17. Definición: Una aplicación $f : A \to B$ entre los anillos A y B, diremos que es un morfismo de anillos si cumple

1. $f(a+a') = f(a) + f(a')$, para todo $a, a' \in A$.

2. $f(aa') = f(a)f(a')$, para todo $a, a' \in A$.

3. $f(1) = 1$.

18. Ejemplos: Sea $I \subset A$ un ideal. El morfismo de paso al cociente $\pi\colon A \to A/I$, $a \mapsto \bar{a}$ es un morfismo de anillos.

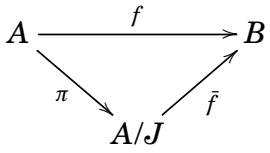
La aplicación $\mathbb{C}[x] \to \mathbb{C}$, $p(x) \mapsto p(33)$, es un morfismo de anillos.

Dada una aplicación continua $\phi\colon X \to Y$ entre espacios topológicos, la aplicación inducida $\tilde{\phi}\colon C(Y) \to C(X)$, $f \mapsto f \circ \phi$ es un morfismo de anillos.

La composición de morfismos de anillos es un morfismo de anillos. La imagen de un morfismo de anillos $f : A \to B$, $\operatorname{Im} f$, es un subanillo de B, es decir, un subconjunto de B que con las operaciones de B es anillo y la unidad de B pertenece al subanillo.

El núcleo de un morfismo de anillos f, $\operatorname{Ker} f := \{a \in A\colon f(a) = 0\}$, es un ideal. La antimagen por un morfismo de anillos de un ideal es un ideal. Si un morfismo de anillos es epiyectivo la imagen de un ideal es un ideal.

Sea $f : A \to B$ un morfismo de anillos. Si $J \subseteq A$ es un ideal incluido en $\operatorname{Ker} f$, entonces existe un único morfismo de anillos $\bar{f}\colon A/J \to B$ (definido por $\bar{f}(\bar{a}) = f(a)$) de modo que el diagrama



es conmutativo, siendo π el morfismo de paso al cociente, $\pi(a) = \bar{a}$. Como consecuencia del teorema de isomorfía para morfismos de grupos obtenemos el siguiente teorema.

19. Teorema de isomorfía: *Sea $f : A \to B$ un morfismo de anillos. La aplicación*

$$\bar{f}\colon A/\operatorname{Ker} f \to \operatorname{Im} f,\ \bar{f}(\bar{a}) := f(a)$$

es un isomorfismo de anillos.

20. Ejemplo: El cuerpo de los números complejos es isomorfo a $\mathbb{R}[x]/(x^2+1)$: Consideremos el morfismo de anillos $f : \mathbb{R}[x] \to \mathbb{C}$, $f(p(x)) := p(i)$. El morfismo f es epiyectivo. Sea $\operatorname{Ker} f = (p(x))$. Obviamente, $x^2 + 1 \in \operatorname{Ker} f$, luego $p(x)$ ha de dividir a $x^2 + 1$. Como no existe ningún polinomio de grado 1 en $\operatorname{Ker} f$, concluimos que $\operatorname{Ker} f = (x^2 + 1)$ y por el teorema de isomorfía $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

0.2.3. Ideales primos. Ideales maximales

21. Definición: Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$, diremos que es un ideal primo de A, si cumple que si $ab \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

22. Proposición: *Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$ es un ideal primo si y solo si $A/\mathfrak{p}$ es un anillo íntegro.*

Demostración. Supongamos que $\mathfrak{p} \subset A$ es un ideal primo. Si $\bar{a} \cdot \bar{a'} = 0$ en $A/\mathfrak{p}$ entonces $\overline{a \cdot a'} = 0$, luego $a \cdot a' \in \mathfrak{p}$. Por tanto, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. En conclusión $A/\mathfrak{p}$ es íntegro.

Recíprocamente, supongamos que $A/\mathfrak{p}$ es íntegro. Si $a \cdot a' \in \mathfrak{p}$, entonces $\overline{a \cdot a'} = 0$ en $A/\mathfrak{p}$. Por tanto, $\bar{a} \cdot \bar{a'} = 0$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. Es decir, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$. En conclusión, $\mathfrak{p}$ es un ideal primo. □

23. Ejercicio: Sea $\mathfrak{p} = (2, x) \subset \mathbb{Z}[x, y]$. Prueba que $\mathbb{Z}[x, y]/\mathfrak{p} \simeq \mathbb{Z}/2\mathbb{Z}[y]$. Prueba que $\mathfrak{p}$ es un ideal primo.

24. Definición: Diremos que un ideal $\mathfrak{m} \underset{\neq}{\subset} A$ es maximal si los únicos ideales que contienen a $\mathfrak{m}$ son $\mathfrak{m}$ y A.

25. Proposición: *En todo anillo $A \neq 0$ existen ideales maximales.*

Demostración. La demostración es una aplicación típica del lema de Zorn (que puede evitarse en anillos noetherianos). Sea X el conjunto de los ideales de A, distintos de A. En X podemos definir una relación de orden: decimos que un ideal I es menor o igual que otro I' cuando $I \subseteq I'$. Observemos que toda cadena de ideales, distintos de A tiene una cota superior: la unión de los ideales de la cadena (que es distinto de A, pues el 1 no está en ninguno de ellos, ni por tanto en la unión). El lema de Zorn nos dice que existen elementos de X maximales, es decir, existen ideales maximales. □

26. Ejercicio: Se dice que un ideal primo es minimal si no contiene estrictamente ningún ideal primo. En todo anillo $A \neq 0$ existen ideales primos minimales.

27. Lema: *Sea $\pi : A \to A/I$ el morfismo de paso al cociente. Las aplicaciones*

$$\begin{array}{rcl} \left\{\begin{array}{l} \textit{Ideales de } A \\ \textit{que contienen a } I \end{array}\right\} & = & \{\textit{Ideales de } A/I\} \\ J & \longmapsto & \pi(J) \\ \pi^{-1}(J') & \longmapsto & J' \end{array}$$

son inversas entre sí (y conservan inclusiones).

Demostración. Observemos que $\pi(\pi^{-1}(J')) = J'$ porque π es epiyectiva, y $\pi^{-1}(\pi(J)) = J + I = J$. □

28. Corolario: *Todo ideal $I \subsetneq A$ está incluido en un ideal maximal.*

Demostración. Por el lema anterior, los ideales maximales de A que contienen a I se corresponden con los ideales maximales de A/I, que no es vacío por la proposición anterior. □

Un elemento $a \in A$ es invertible si y solo si $(a) = A$. Por tanto, $a \in A$ es invertible si y solo si no está incluido en ningún ideal maximal (suponemos $A \neq 0$).

29. Proposición: *Un ideal $\mathfrak{m} \subsetneq A$ es maximal si y solo si $A/\mathfrak{m}$ es un cuerpo. En particular, por la proposición 0.2.22, los ideales maximales son ideales primos.*

Demostración. $A/\mathfrak{m}$ es cuerpo si y solo si el único ideal maximal es el (0). Que equivale a decir que el único ideal maximal de A que contiene a $\mathfrak{m}$ es $\mathfrak{m}$, es decir, $\mathfrak{m}$ es maximal. □

30. Definiciones: Sea A un anillo íntegro y $a \in A$. Se dice que a es propio si no es nulo ni invertible. Se dice que a es irreducible si es propio y no descompone en producto de dos elementos propios. Se dice que a es primo (en A) si es propio y (a) es un ideal primo.

31. Nota: Observemos que decimos que -5 es un elemento primo de $\mathbb{Z}$.

32. Proposición: *Sea A un anillo íntegro. Si $a \in A$ es primo, entonces es irreducible.*

Demostración. Si $a = b \cdot c$, entonces $b \in (a)$ (o $c \in (a)$) porque (a) es un ideal primo. Luego, $b = ad$ para cierto $d \in A$. Por tanto, $a = bc = adc$ y $dc = 1$. Es decir, c es invertible y a es irreducible. □

33. Proposición: *Sea p un elemento no nulo de un dominio de ideales principales A. Las siguientes condiciones son equivalentes:*

1. *p es irreducible.*
2. *p es primo.*
3. *pA es un ideal maximal de A.*

Demostración. 3. $\Rightarrow$ 2. Obvio.

2. $\Rightarrow$ 1. Es consecuencia de 0.2.32.

1. $\Rightarrow$ 3. Si $pA \subseteq I = aA \underset{\neq}{\subset} A$, entonces existe $b \in A$ tal que $ab = p$. Luego, b es invertible y $I = pA$. En conclusión, pA es maximal.

□

Congruencias de Wilson y Fermat

34. Notaciones: Escribiremos $m \equiv m' \, mod \, n$ y leeremos m es congruente con m' módulo n, cuando $\bar{m} = \bar{m'}$ en $\mathbb{Z}/n\mathbb{Z}$ (es decir, el resto de dividir m por n coincide con el resto de dividir m' por n).

Dado un anillo A, denotaremos A^* al grupo (con la multiplicación) formado por los elementos invertibles de A.

Si $p \in \mathbb{Z}$ es un número primo entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, porque $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ por la proposición 0.2.33

35. Congruencia de Wilson: *Si p es un número natural primo, entonces:*

$$(p-1)! \equiv -1 \, mod \, p.$$

Demostración. $(p-1)! \, mod \, p$ es el producto de todos los elementos del grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Si $\bar{m} \in (\mathbb{Z}/p\mathbb{Z})^*$ no es igual a su inverso, entonces en este producto ambos se cancelan (dando 1) luego en el producto mencionado solo permanecen aquellos $\bar{m}$ que verifiquen que son igual a su inverso. Ahora bien, $1 = \bar{m} \cdot \bar{m} = \bar{m}^2$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\bar{m}$ es raíz del polinomio $x^2 - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[x]$. Como $x^2 - \bar{1} = (x + \bar{1}) \cdot (x - \bar{1})$, $\bar{m}$ es igual a su inverso si y solo si $\bar{m} = \pm\bar{1}$. Por tanto, $(p-1)! = 1 \cdot (-1) = -1$ en $\mathbb{Z}/p\mathbb{Z}$. □

36. Congruencia de Fermat: *Si p es un número natural primo y m no es divisible por p, entonces*

$$m^{p-1} \equiv 1 \, mod \, p.$$

Demostración. Es consecuencia de 0.1.27, aplicado al caso $G = (\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ y $g = \bar{m}$. □

0.3. Dominios de factorización única

1. Definición: Un anillo íntegro se dice que es un dominio de factorización única si todo elemento propio (no nulo ni invertible) del anillo es producto de elementos irreducibles, de modo único salvo orden de los factores y multiplicación de éstos por invertibles. DFU significará dominio de factorización única.

En la demostración de que todo número natural es producto de irreducibles es esencial observar que toda sucesión de números naturales $n_1, n_2, \ldots, n_r, \ldots$ tal que n_{i+1} divide a n_i estabiliza, es decir, existe m tal que $n_m = n_{m+1} = n_{m+2} = \cdots$. Para demostrar la unicidad es esencial probar que los números naturales irreducibles son los números (naturales) primos.

Diremos que una cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ estabiliza si existe m, tal que $I_m = I_{m+1} = I_{m+2} = \cdots$.

2. Lema: *Sea A un anillo íntegro y $a, b \in A$. Entonces, $(a) = (b)$ si y solo si $a = b \cdot i$ para cierto invertible $i \in A$.*

Demostración. $\Rightarrow$) Si $(a) = (b)$ existen $i, i' \in A$ tales que $a = bi$ y $b = ai'$. Por tanto, $a = ai'i$. Como A es íntegro, $1 = ii'$, luego i es invertible.

□

3. Teorema de descomposición única en factores irreducibles: *Sea A un anillo íntegro. A es un dominio de factorización única si y solo si toda cadena ascendente de ideales principales estabiliza y todo elemento irreducible es primo.*

Demostración. $\Rightarrow$) Si $a = p_1 \cdots p_r$ (p_i irreducibles para todo i) y $aA \underset{\neq}{\subseteq} bA$ entonces reordenando los factores $b = p_1 \cdots p_s \cdot inv$ con $s < r$. Ahora, es claro que toda cadena ascendente de ideales principales es estable.

Sea $a \in A$ irreducible. Si $b \cdot c \in (a)$, entonces existe $d \in A$ tal que $bc = ad$. Sea $b = b_1 \cdots b_r$, $c = c_1 \cdots c_s$ y $d = d_1 \cdots d_t$ las descomposiciones en factores irreducibles de b, c, d. Entonces,

$$b_1 \cdots b_r \cdot c_1 \cdots c_s = a \cdot d_1 \cdots d_t.$$

Como A es un dominio de factorización única, a ha de coincidir, salvo multiplicación por un invertible, con algún b_i o algún c_j. Luego, a divide a b, es decir. $b \in (a)$; o a divide a c, es decir, $c \in (a)$. En conclusión, (a) es un ideal primo.

$\Leftarrow$) Empecemos probando que a todo elemento $a \in A$ lo divide algún elemento irreducible: Si a no es irreducible entonces $a = a_1 \cdot b_1$, a_1, b_1 elementos propios. Si a_1 no es irreducible, entonces $a_1 = a_2 \cdot b_2$, con a_2, b_2 elementos propios. Así sucesivamente, vamos obteniendo una cadena de ideales principales $(a) \underset{\neq}{\subseteq} (a_1) \underset{\neq}{\subseteq} (a_2) \underset{\neq}{\subseteq} \ldots$ que ha de

ser finita y terminará cuando a_n sea irreducible, para cierto n. Con lo que tenemos un irreducible, a_n, que divide a a.

Ahora ya, sea a_1 irreducible que divide a a y escribamos $a = a_1 \cdot b_1$. Si b_1 no es irreducible sea a_2 irreducible, que divide a b_1 y escribamos $a = a_1 \cdot b_1 = a_1 \cdot a_2 \cdot b_2$. Así sucesivamente, vamos obteniendo la cadena $(a) \underset{\neq}{\subset} (b_1) \underset{\neq}{\subset} (b_2) \underset{\neq}{\subset} \dots$ que ha de ser finita y terminará cuando b_n sea irreducible. En tal caso, $a = a_1 \cdots a_{n-1} \cdot b_n$ que es producto de irreducibles.

Sean $p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones en factores irreducibles. Entonces, q_1 divide algún factor p_i, luego coincide con él (salvo multiplicación por un invertible). Reordenando los factores podemos decir que $p_1 = q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$ (salvo multiplicación por un invertible). Razonando con q_2 como hemos hecho antes con q_1 llegamos a que q_2 coincide con algún p_i. Reiterando el argumento, obtendremos que las dos descomposiciones son iguales (salvo orden y factores invertibles).

□

4. Teorema: *Los dominios de ideales principales son dominios de factorización única.*

Demostración. Si $p \in A$ es irreducible entonces es primo, por la proposición 0.2.33. Sea $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ una cadena ascendente de ideales. Sea $I = \cup_{i=1}^{\infty} I_i$, que es un ideal de A, luego $I = a \cdot A$. Sea I_m tal que $a \in I_m$, entonces $I = I_m = I_{m+1} = \cdots$. Por el teorema 0.3.3, hemos terminado. □

5. Corolario: *Los anillos euclídeos son dominios de factorización única.*

Demostración. Recordemos que los anillos euclídeos son dominios de ideales principales (ver 0.2.15). □

0.3.1. Máximo común divisor

6. Definición: Se dice que dos elementos de un anillo íntegro son primos entre sí si no existe un elemento propio que los divida a los dos.

Sea A un dominio de factorización única, $a, b \in A$ y escribamos $a = u \cdot p_1^{n_1} \cdots p_r^{n_r}$, $b = v \cdot p_1^{m_1} \cdots p_r^{m_r}$, con u, v invertibles, $n_i, m_i \geq 0$ y $p_1, \dots, p_r$ irreducibles y primos entre sí. Definimos (salvo multiplicación por invertibles) el máximo común divisor de a y b, que denotaremos $m.c.d.(a,b)$ y el mínimo común múltiplo de a y b, que denotaremos $m.c.m.(a,b)$ como sigue:

$$m.c.d.(a,b) := p_1^{\text{mín}(n_1,m_1)} \cdots p_r^{\text{mín}(n_r,m_r)}$$
$$m.c.m.(a,b) := p_1^{\text{máx}(n_1,m_1)} \cdots p_r^{\text{máx}(n_r,m_r)}$$

Observemos que $m.c.d.(a,b)$ divide á a y b y si m divide a a y b, entonces m divide a $m.c.d.(a,b)$. Estas dos propiedades caracterizan al máximo común divisor, porque si d las cumple entonces d divide a $m.c.d.(a,b)$ y recíprocamente, luego salvo multiplicación por un invertible d es igual a $m.c.d.(a,b)$.

Observemos que $m.c.m.(a,b)$ es múltiplo de a y b y si m es múltiplo de a y b, entonces m es múltiplo de $m.c.m.(a,b)$. Estas dos propiedades caracterizan al mínimo común múltiplo.

7. Teorema : *Un anillo A es DIP si y solo si es DFU y todo ideal primo no nulo es maximal.*

Demostración. $\Rightarrow$) Es consecuencia del teorema 0.3.4 y la proposición 0.2.33.

$\Leftarrow$) Sea $\mathfrak{p}$ un ideal primo no nulo. Dado $0 \neq a \in \mathfrak{p}$, tenemos que $a = p_1 \cdots p_r$, con p_i irreducibles, luego algún irreducible $p_i \in \mathfrak{p}$, luego $(p_i) = \mathfrak{p}$. Si $a,b \in A$, no nulos, son primos entre sí, entonces (a,b) no está incluido en ningún ideal primo, luego $(a,b) = A$. Dados $a,b \in A$ no nulos, tenemos que

$$(a,b) = (m.c.d(a,b)\cdot c, m.c.d(a,b)\cdot d) = m.c.d(a,b)\cdot(c,d) = m.c.d(a,b)\cdot A.$$

Dado un ideal I no nulo y distinto de A, sea $a = p_1 \cdots p_r \in I$ con p_i irreducibles con r mínimo posible. Dado $b \in I$ no nulo, tenemos que $m.c.d(a,b) \in (a,b) \subseteq I$ y divide a a, luego $m.c.d.(a,b) = a \cdot inv$. En conclusión, $b \in (a)$ y $I = (a)$.

□

Si A es un dominio de ideales principales y $a,b \in A$, entonces $aA + bA = dA$, siendo d "el máximo común divisor de a y b": Si c divide á a y b entonces divide á d y obviamente d divide á a y b. Igualmente, el mínimo común múltiplo de a y b es el generador del ideal $aA \cap bA$.

8. Identidad de Bézout: *Sea A un dominio de ideales principales y sean $a,b \in A$. Sea d el máximo común divisor de a y b. Existen elementos $\alpha, \beta \in A$ tales que*

$$d = \alpha a + \beta b.$$

9. Algoritmo de Euclides : Este algoritmo nos permite calcular en anillos euclídeos el máximo común divisor de dos elementos del anillo. Dados $a_1, a_2 \in A$ definimos por recurrencia a_{i+1} el resto de dividir a_{i-1} por a_i. Entonces, escribimos

$$\begin{aligned} a_1 &= a_2 c_1 + a_3 \\ a_2 &= a_3 c_2 + a_4 \\ a_3 &= a_4 c_3 + a_5 \\ &\cdots \\ a_{s-2} &= a_{s-1} c_{s-2} + a_s \end{aligned}$$

y terminamos cuando s sea el primero tal que $a_s = 0$.

Observemos que d divide á a_1 y a_2 si y solo si divide a a_2 y a_3, si y solo si ... divide a a_{s-2} y a_{s-1}, si y solo si divide a a_{s-1}. Luego, $m.c.d(a_1, a_2) = a_{s-1}$ (único salvo multiplicación por invertibles).

Además, el algoritmo de Euclides nos permite calcular λ, μ tales que $\lambda \cdot a_1 + \mu \cdot a_2 = m.c.d(a_1, a_2)$: Sabemos expresar a_3 como combinación A-lineal de a_1 y a_2, luego sabemos expresar a_4 como combinación A-lineal de a_1 y a_2, y así sucesivamente sabremos expresar a_{s-1} como combinación A-lineal de a_1 y a_2.

10. Teorema chino de los restos: *Sea A un anillo e $I_1, I_2 \subseteq A$ dos ideales tales que $I_1 + I_2 = A$. Entonces, el morfismo natural*

$$A/(I_1 \cap I_2) \to A/I_1 \times A/I_2, \quad \bar{a} \mapsto (\bar{a}, \bar{a})$$

es un isomorfismo

Demostración. El núcleo del morfismo $f : A \to A/I_1 \times A/I_2$, $f(a) = (\bar{a}, \bar{a})$ es claramente $I_1 \cap I_2$. Por el teorema de isomorfía, solo nos falta probar que es epiyectivo. Sea $(\bar{a}, \bar{b}) \in A/I_1 \times A/I_2$. Observemos que en A/I_2, $A/I_2 = \overline{a + I_1 + I_2} = \overline{a + I_1}$. Por tanto, existe $i_1 \in I_1$ de modo que $\overline{a + i_1} = \bar{b}$ en A/I_2. Por tanto, $f(a + i_1) = (\overline{a + i_1}, \overline{a + i_1}) = (\bar{a}, \bar{b})$. □

11. Sean $n, m \in \mathbb{Z}$ primos entre sí (luego $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$). Por el teorema chino de los restos se tiene el isomorfismo

$$\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \bar{r} \mapsto (\bar{r}, \bar{r})$$

Calculemos el morfismo inverso: Sabemos calcular $\lambda, \mu \in \mathbb{Z}$ de modo que $\lambda \cdot n + \mu \cdot m = 1$. Luego, $\lambda \cdot n \mapsto (\bar{0}, \bar{1})$ y $\mu \cdot m \mapsto (\bar{1}, \bar{0})$. Luego, el morfismo $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z}$, $(\bar{r}, \bar{s}) \mapsto \overline{r \cdot \mu \cdot m + s \cdot \lambda \cdot n}$ es el morfismo inverso buscado.

12. Calculemos las soluciones enteras de la siguiente ecuación diofántica (es decir, ecuación con coeficientes enteros),

$$2000x - 266y = -4.$$

Primero calculemos mediante el algoritmo de Euclides, $n, m \in \mathbb{Z}$, tales que

$$2000n + 266 \cdot (-m) = m.c.d(2000, 266).$$

a. $2000 = 7 \cdot 266 + 138$. b. $266 = 1 \cdot 138 + 128$. c. $138 = 1 \cdot 128 + 10$. d. $128 = 12 \cdot 10 + 8$ e. $10 = 1 \cdot 8 + 2$. Luego, $m.c.d(2000, 266) = 2$. Lo cual era evidente, pero ahora sabremos calcular n y m: $2 = 10 - 1 \cdot 8 = 10 - 1 \cdot (128 - 12 \cdot 10) = -128 + 13 \cdot 10 = -128 + 13(138 - 128) =$

$13\cdot 138-14\cdot 128=13\cdot 138-14(266-138)=-14\cdot 266+27\cdot 138=-14\cdot 266+27(2000-7\cdot 266)=27\cdot 2000-203\cdot 266$.

Por tanto, una solución particular de nuestro sistema de ecuaciones diofánticas es $x_0=-2\cdot 27=-54$, $y_0=-2\cdot 203=-406$. Las soluciones de la ecuación homogénea $2000x-266y=0$ son las soluciones de $1000x-133y=0$, que son $x=n\cdot 133$, $y=n\cdot 1000$. Todas las soluciones de nuestro sistema de ecuaciones diofánticas son

$$\begin{cases} x=-54+n\cdot 133 \\ y=-406+n\cdot 1000 \end{cases}$$

0.3.2. Anillo de fracciones

13. Definición: Sea A un anillo y $S\subseteq A$ un subconjunto. Diremos que S es un sistema multiplicativo de A si cumple

1. $1\in S$.
2. Si $s,s'\in S$ entonces $s\cdot s'\in S$.

14. Ejemplos: $\mathbb{Z}\backslash\{0\}$ es un sistema multiplicativo de $\mathbb{Z}$. Si A es un anillo íntegro, entonces $A\backslash\{0\}$ es un sistema multiplicativo. Si $\mathfrak{p}\subset A$ es un ideal primo, entonces $A\backslash\mathfrak{p}$ es un sistema multiplicativo. Dado $a\in A$, $S=\{1,a,a^2,\ldots,a^n,\ldots\}$ es un sitema multiplicativo.

Sea A un anillo y $S\subset A$ un sistema multiplicativo de A. Podemos definir en el conjunto $A\times S$ la siguiente relación de equivalencia:

$$(a,s)\sim(a',s') \iff \text{existen } s_1,s_2\in S \text{ tales que } (as_1,ss_1)=(a's_2,s's_2).$$

Denotaremos $\frac{a}{s}$ a la clase de equivalencia de (a,s).

15. Definición: Sea A un anillo y $S\subset A$ un sistema multiplicativo de A. La localización de A por S, A_S, es el conjunto

$$A_S:=\left\{\frac{a}{s},\ \forall\, a\in A \text{ y } \forall\, s\in S\right\}.$$

Observemos que $\frac{a}{s}=\frac{a'}{s'}$ si y solo si existen $s_1,s_2\in S$ tales que $as_1=a's_2$ y $ss_1=s's_2$.. Luego, $\frac{a}{s}=\frac{as_1}{ss_1}=\frac{a's_2}{s's_2}=\frac{a'}{s'}$, donde las fracciones del medio tienen igual numerador y denominador. Ahora es fácil probar la siguiente afirmación:

> Sea B un conjunto. Dar una aplicación $\phi\colon A_S\to B$, es asignar a cada $\frac{a}{s}\in A_S$ un elemento $\varphi(a,s)\in B$ de modo que $\varphi(at,st)=\varphi(a,s)$ para todo $t\in S$.

Con la suma y producto ordinarios de fracciones

$$\frac{a}{s}+\frac{a'}{s'}:=\frac{s'a+sa'}{ss'}$$
$$\frac{a}{s}\cdot\frac{a'}{s'}:=\frac{aa'}{ss'}$$

A_S es un anillo. El elemento unidad de A_S es la fracción $\frac{1}{1}$. Si $s\in S$ entonces la fracción $\frac{s}{1}$ es invertible, de inverso $\frac{1}{s}$. La fracción $\frac{0}{s}=\frac{0\cdot s}{1\cdot s}=\frac{0}{1}$ es el elemento nulo de A_S.

16. Definición: Al morfismo natural de anillos $A\to A_S$, $a\mapsto\frac{a}{1}$ se le denomina morfismo de localización por S.

Denotaremos $\frac{a}{1}=a$, cuando no sea causa de confusión.

17. Definición: Si A es un anillo íntegro, obviamente $A_{A\setminus\{0\}}$ es un cuerpo y diremos que es el cuerpo de fracciones de A.

18. Ejemplos: 1. $\mathbb{Q}=\mathbb{Z}_{\mathbb{Z}\setminus\{0\}}$,

2. $\mathbb{Q}(x):=\mathbb{Q}[x]_{\mathbb{Q}[x]\setminus\{0\}}$

3. $k(x):=k[x]_{k[x]\setminus\{0\}}=\{p(x)/q(x)\colon\ p(x),q(x)\in k[x],q(x)\neq 0\}$, o con mayor generalidad, el cuerpo de funciones racionales en n-variables con coeficientes en k,

$$k(x_1,\ldots,x_n):=k[x_1,\ldots,x_n]_{k[x_1,\ldots,x_n]\setminus\{0\}}=\{p(x)/q(x)\colon\\ p(x),0\neq q(x)\in k[x_1,\ldots,x_n]\}$$

19. Proposición: *Sea A_S la localización de A por S. Entonces,*

1. *$\frac{a}{s}=0$ si y solo si existe $s'\in S$ tal que $s'\cdot a=0$ (en A).*

2. *$\frac{a}{s}=\frac{a'}{s'}$ en A_S si y solo si existe un $t\in S$ de modo que $t\cdot(as'-a's)=0$.*

Demostración. 1. $\Rightarrow$) $0=\frac{0}{1}=\frac{a}{s}$ luego existen $t,t'\in S$ tales que $t\cdot 0=t'\cdot a$ (y $t\cdot 1=t'\cdot s$), luego $t'\cdot a=0$.
$\Leftarrow$) $\frac{a}{s}=\frac{as'}{ss'}=\frac{0}{ss'}=\frac{0}{1}=0$.
2. $\Rightarrow$) $0=\frac{a}{s}-\frac{a'}{s'}=\frac{as'-a's}{ss'}$, existe un $t\in S$ de modo que $t\cdot(as'-a's)=0$, por el punto 1.
$\Leftarrow$) Si $t\cdot(as'-a's)=0$, entonces $0=\frac{as'-a's}{ss'}=\frac{a}{s}-\frac{a'}{s'}$, entonces $\frac{a}{s}=\frac{a'}{s'}$.

□

20. Ejercicio: Sea A un anillo y $S\subseteq A$ un sistema multiplicativo. Entonces, $A_S=\{0\}$ $\iff$ $0\in S$.

21. Ejercicio: Sea A un anillo íntegro y $S \subseteq A\setminus\{0\}$ un sistema multiplicativo. Entonces, $\frac{a}{s} = \frac{a'}{s'}$ en A_S si y solo si $as' - a's = 0$ (en A).

22. Ejercicio: Pruébese que $(\mathbb{Z}[x])_{\mathbb{Z}\setminus\{0\}} = \mathbb{Q}[x]$.

23. Ejercicio: Sea $S \subset A$ un sistema multiplicac¡tivo. Un morfismo de anillos $f : A \to B$ factoriza (de modo único) a través del morfismo de localización $A \to A_S$ si y solo si $f(s)$ es invertible para todo $s \in S$.

0.3.3. Lema de Gauss

24. Lema: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Sean $P(x), Q(x) \in A[x]$ dos polinomios primitivos. Entonces,*

1. *$P(x)\cdot Q(x)$ es primitivo.*

2. *Si existen $a, b \in A$ tales que $a \cdot P(x) = b \cdot Q(x)$, entonces $b = a \cdot u$, para cierto invertible $u \in A$. Por tanto, si $P(x) = \frac{b}{a} \cdot Q(x)$ en $\Sigma[x]$, entonces $\frac{b}{a} = u \in A$ es un invertible de A.*

Demostración. 1. Supongamos que $P(x)\cdot Q(x) = a \cdot R(x)$, con $R(x) \in A[x]$ y $a \in A$ no invertible. Sea $p \in A$ irreducible que divida a a. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que

$$\overline{P(x)} \cdot \overline{Q(x)} = 0 \in (A/pA)[x]$$

lo cual es contradictorio, porque $(A/pA)[x]$ es íntegro y $\overline{P(x)}$ y $\overline{Q(x)}$ son no nulos.

2. Sea p un elemento irreducible que divida a a. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que $0 = \bar{b} \cdot \overline{Q(x)}$, luego $\bar{b} = 0$ y p divide a b. Dividiendo a a y b a la vez por p y repitiendo sucesivamente este proceso obtendremos que a divide a b, y por simetría que b divide a a. Luego, $b = a \cdot u$, para cierto invertible $u \in A$. □

25. Lema de Gauss: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio primitivo, $P(x) \in A[x]$, es irreducible en $A[x]$ si y solo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $P(x)$ es irreducible en $\Sigma[x]$. Si $P(x) = P_1(x)\cdot P_2(x)$, con $P_1(x), P_2(x) \in A[x]$, entonces como $P(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $P_1(x)$ o $P_2(x)$ ha de ser de grado cero, digamos $P_1(x) = a$. Como $P(x)$ es primitivo $P_1(x) = a \in A$ es invertible. En conclusión, $P(x)$, es irreducible en $A[x]$.

Supongamos que $P(x)$ es irreducible en $A[X]$. Supongamos que $P(x) = \tilde{P}_1(x) \cdot \tilde{P}_2(x)$, siendo $\tilde{P}_1(x)$ y $\tilde{P}_2(x)$ dos polinomios de $\Sigma[x]$. Eliminando denominadores y sacando el máximo común divisor en los numeradores, podemos suponer que

$$P(x) = \frac{a}{b} P_1(x) \cdot P_2(x)$$

con $P_1(x), P_2(x) \in A[x]$, primitivos. Por el lema 0.3.24, $\frac{a}{b} = u \in A$, luego $P(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

26. Teorema: *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

Demostración. Sea $\Sigma = A_{A\setminus\{0\}}$ el cuerpo de fracciones. Sea $P(x) \in A[x]$ y escribamos $P(x) = a \cdot Q(x)$, con $a \in A$ y $Q(x) \in A[x]$ primitivo. Sea

$$Q(x) = \widetilde{Q}_1(x) \cdots \widetilde{Q}_r(x)$$

la descomposición en irreducibles en $\Sigma[x]$. Eliminando denominadores y sacando el máximo común divisor en los numeradores, es claro que se puede escribir $\widetilde{Q}_i(x) = \frac{a_i}{b_i} \cdot Q_i(x)$ con $Q_i(x) \in A[x]$ primitivos. Luego,

$$Q(x) = \frac{b}{c} \cdot Q_1(x) \cdots Q_r(x) \qquad (*)$$

- Por el lema 0.3.24, $\frac{b}{c} = u \in A$ es un invertible de A.
- Cada $Q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por el lema de Gauss 0.3.25.

Descomponiendo $a = p_1 \cdots p_s$ en producto de irreducibles en A, se obtiene una descomposición de

$$P(x) = a \cdot Q(x) = u \cdot p_1 \cdots p_s Q_1(x) \cdots Q_r(x)$$

en $A[x]$.

Unicidad: Si $P(x) = q_1 \cdots q_l P_1(x) \cdots P_t(x)$, entonces cada $P_i(x)$ es irreducible en $\Sigma[x]$ por el lema de Gauss 0.3.25. Por tanto, los polinomios $P_i(x)$ (una vez reordenados) difieren de los $Q_i(x)$ en invertibles de A. Tachando los términos polinómicos comunes se obtiene salvo unidades la igualdad $q_1 \cdots q_l = p_1 \cdots p_s$, de donde salvo permutación de los factores es $q_i = p_i$ (salvo invertibles de A).

□

Como corolario se obtiene el siguiente teorema.

27. Teorema: *Los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ y $k[x_1, \ldots, x_n]$ (k un cuerpo) son dominios de factorización única.*

0.3.4. Factorización en $\mathbb{Q}[x_1,\ldots,x_n]$

El anillo de polinomios $k[x]$ es un anillo euclídeo, luego es un dominio de factorización única. Un polinomio no nulo $p(x)\in k[x]$ es invertible si y solo si es de grado cero. Si $p(x)=ax+b$ es de grado 1 entonces es irreducible, además $p(\frac{-b}{a})=0$ y $p(x)=a\cdot(x-\frac{-b}{a})$.

28. Definición: Sea $p(x)\in k[x]$ un polinomio y $\alpha\in k$. Se dice que α es una raíz de $p(x)$ si $p(\alpha)=0$.

29. Proposición: *Sea $p(x)\in k[x]$ un polinomio y $\alpha\in k$. Entonces, α es una raíz de $p(x)$ si y solo si $p(x)$ es múltiplo de $x-\alpha$.*

Demostración. Por el algoritmo de Euclides, existen $c(x)\in k[x]$ y $\lambda\in k$, tales que $p(x)=c(x)(x-\alpha)+\lambda$. Si α es una raíz de $p(x)$ entonces $0=p(\alpha)=\lambda$ y $p(x)$ es múltiplo de $x-\alpha$. El recíproco es obvio. □

La siguiente proposición nos muestra cómo calcular las raíces racionales de un polinomio con coeficientes racionales.

30. Proposición: *Sea $p(x)=\sum_{i=0}^{n}a_ix^{n-i}\in\mathbb{Z}[x]$ un polinomio con coeficientes enteros. Sea $q=\frac{r}{s}\in\mathbb{Q}$ una fracción irreducible (r y s son números enteros primos entre sí). Si q es una raíz de $p(x)$, entonces r divide a a_n y s a a_0*

Demostración. Tenemos que $0=p(\frac{r}{s})=(\frac{r}{s})^na_0+(\frac{r}{s})^{n-1}a_1+\cdots+a_n$ y multiplicando por s^n, $0=r^na_0+r^{n-1}sa_1+\cdots+s^na_n$. Por tanto, s^na_n es múltiplo de r y r^na_0 es múltiplo de s. Luego, a_n es múltiplo de r y a_0 es múltiplo de s. □

31. Lema: *Si $p(x)\in k[x]$ es un polinomio de grado n, entonces existen a lo más n raíces distintas de $p(x)$ en k.*

Demostración. Si $\alpha_1,\ldots,\alpha_r$ son raíces distintas de $p(x)$, entonces $(x-\alpha_1)\cdots(x-\alpha_r)$ divide a $p(x)$, luego $r\leq \mathrm{gr}(p(x))$.

□

32. Fórmula de interpolación de Lagrange: *Dados $\alpha_0,\ldots,\alpha_n\in k$ distintos entre sí y $\beta_0,\ldots,\beta_n\in k$ existe un único polinomio $p(x)$ de grado menor o igual que n tal que $p(\alpha_i)=\beta_i$, para todo i. Además,*

$$p(x)=\sum_{i=0}^{n}\beta_i\cdot\frac{(x-\alpha_0)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)\cdots\widehat{(\alpha_i-\alpha_i)}\cdots(\alpha_i-\alpha_n)}.$$

Diremos que $p(x)$ es el polinomio de interpolación de $\alpha_0,\ldots,\alpha_n$ con valores $\beta_0,\ldots,\beta_n$.

Demostración. $p(x)$ es de grado menor o igual que n y $p(\alpha_i) = \beta_i$, para todo i.

Si $q(x)$ fuese otro polinomio tal que $q(\alpha_i) = \beta_i$ para todo i, entonces $p(x) - q(x)$ sería un polinomio de grado menor o igual que n con $n+1$ raíces:$\alpha_0, \ldots, \alpha_n$. Por tanto, $p(x) - q(x) = 0$ y $q(x) = p(x)$. □

33. Descomposición de un polinomio con coeficientes racionales en producto de polinomios irreducibles:

1. Dado $p(x) \in \mathbb{Q}[x]$, escribamos $p(x) = m \cdot q(x)$, con $m \in \mathbb{Q}$ y $q(x) \in \mathbb{Z}[x]$ primitivo. Para descomponer $p(x)$ en factores irreducibles basta descomponer $q(x)$ en factores irreducibles en $\mathbb{Z}[x]$.

2. Calculemos los polinomios $q_n(x) \in \mathbb{Z}[x]$, con $n = \operatorname{gr} q_n(x) \leq \operatorname{gr} q(x))/2$ que dividen a $q(x)$: Todo polinomio de grado n, $r(x)$, coincide con el polinomio de interpolación de $0, 1, \ldots, n$ con valores $r(0), \ldots, r(n)$. Si $q(x) = q_n(x) \cdot q'(x)$, entonces $q_n(i)$ divide a $q(i)$. Observemos que solo hay un número finito de enteros que dividen al entero $q(i)$. Sea $Y = \{(\beta_0, \ldots, \beta_n) \in \mathbb{Z}^{n+1} \colon \ \beta_i$ divide a $q(i)$, para todo $i\}$, y para cada $y = (\beta_0, \ldots, \beta_n) \in Y$ sea $q_y(x)$ el polinomio de interpolación de $0, 1, \ldots, n$ con valores $\beta_0, \ldots, \beta_n$. $Y' = \{q_y(x) \colon y \in Y$ y $q_y(x)$ divide a $q(x)\}$ es el conjunto buscado que sabemos calcular.

34. Descomposición de un polinomio $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ en producto de factores irreducibles. Procedemos por inducción sobre n. Caso $n = 1$ lo acabamos de resolver. Supongamos resuelta la cuestión hasta $n-1$. Se procede igual que en el caso $n = 1$, sustituyendo $\mathbb{Z}$ por $\mathbb{Z}[x_1, \ldots, x_{n-1}]$ y $\mathbb{Z}[x]$ por $\mathbb{Z}[x_1, \ldots, x_n]$.

35. Descomposición de un polinomio con coeficientes en $\mathbb{Q}[x_1, \ldots, x_n]$ en factores irreducibles. Por el lema de Gauss, se reduce al problema de descomponer un polinomio en $\mathbb{Z}[x_1, \ldots, x_n]$ en producto de factores irreducibles.

0.3.5. Algunos criterios de irreducibilidad de polinomios

36. Proposición: *Sean A y B anillos íntegros, $p(x) = \sum_{i=0}^{n} a_i \cdot x^{n-i} \in A[x]$ un polinomio primitivo y $f : A \to B$ un morfismo de anillos. Si $f(a_0) \neq 0$ y $q(x) = \sum_{i=0}^{n} f(a_i) \cdot x^{n-i} \in B[x]$ es irreducible, entonces $p(x)$ es irreducible.*

Demostración. La aplicación $F \colon A[x] \to B[x]$, $F(\sum_i c_i x^i) := \sum_i f(c_i) x^i$ es un morfismo de anillos. Supongamos que $p(x) = p_1(x) \cdot p_2(x)$. Entonces,

$$q(x) = F(p(x)) = F(p_1(x)) \cdot F(p_2(x)).$$

Como $q(x)$ tiene grado n y es irreducible, entonces podemos decir que $F(p_1(x))$ es de grado cero y $F(p_2(x))$ es de grado n. Por tanto, $p_1(x)$ tiene grado cero y $p_2(x)$ tiene grado n. Como $p(x)$ es primitivo, $p_1(x)$ es un invertible de A. En conclusión, $p(x)$ es irreducible.

□

37. Ejercicio: Calcula todos los polinomios de grado dos irreducibles de $\mathbb{Z}/2\mathbb{Z}[x]$. Demuestra que $x^4+x^3+x^2+x+1 \in \mathbb{Q}[x]$ es irreducible.

38. Criterio de Eisenstein: *Sea A un dominio de factorización única, $p \in A$ irreducible y $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$ un polinomio. Si se cumple que*

1. *$p(x)$ es primitivo,*
2. *$a_1, \ldots, a_n$ son múltiplos de p*
3. *a_n no es múltiplo de p^2.*

entonces $p(x)$ es irreducible.

Demostración. Si $p(x) = c(x) \cdot d(x)$ es una descomposición propia, entonces por ser $p(x)$ primitivo es $n > gr\, c(x), gr\, d(x) > 0$. Sean $\overline{p(x)}, \overline{c(x)}, \overline{d(x)} \in (A/(p))[x]$ las clases de $p(x), c(x)$ y $d(x)$ módulo p. Por 2., es $\overline{p(x)} = \overline{a}_0x^n$. Por tanto (ejercicio), $\overline{c(x)} = \overline{c}_{n-i}x^i$ y $\overline{d(x)} = \overline{d}_ix^{n-i}$ (con $n > n-i$ y $n > i$, es decir, $i, n-i > 0$). En particular, los términos independientes de $c(x), d(x)$ son múltiplos de p y, por tanto, el de $p(x)$ es múltiplo de p^2, lo que contradice 3.

□

39. Ejercicio: Prueba que $x^n - 2 \in \mathbb{Q}[x]$ es un polinomio irreducible, para todo $n > 0$.

0.4. Extensiones de cuerpos

0.4.1. Teorema de Kronecker

1. Definición: Dado un morfismo de anillos entre cuerpos $k \to K$, diremos que K es una extensión (de cuerpos) de k.

En todo cuerpo k no hay más ideales que el ideal $\{0\}$ y todo k. Por tanto, todo morfismo de anillos $k \to K$ entre cuerpos (con $K \neq \{0\}$) es inyectivo. Dado un morfismo de cuerpos $k \to K$, escribiremos habitualmente $\lambda \mapsto \lambda$. Dada extensión de cuerpos $k \hookrightarrow K$, tenemos el morfismo obvio $k[x] \hookrightarrow K[x]$, $\sum_i \lambda_i x^i \mapsto \sum_i \lambda_i x^i$, es decir, todo polinomio con coeficientes en k es obviamente un polinomio con coeficientes en K.

2. Teorema de Kronecker: *Sea $p(x) \in k[x]$ un polinomio de grado $n > 0$. Existe una extensión de cuerpos K de k en la que $p(x)$ descompone en factores simples, es decir, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que*

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n), \qquad \lambda \in k.$$

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x - \alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K_1 = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K_1[x]$ tenemos que $p(x) = (x - \alpha_1) \cdot p_2(x)$. Por hipótesis de inducción, existe una extensión $K_1 \hookrightarrow K$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Luego en K, que es una extensión de k,

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

□

3. Dadas dos k-extensiones de cuerpos K y K', puede probarse que existe una extensión de cuerpos de k, L, que contiene a K y K': Consideremos el epimorfismo de k-álgebras $\pi\colon k[x_k]_{\{k \in K\}} \to K$, $x_k \mapsto k$. Luego $K = k[x_k]_{\{k \in K\}}/\mathrm{Ker}\,\pi$. Igualmente, consideremos el epimorfismo de k-álgebras $\pi'\colon k[y_{k'}]_{\{k' \in K'\}} \to K'$, $y_{k'} \mapsto k'$. Luego $K' = k[y_{k'}]_{\{k' \in K'\}}/\mathrm{Ker}\,\pi'$. Sea $B = k[x_k, y_{k'}]_{\{k \in K, k' \in K'\}}/(\mathrm{Ker}\,\pi, \mathrm{Ker}\,\pi')$. Tenemos los morfismos de anillos obvios $K \hookrightarrow B$ y $K' \hookrightarrow$. Sea $\mathfrak{m} \subset B$ un ideal maximal y $L = B/\mathfrak{m}$. Por paso al cociente, tenemos los morfismos $K \hookrightarrow L$ y $K' \hookrightarrow L$ buscados.

Por tanto, si K y K' son dos k-extensiones de cuerpos que contienen todas las raíces de $p(x)$ y consideramos una k-extensión L que contenga a K y K', entonces las raíces de $p(x)$ en K y K' han de coincidir en L.

El teorema fundamental del Álgebra, que probaremos más adelante, afirma que para todo polinomio $p(x) = a_0 x^n + \cdots + a_n \in \mathbb{C}[x]$ (con $a_0 \neq 0$ y $n > 0$) existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ de modo que

$$p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

4. Definición: Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Se dice que $\alpha \in k$ es una raíz múltiple de $p(x)$ si $p(x)$ es múltiplo de $(x - \alpha)^2$. Se dice que $r > 0$ es la multiplicidad de una raíz de $p(x)$ si $p(x) = (x - \alpha)^r \cdot q(x)$, con $q(\alpha) \neq 0$.

Si $\alpha_1, \ldots, \alpha_s$ son raíces distintas de $p(x)$ con multiplicidad $n_1, \ldots, n_s$ respectivamente, entonces $p(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_s)^{n_s} \cdot q(x)$, con $q(\alpha_i) \neq 0$ para todo i.

5. Proposición: *Sea $p(x) \in k[x]$ un polinomio. Entonces, $\alpha \in k$ es una raíz múltiple de $p(x)$ si y solo si es raíz de $p(x)$ y $p'(x)$ (la derivada "formal" de $p(x)$).*

Demostración. Tenemos que α es una raíz de $p(x)$, entonces $p(x) = (x-\alpha)\cdot q(x)$ y $p'(x) = q(x) + (x-\alpha)\cdot q'(x)$. Por tanto, α es una raíz de $p'(x)$ si y solo si es raíz de $q(x)$, es decir, si y solo si α es una raíz múltiple de $p(x)$. □

Sea $k \hookrightarrow K$ una extensión de cuerpos y $p(x) \in k[x]$. Se dice que $\alpha \in K$ es raíz de $p(x)$ si $p(\alpha) = 0$. Igualmente, diremos que $\alpha \in K$ es una raíz de multiplicidad r si es una raíz de multiplicidad r de $p(x) \in K[x]$. Si $\alpha \in k$, la multiplicidad de $p(x)$ en α no varía si consideramos $\alpha \in k$ o $\alpha \in K$.

6. Proposición: *Sean $p(x), q(x) \in k[x]$ dos polinomios y $k \hookrightarrow K$ una extensión de cuerpos. El máximo común divisor de $p(x)$ y $q(x)$ en $k[x]$ coincide con el máximo común divisor de $p(x)$ y $q(x)$ en $K[x]$.*

Demostración. El máximo común divisor de dos polinomios $p(x)$ y $q(x)$ se puede calcular por el algoritmo de Euclides, cálculo que es el mismo si consideramos que estamos en $k[x]$ o si consideramos que estamos en $K[x]$.

□

7. Proposición: *Sean $p(x), q(x) \in k[x]$ dos polinomios y K una extensión de cuerpos de k donde estén todas las raíces de $p(x)$ y $q(x)$. Escribamos en $K[x]$*

$$p(x) = a_0 \cdot (x-\alpha_1)^{n_1} \cdots (x-\alpha_r)^{n_r}$$
$$q(x) = b_0 \cdot (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}$$

con $\alpha_1, \ldots, \alpha_r \in K$ y $n_i, m_i \geq 0$, para todo i. Entonces,

$$m.c.d.(p(x), q(x)) = (x-\alpha_1)^{\min\{n_1,m_1\}} \cdots (x-\alpha_r)^{\min\{n_r,m_r\}}$$

Además, $p(x)$ y $q(x)$ son primos entre sí si y solo si no tienen raíces comunes (en K).

8. Sea K un cuerpo, $k \subseteq K$ un subcuerpo, y sea $\alpha \in K$. Se denota $k[\alpha] := \{p(\alpha) \in K$, para todo $p(x) \in k[x]\}$. Consideremos el morfismo $\phi\colon k[x] \to K$, $\phi(p(x)) := p(\alpha)$. Se cumple que ϕ es un morfismo de anillos y $\operatorname{Im}\phi = k[\alpha]$. $\operatorname{Ker}\phi$ es un ideal de $k[x]$. Si $\operatorname{Ker}\phi \neq \{0\}$, entonces está generado por el polinomio $p(x)$ no nulo mónico[2] de grado más pequeño tal que $p(\alpha) = 0$. Por tanto, por el teorema de isomorfía

$$k[\alpha] = \begin{cases} k[x], & \text{si no existe ningún polinomio no nulo } p(x) \text{ tal que } p(\alpha) = 0. \\ k[x]/(p(x)), & \text{donde } p(x) \in k[x] \text{ es el pol. no nulo mónico mín. anulador de } \alpha. \end{cases}$$

Observemos que el polinomio mínimo anulador de α, $p(x)$, es irreducible (es decir, no es producto de dos polinomios de grado menor que el de $p(x)$), porque si no lo es

[2] Se dice que un polinomio $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ de grado n es mónico si $a_0 = 1$.

entonces $p(x) = p_1(x) \cdot p_2(x)$, con $\mathrm{gr}(p_1(x)), \mathrm{gr}(p_2(x)) < \mathrm{gr}(p(x))$ y $p_1(x)$ ó $p_2(x)$ anula a α. Recíprocamente, si $p(x)$ es mónico, anula a α y es irreducible, entonces es el polinomio mónico mínimo anulador de α.

$k[x]/(p(x))$ es un k-espacio vectorial de base $\{\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}\}$, con $n = \mathrm{gr}(p(x))$: En efecto dado $\overline{q(x)} \in k[x]/(p(x))$, como $q(x) = c(x) \cdot p(x) + r(x)$, con $\mathrm{gr}(r(x)) < n$, tenemos que $\overline{q(x)} = \overline{r(x)}$. Como $r(x)$ es combinación lineal de $1, \cdots, x^{n-1}$, $\{\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}\}$ es un sistema generador. Veamos que $\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}$ son linealmente independientes. Si

$$0 = \sum_{i=0}^{n-1} \lambda_i \bar{x}^i = \overline{\sum_{i=0}^{n-1} \lambda_i x^i}.$$

Entonces, $\sum_{i=0}^{n-1} \lambda_i x^i$ es múltiplo de $p(x)$, lo cual es imposible, salvo que $\sum_{i=0}^{n-1} \lambda_i x^i = 0$, es decir, $\lambda_i = 0$ para todo i.

Consideremos la inclusión $\mathbb{Q} \subset \mathbb{C}$ y $\sqrt[3]{2} \in \mathbb{C}$. El polinomio con coeficientes racionales mínimo anulador de $\sqrt[3]{2}$ es $x^3 - 2$, porque es irreducible ya que si no lo es $x^3 - 2$ tendría raíces en $\mathbb{Q}$, que es imposible. Por tanto,

$$\mathbb{Q}[x]/(x^3 - 2) = \mathbb{Q}[\sqrt[3]{2}].$$

Por tanto, $\mathbb{Q}[\sqrt[3]{2}]$ es un $\mathbb{Q}$-espacio vectorial de dimensión 3, de base $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$.

0.4.2. Operador de Euler. Polinomios ciclotómicos

Por la proposición 0.1.29, un elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es un generador del grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ si y solo m es primo con n. Así pues, si $G = \langle g \rangle$ es un grupo cíclico de orden $n > 0$, entonces g^m es un generador de G si y solo si m y n son primos entre sí.

9. Proposición: *$\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ si y solo si m es primo con n.*

Demostración. Un elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es invertible si y solo si existe $\bar{m}' \in \mathbb{Z}/n\mathbb{Z}$ tal que $\bar{m}' \cdot \bar{m} = \bar{1}$, para esto es necesario y suficiente que exista m' tal que $m' \cdot \bar{m} = \bar{1}$, o equivalentemente, $\mathbb{Z} \cdot \bar{m} = \mathbb{Z}/n\mathbb{Z}$. Es decir, $\bar{m}$ es un invertible de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $\bar{m}$ genera el grupo aditivo $\mathbb{Z}/n\mathbb{Z}$. Por 0.1.29, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es invertible si y solo si m es primo con n.

□

De estas proposiciones obtendremos la congruencia de Euler.

10. Definición: Sea $\phi \colon \mathbb{N}^* \to \mathbb{N}$ la aplicación definida por

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

A la aplicación ϕ la denominaremos operador de Euler.

Es decir, $\phi(n) = |$Conjunto de los números naturales inferiores a n y primos con él$|$.

11. Congruencia de Euler: *Si n, m son números naturales primos entre sí, entonces*

$$m^{\phi(n)} \equiv 1 \, mod \, n.$$

Demostración. Es consecuencia de 0.1.27, aplicado al caso $G = (\mathbb{Z}/n\mathbb{Z})^*$ y $g = \bar{m}$. □

Calculemos $\phi(n)$.

12. Proposición: *Si n, m son números naturales primos entre sí, entonces*

$$\phi(nm) = \phi(n)\phi(m).$$

Demostración. Por el teorema chino de los restos tenemos el isomorfismo de anillos $\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Tomando los invertibles de los anillos

$$\boxed{(\mathbb{Z}/nm\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*}$$

luego $\phi(nm) = |(\mathbb{Z}/nm\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*| \cdot |(\mathbb{Z}/m\mathbb{Z})^*| = \phi(n)\phi(m)$. □

13. Proposición: *Si p es un número natural primo, entonces:*

$$\phi(p^n) = p^{n-1}(p-1).$$

Demostración. Un número r es primo con p^n si y solo si es primo con p. Obviamente $1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p$ son los números naturales m, con $0 < m \leq p^n$, que no son primos con p^n. Luego, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

14. Teorema: *Si $n = p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de $n \in \mathbb{N}$ en producto de potencias de números naturales primos, entonces:*

$$\phi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1 - 1) \cdots (p_r - 1).$$

15. Proposición: *Si G es un grupo cíclico finito de orden n, entonces para cada divisor d de n existe un único subgrupo $H \subseteq G$ de orden d.*

Demostración. Podemos suponer que $G = \mathbb{Z}/n\mathbb{Z}$. Cada subgrupo de $H \subset G$ es cíclico. Luego, $H = \langle \bar{m} \rangle$ (donde $0 \leq m < n$). El orden d de H, que es el de $\bar{m}$, divide al orden de G, que es n. Luego $m' := \frac{n}{d} \in \mathbb{N}$ y $d \cdot \bar{m} = \bar{0}$, es decir, $d \cdot m = r \cdot n$, para cierto $r > 0$, y $m = r \cdot m'$. Por tanto, $H \subseteq \langle \bar{m'} \rangle$. Como el subgrupo de G generado por $\bar{m'}$ es de orden d, $H = \langle \bar{m'} \rangle$. □

16. Proposición: *Se cumple la fórmula:*

$$n = \sum_{d|n} \phi(d)$$

Demostración. $\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} X_d$, siendo $X_d \subset \mathbb{Z}/n\mathbb{Z}$ los elementos de orden d. Por ser $\mathbb{Z}/n\mathbb{Z}$ cíclico, para cada $d|n$ existe un único subgrupo H de orden d (que además es cíclico), luego todo elemento de orden d genera H y recíprocamente, es decir, X_d son los generadores de $H \approx \mathbb{Z}/d\mathbb{Z}$. De aquí que $n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d|n} |X_d| = \sum_{d|n} \phi(d)$.

□

17. Proposición: *Un grupo finito es cíclico si y solo si para cada divisor d de su orden admite como mucho un subgrupo de orden d.*

Demostración. El directo ya está probado (proposición 0.4.15).

Recíproco: sea G verificando la hipótesis. Como en la demostración anterior escribamos $G = \coprod_{d|n} G_d$, siendo $G_d \subset G$ los elementos de orden d. Si existe un elemento de orden d, entonces el grupo generado H es el único de dicho orden, luego G_d es el conjunto de generadores de H y, por tanto, $|G_d| = \phi(d)$. Por tanto, $|G_d| = 0, \phi(d)$. Pero como $\sum_{d|n} \phi(d) = n = |G| = \sum_{d|n} |G_d|$, se concluye que para cada divisor de d es $|G_d| = \phi(d) \neq 0$. En particular, $G_n \neq \emptyset$, es decir, G admite un generador y por tanto es cíclico. □

18. Definición: Sea k un cuerpo. Se dice que $\alpha \in k$ es una raíz n-ésima de la unidad si $\alpha^n = 1$. Se dice que α es una raíz n-ésima primitiva de la unidad si $\alpha^n = 1$ y $\alpha^m \neq 1$, para todo $0 < m < n$.

Sea α una raíz n-ésima de la unidad y $r = \text{ord}(\alpha)$ el mínimo número natural (no nulo) tal que $\alpha^r = 1$, entonces el grupo (multiplicativo) generado por α es $\langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ y tiene orden r. Si $x^n - 1$ no tiene raíces múltiples (es decir, $n \neq 0$ en k), α es una raíz primitiva de la unidad si y sólo si $\langle\alpha\rangle$ es el grupo de todas las raíces n-ésimas de la unidad.

Consideremos ahora $k = \mathbb{C}$. Observemos que

$$\mu_n := \{e^{k \cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i\,sen\,\frac{2k\pi}{n} \in \mathbb{C},\ 0 \leq k < n\},$$

es el conjunto de todas las raíces n-ésimas de la unidad, que es un subgrupo (multiplicativo) de $\mathbb{C}^*$, de orden n. El morfismo

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n,\ \ \bar{m} \mapsto e^{m \cdot 2\pi i/n}$$

es un isomorfismo de grupos. Vía este isomorfismo, el conjunto de generadores $\mathbb{Z}/n\mathbb{Z}$ se identifica con el conjunto $R_n \subset \mu$, de todas las raíces n-ésimas primitivas de la unidad ($R_n = \{\varepsilon \in \mu_n$ tales que $\varepsilon^m \neq 1$ para cada $m < n\}$). El conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con los invertibles de $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z}, (k,n) = (1)\}$. Luego,

$$R_n = \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i\,sen\,\frac{2k\pi}{n},\ \text{con}\ \ 0 < k < n \text{ y } (k,n) = (1)\}.$$

19. Definición: Para cada $n \in \mathbb{N}$ se denomina n-ésimo *polinomio ciclotómico* al polinomio mónico

$$\Phi_n(x) = \prod_{k<n,(k,n)=(1)} (x - e^{k\cdot 2\pi i/n}).$$

Se cumple $\xi \in \mathbb{C}$ es una raíz n-ésima de la unidad si y solo si ξ es una raíz primitiva d-ésima de la unidad para algún $d|n$. Por tanto,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Luego,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n,\,d|n} \Phi_d(x)}.$$

Por recurrencia se demuestra que $\Phi_n(x) \in \mathbb{Z}[x]$ (obsérvese que $\Phi_1(x) = x - 1$).

Dejamos que el lector pruebe la siguiente proposición.

20. Proposición: *Se cumple*

1. $\Phi_1(x) = x - 1$.
2. $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = x + 1$.
3. $\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = x^2 + x + 1$.
4. $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\cdot\Phi_2(x)} = x^2 + 1$.
5. $\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$.
6. $\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_3(x)} = x^2 - x + 1$.
7. *Si* $p > 0$ *es primo,* $\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = x^{p-1} + x^{p-2} + \cdots + x + 1$.

8. *Si $p>0$ es primo, $\Phi_{p^n}(x)=\Phi_p(x^{p^{n-1}})=x^{p^{n-1}(p-1)}+x^{p^{n-1}(p-2)}+\cdots+x^{p^{n-1}}+1$. También, $\Phi_{p^n}(x)=\frac{x^{p^n}-1}{x^{p^{n-1}}-1}$.*

9. *Si $p>0$ es primo y r no es divisible por p, $\Phi_{r\cdot p^n}(x)=\frac{\Phi_r(x^{p^n})}{\Phi_r(x^{p^{n-1}})}$: Las raíces de $\Phi_r(x^{p^n})$ son aquellas $\alpha\in\mathbb{C}$ tales que $\operatorname{ord}(\alpha^{p^n})=r$, es decir, aquellas $\alpha\in\mathbb{C}$ tales que $\operatorname{ord}(\alpha)=r\cdot p^i$, con $i\leq n$. Por tanto,*

$$\begin{aligned}\{\textit{Raíces de } \Phi_r(x^{p^n})\}\setminus\{\textit{Raíces de } \Phi_r(x^{p^{n-1}})\} &= \{\alpha\in\mathbb{C}\colon \operatorname{ord}(\alpha)=r\cdot p^n\}\\ &= \{\textit{Raíces de } \Phi_{r\cdot p^n}(x)\}\end{aligned}$$

y hemos terminado.

10. *Si r es impar, $\Phi_{2r}(x)=\pm\Phi_r(-x)$: Si $\operatorname{ord}(\alpha)=2r$ entonces $\alpha^r=-1$, luego $(-\alpha)^r=1$ y $\operatorname{ord}(-\alpha)=r$. Por tanto, las raíces de $\Phi_{2r}(x)$ son raíces de $\Phi_r(-x)$ y como $\operatorname{gr}(\Phi_{2r}(x))=\phi(2r)=\phi(2)\phi(r)=\phi(r)=\operatorname{gr}\Phi_r(-x)$ hemos terminado.*

21. Lema: *Sea $p\in\mathbb{N}$ un número primo. Para todo $q(x)\in\mathbb{Z}/p\mathbb{Z}[x]$ se cumple que*

$$q(x)^p=q(x^p).$$

Demostración. Para cada $a\in\mathbb{Z}/p\mathbb{Z}$ es $a^p=a$ y $(r(x)+s(x))^p=r(x)^p+s(x)^p$, para cada $r(x),s(x)\in\mathbb{Z}/p\mathbb{Z}[x]$, luego

$$q(x)^p=(a_0+a_1x+\cdots a_nx^n)^p=a_0^p+a_1^px^p+\cdots a_n^p(x^p)^n=q(x^p).$$

□

22. Teorema: *Los polinomios ciclotómicos $\Phi_n(x)\in\mathbb{Z}[x]$ son polinomios irreducibles.*

Demostración. Supongamos que $\Phi_n(x)=p(x)\cdot q(x)$. Sea p un número primo que no divida a n. Veamos que si ε es raíz de $p(x)$ entonces ε^p es también raíz de $p(x)$: Observemos que ε^p es una raíz n-ésima primitiva de la unidad, luego es raíz de $\Phi_n(x)$. Si ε^p es raíz de $q(x)$, entonces, los polinomios $p(x)$ y $q(x^p)$ tienen la raíz ε en común, luego no son primos entre sí. Entonces, en $\mathbb{Z}/p\mathbb{Z}[x]$, $\overline{p(x)}$ y $\overline{q(x^p)}=\overline{q(x)}^p$ no son primos entre sí. Por tanto, $\overline{p(x)}$ y $\overline{q(x)}$ no son primos entre sí, y $\overline{\Phi_n(x)}=\overline{p(x)}\cdot\overline{q(x)}$ tiene raíces múltiples. Entonces, $x^n-\bar{1}\in\mathbb{Z}/p\mathbb{Z}[x]$ tiene raíces múltiples. Pero, $x^n-\bar{1}$ es primo con su derivada $\bar{n}\cdot x^{n-1}$ (donde $\bar{n}\neq 0$, porque p no divide a n), lo que implica que no tiene raíces múltiples. Hemos llegado a contradicción, luego ε^p no es raíz de $q(x)$ y ha de ser raíz de $p(x)$.

Sin pérdida de generalidad, podemos suponer que $e^{\frac{2\pi i}{n}}$ es raíz de $p(x)$. Sea $e^{\frac{2m\pi i}{n}}$ una raíz primitiva de la unidad, luego m es primo con n y $m = p_1 \cdots p_r$, donde los primos p_i no dividen a n. Por el párrafo anterior, $e^{\frac{2p_1\pi i}{n}}$ es raíz de $p(x)$, luego $e^{\frac{2p_1p_2\pi i}{n}}$ es raíz de $p(x)$ y así sucesivamente obtenemos que $e^{\frac{2m\pi i}{n}}$ es raíz de $p(x)$. En conclusión, $\Phi_n(x) = p(x)$.

□

23. Proposición: $\mathbb{Q}[e^{\frac{2\pi i}{n}}] \simeq \mathbb{Q}[x]/(\Phi_n(x))$.

Demostración. El polinomio mónico con coeficientes en $\mathbb{Q}$ mínimo anulador de $e^{\frac{2\pi i}{n}}$ es $\Phi_n(x)$, por el teorema 0.4.22 y el lema 0.3.25. Luego, $\mathbb{Q}[e^{\frac{2\pi i}{n}}] \simeq \mathbb{Q}[x]/(\Phi_n(x))$. □

0.4.3. Cierre algebraico

24. Definición: Dado un morfismo de anillos $f: A \to B$, se dice que B es una A-álgebra. Dadas dos A-álgebras $f: A \to B$ y $g: A \to C$, se dice que un morfismo de anillos $h: B \to C$ es un morfismo de A-álgebras si $h(f(a)) = g(a)$, para toda $a \in A$.

25. Notación: Dada un morfismo de anillos $f: A \to B$, en el contexto de A-álgebras, suele ser habitual denotar $f(a) = a$.

El conjunto de morfismos de A-álgebras de una A-álgebra B en otra C, se denotará $\mathrm{Hom}_{A-alg}(B, C)$.

26. Ejemplo: $A[x_1, \ldots, x_n]$ es de modo obvio una A-álgebra y si B es una A-álgebra, entonces tenemos la biyección

$$\mathrm{Hom}_{A-alg}(A[x_1, \ldots, x_n], B) = B^n,\ f \mapsto (f(x_1), \ldots, f(x_n))$$

27. Definición: Una extensión de cuerpos es un morfismo de anillos $k \to K$, donde k y K son cuerpos. También se dice que K es una extensión de cuerpos de k o que K es una k-extensión de cuerpos.

Obsérvese que todo morfismo de anillos $k \to K$, entre cuerpos, es inyectivo pues el núcleo es un ideal, que ha de ser el ideal (0) y no el ideal $k = (1)$, porque el elemento unidad de k se aplica en el elemento unidad de K (suponemos $K \neq 0$).

28. Definición: Diremos que una extensión de cuerpos $k \hookrightarrow K$ es una extensión finita de cuerpos si K es un k-espacio vectorial de dimensión finita. Llamaremos grado de K sobre k a $\dim_k K$.

29. Ejemplo: La inclusión $\mathbb{R} \subset \mathbb{C}$ es una extensión finita de cuerpos de grado 2.

Sea $k \hookrightarrow K$ una extensión de cuerpos. Dados $\alpha_1, \ldots, \alpha_n \in K$, definimos

$$k[\alpha_1, \ldots, \alpha_n] := \{p(\alpha) \in K : p(x) \in k[x_1, \ldots, x_n]\}.$$
$$k(\alpha_1, \ldots, \alpha_n) := \{\tfrac{p(\alpha)}{q(\alpha)} \in K : p(x), q(x) \in k[x_1, \ldots, x_n] \text{ y } q(\alpha) \neq 0\}.$$

$k[\alpha_1, \ldots, \alpha_n]$ es una k-álgebra íntegra y $k(\alpha_1, \ldots, \alpha_n)$ es una k-extensión de cuerpos. Si $\dim_k k[\alpha_1, \ldots, \alpha_n] < \infty$ entonces es un cuerpo: Dado $p(\alpha) \in k[\alpha_1, \ldots, \alpha_n]$, la aplicación k-lineal $k[\alpha_1, \ldots, \alpha_n] \to k[\alpha_1, \ldots, \alpha_n]$, $q(\alpha) \mapsto q(\alpha) \cdot p(\alpha)$ es inyectiva, luego epiyectiva por dimensiones. Luego, existe $q(\alpha)$ tal que $q(\alpha) \cdot p(\alpha) = 1$. En este caso, $k[\alpha_1, \ldots, \alpha_n] = k(\alpha_1, \ldots, \alpha_n)$.

30. Definición: Dado una extensión de cuerpos $k \hookrightarrow K$. Diremos que $\alpha \in K$ es algebraica sobre k si existe un polinomio $0 \neq p(x) \in k[x]$ tal que $p(\alpha) = 0$. En caso contrario diremos que α es trascendente sobre k.

31. Ejemplos: $\sqrt{2} \in \mathbb{R}$ es un elemento $\mathbb{Q}$-algebraico, porque es raíz de $x^2 - 2 \in \mathbb{Q}[x]$. El número $\pi \in \mathbb{R}$ es $\mathbb{Q}$-trascendente, como probó Lindemann en 1882. El número $e \in \mathbb{R}$ es $\mathbb{Q}$-trascendente, como probó Hermite en 1873.

Si $\alpha \in K$ es algebraica entonces

$$\boxed{k[\alpha] = k[x]/(p(x))},$$

donde $p(x)$ es el polinomio mónico con coeficientes en k de grado mínimo que anula a α. En efecto, el núcleo del morfismo $\phi\colon k[x] \to K$, $\phi(q(x)) := q(\alpha)$ es el ideal formado por todos los polinomios que anulan a α y este ideal está generado por el polinomio $p(x)$ (que podemos suponer mónico) de grado mínimo que anula a α. Observemos que $p(x)$ ha de ser irreducible, porque $k[x]/(p(x)) = k[\alpha]$ es íntegro. Luego, $k[\alpha]$ es cuerpo y $k(\alpha) = k[\alpha]$. Además, el grado de $k[\alpha]$ es igual al grado de $p(x)$.

32. Ejemplo: Sea $\sqrt{2} \in \mathbb{C}$, entonces $\mathbb{Q}[\sqrt[2]{2}] \subseteq \mathbb{C}$ es una $\mathbb{Q}$-extensión finita de cuerpos de grado 2, porque $\mathbb{Q}[\sqrt[2]{2}] = \mathbb{Q}[x]/(x^2 - 2)$.

33. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos y $\alpha \in K$. Entonces, α es algebraica sobre k, si y solo si* $\dim_k k(\alpha) < \infty$.

Demostración. Si α es algebraica y $p(x)$ es el polinomio mínimo anulador de α, entonces $\dim_k k(\alpha) = \operatorname{gr} p(x) < \infty$ (véase 0.6.69). Recíprocamente, si $\dim_k k(\alpha) = n < \infty$ entonces $1, \alpha, \ldots, \alpha^n$ son k-linealmente dependientes, luego existe un polinomio de grado n que anula a α. □

34. Proposición: *Si $k \to K$ es una extensión finita de cuerpos de grado n y $K \to \Sigma$ es una extensión finita de grado m, entonces $k \to \Sigma$ es una extensión finita de grado $n \cdot m$. En particular, la composición de extensiones finitas es una extensión finita.*

Demostración. Se tienen los isomorfismos de espacios vectoriales $\Sigma = K \oplus \overset{m}{\dots} \oplus K$, y $K = k \oplus \overset{n}{\dots} \oplus k$, luego $\Sigma = k \oplus \overset{n \cdot m}{\dots} \oplus k$ y se concluye. □

Si $\alpha_1, \dots, \alpha_n \in K$ son elementos k-algebraicos entonces $k(\alpha_1, \dots, \alpha_n)$ es un extensión finita de k, porque es composición de las extensiones finitas de cuerpos $k \hookrightarrow k(\alpha_1) \hookrightarrow k(\alpha_1, \alpha_2) \hookrightarrow \cdots \hookrightarrow k(\alpha_1, \dots, \alpha_n)$. En particular, dado $p(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$, entonces $p(\alpha_1, \dots, \alpha_n) \in k(\alpha_1, \dots, \alpha_n)$ es k-algebraico.

35. Definición: Se dice que una extensión de cuerpos $k \hookrightarrow K$ es algebraica si todos los elementos de K son algebraicos sobre k.

36. Proposición: *Si $k \hookrightarrow K$ y $K \hookrightarrow K'$ son extensiones algebraicas entonces $k \hookrightarrow K'$ es algebraica.*

Demostración. Dado $\alpha \in K'$, existe un polinomio $p(x) = \sum_i a_i x^i \in K[x]$ tal que $p(\alpha) = 0$. La extensión $k \hookrightarrow k(a_1, \dots, a_n, \alpha)$ es finita, luego $k \hookrightarrow k(\alpha)$ también y α es algebraica sobre k. □

37. Proposición: *Sean $k \hookrightarrow K$ y $k \hookrightarrow K'$ dos extensiones de cuerpos. Entonces, existen una k-extensión de cuerpos L y morfismos de k-extensiones $K \hookrightarrow L$ y $K' \hookrightarrow L$.*

Demostración. Véase 0.4.3. □

38. Definición: Diremos que un cuerpo $\bar{k}$ es algebraicamente cerrado si no admite extensiones de cuerpos finitas (o algebraicas), es decir, todo polinomio con coeficientes en $\bar{k}$ tiene todas sus raíces en $\bar{k}$.

39. Teorema: *Dado un cuerpo k, existe una única extensión de cuerpos $k \hookrightarrow \bar{k}$, salvo isomorfismos, que es algebraica y tal que $\bar{k}$ es algebraicamente cerrado. Diremos que $\bar{k}$ es el cierre algebraico de k.*

Demostración. Sea P el conjunto de polinomios mónicos irreducibles de $k[x]$. Para cada $p \in P$, sean $\alpha_{p1}, \dots, \alpha_{p\,\mathrm{gr}(p)}$ las raíces de $p(x)$ y $K_p = k[\alpha_{p1}, \dots, \alpha_{p\,\mathrm{gr}(p)}]$. Para cada p consideremos un epimorfismo de k-álgebras $\pi_p \colon k[x_{p1}, \dots, x_{p\,\mathrm{gr}(p)}] \to K_p$, y sea $B := k[x_{pi}]_{\{p \in P, 1 \le i\,\mathrm{gr}(p)\}} / (\mathrm{Ker}\,\pi_p)_{\{p \in P\}}$. Sea $\mathfrak{m} \subset B$ un ideal maximal y $\bar{k} = B/\mathfrak{m}$.

Veamos que $\bar{k} = B/\mathfrak{m}$ es k-algebraica y es algebraicamente cerrado. Los elementos $\bar{x}_{pi}$ son k-algebraicos pues son raíces de $p(x)$. Por tanto, los elementos de $\bar{k}$, que son polinomios en estos elementos, son algebraicos.

Si $\bar{k} \hookrightarrow K$ es una extensión de cuerpos algebraica y $\alpha \in K$, entonces α es algebraica y es una de las raíces de un polinomio mónico irreducible $p \in P$, es decir, coincide con alguno de los $\bar{x}_{pi}$. Luego $\alpha \in \bar{k}$ y $K = \bar{k}$.

Sea k' es una extensión algebraica de k y sea L una k extensión de cuerpos que contenga a $\bar{k}$ y k'. Considérese el subcuerpo K de L generado k-algebraicamente por los elementos de $\bar{k}$ y k'. K es una extensión algebraica de K que contiene a $\bar{k}$ y k'. Luego, $k' \subset K = \bar{k}$.

□

0.4.4. Grado de trascendencia de una extensión de cuerpos

40. Definición: Sea A una k-álgebra. Diremos que $\xi_1, \ldots, \xi_n \in A$ son algebraicamente independientes sobre k si el morfismo de k-álgebras

$$\begin{aligned} k[x_1, \ldots, x_n] &\to A \\ p(x_1, \ldots, x_n) &\mapsto p(\xi_1, \ldots, \xi_n) \end{aligned}$$

es inyectivo; es decir, cuando cualquier relación algebraica de los ξ_i con coeficientes en k,

$$\sum_{i_1, \ldots, i_n} a_{i_1 \ldots i_n} \xi_1^{i_1} \ldots \xi_n^{i_n} = 0,$$

implique necesariamente que todos sus coeficientes $a_{i_1 \ldots i_n}$ sean nulos. Diremos que $\xi_1, \ldots, \xi_n$ son algebraicamente dependientes si existe $0 \neq p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ tal que $p(\xi_1, \ldots, \xi_n) = 0$.

41. Definición: Dados $\xi_1, \ldots, \xi_n \in K$, diremos que ξ_n es algebraico sobre $\xi_1, \ldots, \xi_{n-1}$ si ξ_n es algebraico sobre $k(\xi_1, \ldots, \xi_{n-1})$.

42. Definición: Sea $k \to \Sigma$ una extensión de cuerpos. Diremos que $\xi_1, \ldots, \xi_n \in \Sigma$ forman una base de trascendencia de Σ sobre k, si son algebraicamente independientes y $k(\xi_1, \ldots, \xi_n) \to \Sigma$ es algebraica; es decir, si son algebraicamente independientes sobre k y todo elemento de Σ es algebraico sobre $\xi_1, \ldots, \xi_n$.

43. Definición: Diremos que una extensión de cuerpos $k \hookrightarrow K$ es de tipo finito si existen $\xi_1, \ldots, \xi_m \in K$ de modo que la k-subextensión mínima de cuerpos de K que contiene a $\xi_1, \ldots, \xi_m$, que denotamos $k(\xi_1, \ldots, \xi_m)$, coincide con K, es decir, $K = k(\xi_1, \ldots, \xi_m)$.

44. Teorema: *Si $k \hookrightarrow \Sigma$ es una extensión de cuerpos de tipo finito, entonces existen bases de trascendencia de Σ sobre k. Si $\xi_1,\dots,\xi_n$ es una base de trascendencia de una extensión $k \hookrightarrow \Sigma$, entonces todas las bases de trascendencia de esta extensión tienen n elementos, número n llamado grado de trascendencia de Σ sobre k.*

Demostración. Sea $\Sigma = k(\xi_1,\dots,\xi_r)$. Reordenando los generadores si fuera preciso, podemos suponer que $\xi_1,\dots,\xi_n$ son algebraicamente independientes sobre k y ξ_i es algebraico sobre $\xi_1,\dots,\xi_n$ para todo $i > n$. Por 0.4.36, Σ es una extensión algebraica de $k(\xi_1,\dots,\xi_n)$, luego $\{\xi_1,\dots,\xi_n\}$ es una base de trascendencia de Σ sobre k.

Por otra parte, sea $\{y_1,\dots,y_m\}$ otra base de trascendencia de Σ sobre k. Probemos por inducción sobre i que, reordenando $\{y_1,\dots,y_m\}$ si fuera preciso, Σ es una extensión algebraica de la k-extensión $k(\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m)$, para $i \le n$. Para $i = 0$ es inmediato. Suponemos el enunciado cierto para $i - 1 \ge 0$. Por hipótesis de inducción ξ_i es algebraico sobre $k(\xi_1,\dots,\xi_{i-1},y_i,\dots,y_m)$, luego $\xi_1,\dots,\xi_i,y_i,\dots,y_m$ son algebraicamente dependientes. Como $\xi_1,\dots,\xi_i$ son algebraicamente independientes, reordenando $y_i,\dots,y_m$ podemos suponer que y_i es algebraico sobre $\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m$. Por tanto se tienen extensiones algebraicas

$$k(\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m) \hookrightarrow k(\xi_1,\dots,\xi_{i-1},\xi_i,y_i,\dots,y_m) \overset{\text{Algebraica}}{\underset{\text{por Hip.Ind.}}{\hookrightarrow}} \Sigma$$

luego Σ es algebraico sobre $k(\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m)$. Ahora, si m fuera menor que n, tendríamos que Σ es algebraico sobre $k(\xi_1,\dots,\xi_m)$, contra la hipótesis de que los elementos $\xi_1,\dots,\xi_m,\xi_{m+1}$ son algebraicamente independientes. Luego $m \ge n$. Por la misma razón $n \ge m$ y $n = m$. □

45. Ejemplo: Sea k un cuerpo. El cuerpo $k(x_1,\dots,x_n)$ de las funciones racionales del espacio afín $\mathbb{A}^n$ tiene grado de trascendencia n, porque las funciones $x_1,\dots,x_n$ forman claramente una base de trascendencia sobre k.

46. Ejemplo: Sea $p(x_1,\dots,x_n)$ un polinomio irreducible no constante con coeficientes en un cuerpo k. Consideremos $k[x_1,\dots,x_n]/(p(x_1,\dots,x_n))$ y denotemos $\xi_i = \bar{x}_i$. Sea $k(\xi_1,\dots,\xi_n)$ el cuerpo de fracciones de $k[x_1,\dots,x_n]/(p(x_1,\dots,x_n))$, que se denomina cuerpo de funciones racionales de la hipersuperficie definida por la ecuación $p(x_1,\dots,x_n) = 0$. $k(\xi_1,\dots,\xi_n)$ tiene grado de trascendencia $n-1$ sobre k. En efecto, reordenando las variables, podemos suponer que el grado de $p(x_1,\dots,x_n)$ en x_n es ≥ 1; es fácil ver entonces que $\{\xi_1,\dots,\xi_{n-1}\}$ es una base de trascendencia.

47. Notación: Denotaremos por $\mathrm{gr\,tr}_k K$ el grado de trascendencia de K sobre k, o simplemente por $\mathrm{gr\,tr}\, K$ cuando se sobrentienda cuál es el cuerpo base.

0.5. Espectro primo de un anillo

1. Definición: Sea k un cuerpo. Si $i: k \to A$ es un morfismo de anillos diremos que A es una k-álgebra. Seguiremos la notación $i(\lambda) \underset{Not.}{=} \lambda$.

Si A y B son k-álgebras, diremos que un morfismo $\phi: A \to B$ de anillos es un morfismo de k-álgebras si $\phi(\lambda) = \lambda$, para todo $\lambda \in k$. Denotaremos $\mathrm{Hom}_{k-alg}(A,B)$ al conjunto de todos los morfismos de k-álgebras de A en B.

2. Ejemplos: El anillo de polinomios $k[x_1,\dots,x_n]$ es obviamente una k-álgebra y tenemos la igualdad $\mathrm{Hom}_{k-alg}(k[x_1,\dots,x_n],B) = B^n$, $\phi \mapsto (\phi(x_1),\dots,\phi(x_n))$

El anillo de funciones continuas reales de un espacio topológico es una $\mathbb{R}$-álgebra.

3. Definición: Diremos que un ideal $\mathfrak{m}$ de una k-álgebra A es racional, si $A/\mathfrak{m} \simeq k$ (como k-álgebras). Llamaremos *espectro primo racional* de A, que denotaremos $\mathrm{Spec}_{rac} A$, al conjunto de los ideales racionales de A.

Los ideales racionales son maximales.

Dado un ideal racional $\mathfrak{m} \subset A$ tenemos el morfismo de k-álgebras $A \to A/\mathfrak{m} = k$. Recíprocamente, dado un morfismo de k-álgebras $\phi: A \to k$ (que ha de ser epiyectivo) tenemos el ideal primo racional $\mathrm{Ker}\,\phi$. En conclusión,

$$\mathrm{Hom}_{k-alg}(A,k) = \mathrm{Spec}_{rac} A,\ \phi \mapsto \mathrm{Ker}\,\phi.$$

4. Ejemplo: Se cumple que

$$k^n = \mathrm{Spec}_{rac}\, k[x_1,\dots,x_n],\ (\alpha_1,\dots,\alpha_n) \mapsto (x_1-\alpha_1,\dots,x_n-\alpha_n).$$

En efecto, el ideal $(x_1-\alpha_1,\dots,x_n-\alpha_n)$ es racional ya que el morfismo

$$k \to k[x_1,\dots,x_n]/(x_1-\alpha_1,\dots,x_n-\alpha_n),\ \lambda \mapsto \lambda$$

es un isomorfismo: es epiyectivo y el núcleo es el ideal (0). Tenemos la biyección

$$k^n = \mathrm{Hom}_{k-alg}(k[x_1,\dots,x_n],k) = \mathrm{Spec}_{rac}(k[x_1,\dots,x_n]),\ \alpha \mapsto \mathrm{Ker}\,\phi_\alpha,$$

donde $\phi_\alpha(p(x_1,\dots,x_n)) := p(\alpha)$. Por último, $\mathrm{Ker}\,\phi_\alpha = (x_1-\alpha_1,\dots,x_n-\alpha_n)$, porque el ideal $(x_1-\alpha_1,\dots,x_n-\alpha_n)$ está incluido en $\mathrm{Ker}\,\phi_\alpha$.

Si "pensamos" $k[x_1,\dots,x_n]$ como las funciones algebraicas del espacio afín k^n, el modo de recuperar k^n a partir de $k[x_1,\dots,x_n]$ es considerando su espectro racional.

5. Ejemplo: Sea $I=(p_1(x),\dots,p_m(x))\subseteq k[x_1,\dots,x_n]$ un ideal. Se cumple que

$$\mathrm{Spec}_{rac}(k[x_1,\dots,x_n]/(p_1(x),\dots,p_m(x))=\{\alpha\in k^n:\, p_1(\alpha)=0,\dots,p_m(\alpha)=0\}.$$

En efecto, $\mathrm{Spec}_{rac}(k[x_1,\dots,x_n]/I)=\mathrm{Hom}_{k-alg}(k[x_1,\dots,x_n]/I,k)$ que es igual al conjunto $\{\phi\in\mathrm{Hom}_{k-alg}(k[x_1,\dots,x_n],k)$, tales que $\phi(p_i(x))=0,\,\forall\, i\}=\{\alpha\in k^n:\, p_i(\alpha)=0,\,\forall\, i\}$.

Si "pensamos" $A=k[x_1,\dots,x_n]/(p_1(x),\dots,p_m(x))$ como el anillo de funciones algebraicas de la variedad de soluciones, V, del sistema de ecuaciones $p_1(x)=\cdots=p_m(x)=0$, entonces $V=\mathrm{Spec}_{rac}\,A$.

6. Ejemplo: Sea X un espacio compacto T_2 y $C(X)$ el anillo de funciones reales continuas definidas sobre X. Dado un punto $p\in X$, el ideal $\mathfrak{m}_p$ de funciones que se anulan en p es un ideal maximal, porque $C(X)/\mathfrak{m}_p\simeq\mathbb{R}$, $\bar{f}\mapsto f(p)$. Además, $\mathfrak{m}_p\neq\mathfrak{m}_q$ si $p\neq q$, porque X es un espacio topológico normal y las funciones continuas separan cerrados disjuntos, por el lema de Urysohn.

Dado un ideal maximal $\mathfrak{m}\subset C(X)$, si $\mathfrak{m}\neq\mathfrak{m}_p$ para todo $p\in X$, entonces para cada $p\in X$ existe una función $f_p\in\mathfrak{m}$ que no se anula en p, luego tampoco en un entorno U_p de p. Como X es compacto, un número finito $U_{p_1},\dots,U_{p_n}$ recubren X. Por tanto, $f:=f_{p_1}^2+\cdots+f_{p_n}^2$ no se anula en ningún punto de X, luego es invertible y $f\in\mathfrak{m}$, contradicción. Hemos probado que todo ideal maximal es racional y que la aplicación

$$(*)\qquad X\longrightarrow\mathrm{Spec}_{rac}\,C(X),\ p\mapsto\mathfrak{m}_p$$

es una biyección. Dado un cerrado $C\subseteq X$, sea I_C el ideal de $C(X)$ de las funciones que se anulan en todo C. El lector puede probar que $C=(I_C)_0^{rac}$ y que la igualdad $(*)$ es un homeomorfismo.

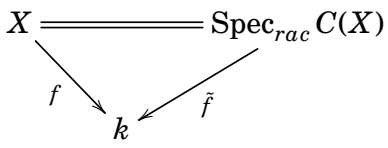
7. Dotemos a $X=\mathrm{Spec}_{rac}\,A$ de topología. Dado un ideal $I\subseteq A$ denotaremos $(I)_0^{rac}:=\{\mathfrak{m}\in X:\, I\subseteq\mathfrak{m}\}$ y diremos que es un cerrado de $\mathrm{Spec}_{rac}\,A$. Observemos que $\emptyset=(A)_0^{rac}$, $X=(0)_0^{rac}$; que $(\sum_i I_i)_0^{rac}=\cap_i(I_i)_0^{rac}$. Por último, $(I_1\cap I_2)_0^{rac}=(I_1)_0^{rac}\cup(I_2)_0^{rac}$: obviamente $(I_1)_0^{rac}\cup(I_2)_0^{rac}\subseteq(I_1\cap I_2)_0^{rac}$; por último, $\mathfrak{m}\notin(I_1)_0^{rac}\cup(I_2)_0^{rac}$ entonces existen $a_1\in I_1$ y $a_2\in I_2$ tales que $a_1,a_2\notin\mathfrak{m}$, luego $a_1\cdot a_2\notin\mathfrak{m}$ y $\mathfrak{m}\notin(I_1\cap I_2)_0^{rac}$.

Si $f:A\to B$ es un morfismo de k-álgebras y $\mathfrak{m}\subset B$ es un ideal racional entonces $f^{-1}(\mathfrak{m})$ es un ideal racional de A. En efecto, el núcleo de la composición $A\to B\to B/\mathfrak{m}=k$ es $f^{-1}(\mathfrak{m})$. Por tanto, f induce la aplicación entre los espectros racionales

$$f^*:\,\mathrm{Spec}_{rac}\,B\to\mathrm{Spec}_{rac}\,A,\ \mathfrak{m}\mapsto f^{-1}(\mathfrak{m}).$$

Además, f^* es una aplicación continua, porque $f^{*-1}((I)_0^{rac})=(f(I))_0^{rac}$. Dada $a\in A$, tenemos el morfismo de k-álgebras $k[x]\to A$, $p(x)\mapsto p(a)$, que induce un morfismo

$\tilde{a}\colon \operatorname{Spec}_{rac} A \to \operatorname{Spec}_{rac} k[x] = k$. En el ejemplo anterior, dada $f \in C(X)$, el diagrama



es conmutativo.

Dado un morfismo de k-álgebras

$$f\colon A = k[x_1,\dots,x_n]/(p_1,\dots,p_r) \to k[y_1,\dots,y_m]/(q_1,\dots,q_s) = B,\ f(\bar{x}_i) = \overline{f_i(y_1,\dots,y_m)},$$

calculemos el morfismo $f^*\colon \operatorname{Spec}_{rac} B \to \operatorname{Spec}_{rac} A$ inducido. Dado $\alpha = (\alpha_1,\dots,\alpha_m) \in \operatorname{Spec}_{rac} B$, es decir, el ideal $\mathfrak{m}_\alpha := (\bar{y}_1 - \alpha_1,\dots,\bar{y}_m - \alpha_m)$, se cumple que

$$f^*(\alpha) = (f_1(\alpha_1,\dots,\alpha_m),\dots,f_n(\alpha_1,\dots,\alpha_m)),$$

pues el núcleo de la composición $A \to B \to B/\mathfrak{m}_\alpha = k$, $\bar{x}_i \mapsto \overline{f_i(y_1,\dots,y_m)} \mapsto f_i(\alpha_1,\dots,\alpha_m)$, es $f^*(\alpha)$ y coincide con $(\bar{x}_1 - f_1(\alpha_1,\dots,\alpha_m),\dots,\bar{x}_n - f_n(\alpha_1,\dots,\alpha_m))$.

8. Ejercicio: Sean X e Y espacios topológicos compactos T_2. Prueba que la aplicación

$$\operatorname{Hom}_{\text{cont.}}(X,Y) \to \operatorname{Hom}_{\mathbb{R}-\text{alg}}(C(Y),C(X)),\ \phi \mapsto \phi^* \text{ (donde } \phi^*(f) := f \circ \phi),$$

es biyectiva (usar el ejemplo 0.5.6 y que todo morfismo $C(Y) \to C(X)$ induce un morfismo entre los espectros racionales).

9. Definición: Se llama espectro primo de un anillo A al conjunto $\operatorname{Spec} A$ de sus ideales primos.

10. Notación: Un ideal primo lo denotaremos por x cuando lo consideremos como elemento de $\operatorname{Spec} A$, y por $\mathfrak{p}_x$ cuando lo consideremos como ideal de A.

Llamaremos funciones a los elementos del anillo A y puntos a los elementos de $\operatorname{Spec} A$. Diremos que una función $a \in A$ se anula en un punto $x \in \operatorname{Spec} A$ cuando $a \in \mathfrak{p}_x$, es decir, cuando $0 = \bar{a} \in A/\mathfrak{p}_x$ (suele denotarse $a(x) = \bar{a} \in A/\mathfrak{p}_x$). Como $\mathfrak{p}_x$ es un ideal primo se verifica:

1. La función 0 se anula en todos los puntos de $\operatorname{Spec} A$.
2. Si dos funciones se anulan en un punto x, su suma también.
3. Si una función se anula en un punto x, sus múltiplos también.
4. Si un producto de funciones se anula en un punto x, algún factor se anula en x.

11. Ejercicio: Prueba que una función $f \in A$ es invertible si y solo si no se anula en ningún punto de $\mathrm{Spec}A$.

12. Ejercicio: Prueba que $p(x,y)$ se anula en el ideal primo $\mathfrak{m}_{\alpha,\beta} = (x-\alpha, y-\beta) \subset k[x,y]$ si y solo si $p(\alpha,\beta) = 0$.

13. Definición: Sea A un anillo. Si $f \in A$, llamaremos *ceros* de la función f al subconjunto $(f)_0 \subset \mathrm{Spec}A$ formado por todos los puntos donde se anule f. Llamaremos ceros de un ideal $I \subseteq A$ al subconjunto de $\mathrm{Spec}A$ formado por los puntos donde se anulen todas las funciones de I y lo denotaremos $(I)_0$, es decir,

$$(I)_0 = \bigcap_{f\in I}(f)_0 = \left\{ \begin{array}{c} \text{Ideales primos } \mathfrak{p}_x \subset A \\ \text{tales que } I \subseteq \mathfrak{p}_x \end{array} \right\}.$$

14. Proposición: *Tenemos las siguientes igualdades:*

1. $(0)_0 = \mathrm{Spec}A$ *y* $(A)_0 = \emptyset$.
2. $(\sum_{j\in J} I_j)_0 = \bigcap_{j\in J}(I_j)_0$.
3. $(\bigcap_{j=1}^{n} I_j)_0 = \bigcup_{j=1}^{n}(I_j)_0$.

Demostración. Todas las igualdades son de demostración inmediata, salvo quizá la 3. Para ésta, basta probar que $(I_1 \cap I_2)_0 = (I_1)_0 \cup (I_2)_0$. Veámoslo:

Obviamente, $(I_1 \cap I_2)_0 \supseteq (I_1)_0 \cup (I_2)_0$. Veamos la otra inclusión: Sea $x \in (I_1 \cap I_2)_0$. Si $x \notin (I_1)_0$ y $x \notin (I_2)_0$, entonces existe $f_1 \in I_1$ y $f_2 \in I_2$ que no se anulan en x, luego $f_1 \cdot f_2$ no se anula en x. Pero como $f_1 \cdot f_2 \in I_1 \cap I_2$ llegamos a contradicción con que $x \in (I_1 \cap I_2)_0$. Por tanto, $x \in (I_1)_0 \cup (I_2)_0$ y $(I_1 \cap I_2)_0 \subseteq (I_1)_0 \cup (I_2)_0$.

□

15. Ejercicio: Demuestra que $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0 = (I_1 \cap I_2)_0$, donde denotamos por $I_1 \cdot I_2 = \{\sum_i a_i b_i \mid a_i \in I_1, b_i \in I_2\}$.

16. Definición: Llamamos topología de Zariski de $\mathrm{Spec}A$, a la topología sobre $\mathrm{Spec}A$ cuyos cerrados son los ceros de los ideales de A.

La proposición anterior nos dice que la topología de Zariski es efectivamente una topología.

Los cerrados $\{(f)_0\}_{f\in A}$ forman una base de cerrados de la topología de Zariski de A, ya que $(I)_0 = \bigcap_{f\in I}(f)_0$.

Dado un punto $x \in \operatorname{Spec} A$ y un cerrado $C = (I)_0$, si $x \notin C$ existe $f \in I \subseteq A$ que no se anula en x, "las funciones de A separan puntos de cerrados en $\operatorname{Spec} A$".

Dada una inclusión $I_1 \subseteq I_2$ de ideales se tiene que $(I_1)_0 \supseteq (I_2)_0$. Dado un cerrado C se verifica que $C = (I)_0$, donde I es el ideal de todas las funciones que se anulan en C: Obviamente $C \subseteq (I)_0$. Por otra parte $C = (J)_0$ para algún ideal $J \subseteq A$. Tenemos que las funciones de J se anulan en C, luego $J \subseteq I$. Por tanto, $C = (J)_0 \supseteq (I)_0$. Hemos concluido.

Si bien, $C = (I)_0$, donde I es el ideal de todas las funciones que se anulan en C, pueden existir ideales $J \subsetneq I$ tales que $C = (I)_0 = (J)_0$. Por ejemplo, $(4)_0 = (2)_0 \subset \operatorname{Spec} \mathbb{Z}$.

17. Ejercicio: Determina los puntos y la topología de $\operatorname{Spec} \mathbb{Z}$.

18. Ejemplo: Los ideales primos de $k[x]$ son los ideales $(p(x))$, con $p(x)$ primo o irreducible y el ideal (0). Si $k = \mathbb{C}$, los ideales primos de $\mathbb{C}[x]$ son $\mathfrak{m}_\alpha = (x - \alpha)$, $\alpha \in \mathbb{C}$ y (0). Así que los ideales primos maximales de $\mathbb{C}[x]$ se corresponden con los puntos de una recta afín. De aquí que se siga la notación $\operatorname{Spec} \mathbb{C}[x] = \mathbb{A}_1(\mathbb{C})$. En resumen

$$\operatorname{Spec} \mathbb{C}[x] = \begin{cases} \text{"Puntos cerrados": } \alpha \equiv (x - \alpha), \text{ con } \alpha \in \mathbb{C}. \\ \text{"Punto genérico": } g \equiv (0). \end{cases}$$

En general, si k es un cuerpo, diremos que $\operatorname{Spec} k[x] =: \mathbb{A}^1(k)$ es la recta afín sobre k.

Dado un ideal $(p(x)) \subset \mathbb{C}[x]$ los ceros de $(p(x))$ se corresponden con las raíces de $p(x)$, salvo cuando $p(x) = 0$, en este caso los ceros es todo el espectro. Por tanto, los cerrados de la topología de Zariski de $\operatorname{Spec} \mathbb{C}[x]$, a parte del vacío y el total, son los conjuntos finitos de puntos cerrados (de la recta afín).

19. Teorema: *El espectro primo de un anillo es un espacio topológico compacto.*

Demostración. Sea $C_j = (I_j)_0$ una familia arbitraria de cerrados de $\operatorname{Spec} A$. Si $\bigcap_j C_j = \emptyset$ entonces

$$\emptyset = \bigcap_j (I_j)_0 = (\sum_j I_j)_0$$

Por tanto, $\sum_j I_j = A$. Luego $1 = f_1 + \cdots + f_n$ para ciertas $f_1 \in I_{j_1}, \ldots, f_n \in I_{j_n}$. Luego, de nuevo $I_{j_1} + \cdots + I_{j_n} = A$ y

$$(I_{j_1})_0 \cap \cdots \cap (I_{j_n})_0 = \emptyset,$$

es decir, $C_{j_1} \cap \cdots \cap C_{j_n} = \emptyset$ y $\operatorname{Spec} A$ es compacto.

□

20. Notación: Dado un subconjunto Y de $\operatorname{Spec} A$, denotamos por $\bar{Y}$ el cierre de Y en $\operatorname{Spec} A$.

21. Proposición: *Sea $Y \subseteq \operatorname{Spec} A$ un subconjunto e $I \subseteq A$ el ideal de todas las funciones que se anulan en todos los puntos de Y, entonces $\bar{Y} = (I)_0$.*

Demostración. Obviamente $Y \subseteq (I)_0$, luego $\bar{Y} \subseteq (I)_0$. Existe un ideal $J \subseteq A$, tal que $(J)_0 = \bar{Y}$. Obviamente, J se anulan en todos los puntos de Y, luego $J \subseteq I$ y $(I)_0 \subseteq (J)_0 = \bar{Y}$. Por tanto, $\bar{Y} = (I)_0$.

□

22. Proposición: *Dado $x \in \operatorname{Spec} A$ se verifica que $\bar{x} = (\mathfrak{p}_x)_0$. En particular,* $\operatorname{Spec} A$ *es un espacio topológico T_0 (puntos distintos tienen cierres distintos) y un punto x es cerrado si y solo si $\mathfrak{p}_x$ es un ideal maximal.*

23. Definición: Diremos que un espacio topológico es irreducible cuando no pueda descomponerse como unión de dos cerrados estrictamente menores. Llamaremos componentes irreducibles de un espacio topológico a los subespacios irreducibles maximales de X (que existen por el lema de Zorn), es decir, los subespacios irreducibles no contenidos estrictamente en otro subespacio irreducible.

El cierre de un subespacio irreducible es irreducible, en particular las componentes irreducibles de un espacio son cerradas.

24. Proposición: *Cada cerrado irreducible del espectro de un anillo es el cierre de un único punto, llamado punto genérico de tal cerrado. Las componentes irreducibles de* $\operatorname{Spec} A$ *son los cierres de los puntos (llamados puntos genéricos de* $\operatorname{Spec} A$*) definidos por los ideales primos minimales de A.*

Demostración. Sea C un cerrado irreducible. Sabemos que $C = (I)_0$, donde I es el ideal de todas las funciones que se anulan en C.

Basta ver que I es primo, porque si $I = \mathfrak{p}_x$ entonces $(I)_0 = \bar{x}$. Si $f \cdot g \in I$, es decir, $f \cdot g$ se anula en C, entonces

$$C = C \cap (fg)_0 = C \cap ((f)_0 \cup (g)_0)) = (C \cap (f)_0) \cup (C \cap (g)_0),$$

luego, o f se anula en C, o bien g, porque C es irreducible. Es decir, o bien $f \in I$, o bien $g \in I$.

□

25. Ejercicio: Calcula las componentes irreducibles de $\operatorname{Spec} k[x,y]/(xy)$.

Sea $j\colon A \to B$ un morfismo de anillos. Si J es un ideal de B, entonces $j^{-1}(J) := \{a \in A : j(a) \in J\}$ es un ideal de A. Es fácil comprobar que si $\mathfrak{p}$ es un ideal primo de B entonces $j^{-1}(\mathfrak{p})$ es un ideal primo de A. Obtenemos así una aplicación natural

$$j^*\colon \operatorname{Spec} B \to \operatorname{Spec} A, \quad j^*(\mathfrak{p}) := j^{-1}(\mathfrak{p}).$$

26. Teorema: *La aplicación inducida en los espectros por cualquier morfismo de anillos es continua.*

Demostración. Consideremos los morfismos

$$\begin{array}{ccc} A & \xrightarrow{\ j\ } & B \\ \operatorname{Spec} A & \xleftarrow[\ j^*\ ]{} & \operatorname{Spec} B \end{array}$$

Sea $(I)_0 \subset \operatorname{Spec} A$ un cerrado. Entonces

$$\begin{aligned} {j^*}^{-1}((I)_0) &= \{x \in \operatorname{Spec} B : j^*(x) \in (I)_0\} = \{x \in \operatorname{Spec} B : j^{-1}(\mathfrak{p}_x) \supseteq I\} \\ &= \{x \in \operatorname{Spec} B : \mathfrak{p}_x \supseteq j(I)\} = ((j(I)))_0 \end{aligned}$$

y concluimos que j^* es continua.

□

27. Teorema: *Sea I un ideal de A. Consideremos los morfismos naturales*

$$\begin{array}{ccc} A & \xrightarrow{\ \pi\ } & A/I \\ \operatorname{Spec} A & \xleftarrow[\ \pi^*\ ]{} & \operatorname{Spec} A/I \end{array} \qquad\qquad a \longmapsto \bar{a}$$

Se cumple que π^* es un homeomorfismo de $\operatorname{Spec} A/I$ *con su imagen, que es el cerrado* $(I)_0$.

Demostración. Los ideales primos de A/I se corresponden con los ideales primos de A que contienen a I. Explícitamente,

$$\left\{\begin{array}{l}\text{Ideales primos de } A \\ \text{que contienen a } I\end{array}\right\} \Longleftrightarrow \{\text{Ideales primos de } A/I\}$$

$$\mathfrak{p} \longmapsto \pi(\mathfrak{p})$$

$$\pi^{-1}(\mathfrak{p}') \longmapsfrom \mathfrak{p}'$$

que es justamente el morfismo

$$\operatorname{Spec} A \supseteq (I)_0 \xrightarrow{\pi^*} \operatorname{Spec} A/I$$

Lo que demuestra la biyección buscada. Sabemos que π^* es continua, para ver que la biyección es un homeomorfismo, nos falta probar que π^* es cerrada. Igualmente, los ideales primos de A/I que contienen a un ideal J, se corresponden con los ideales primos de A que contienen a $\pi^{-1}(J)$. Es decir, $\pi^*((J)_0) = (\pi^{-1}(J))_0$. Por tanto, π^* es cerrada.

□

28. Ejercicio: Sea Y un subespacio cerrado de un espacio topológico X. Prueba que el subconjunto, del anillo de funciones reales continuas $C(X)$ de X, formado por las funciones que se anulan en Y es un ideal, I. Si X es un espacio topológico normal prueba que $C(X)/I \simeq C(Y)$ (recuérdese que el teorema de extensión de Tietze afirma que toda función continua sobre un cerrado Y admite una extensión continua a todo X).

29. Corolario: $\operatorname{Spec}(A \times B) = (\operatorname{Spec} A) \coprod (\operatorname{Spec} B)$.

Demostración. Consideremos en el anillo $A \times B$ los ideales $I = A \times 0$, $J = 0 \times B$. Como $I + J = A \times B$ y $I \cap J = 0$, tomando ceros tenemos $(I)_0 \cap (J)_0 = \emptyset$ y $(I)_0 \cup (J)_0 = \operatorname{Spec}(A \times B)$. Es decir, $\operatorname{Spec}(A \times B) = (I)_0 \coprod (J)_0$.

Para concluir basta observar que, de acuerdo con el teorema anterior,

$$(I)_0 = \operatorname{Spec}(A \times B)/I = \operatorname{Spec} B$$
$$(J)_0 = \operatorname{Spec}(A \times B)/J = \operatorname{Spec} A$$

□

Explícitamente, los ideales primos de $A \times B$ son de la forma $\mathfrak{p} \times B$ o $A \times \mathfrak{q}$, donde $\mathfrak{p}$ es un ideal primo de A y $\mathfrak{q}$ es un ideal primo de B.

30. Ejercicio: Sean X e Y espacios topológicos y consideremos el espacio topológico $X \coprod Y$. Demuestra que

$$C(X \coprod Y) = C(X) \times C(Y).$$

Justificar la frase "$A \times B$ es el anillo de funciones de $\operatorname{Spec} A \coprod \operatorname{Spec} B$".

0.5.1. Localización y espectro primo. Fórmula de la fibra

Nuestro primer objetivo es mostrar que el proceso algebraico de división se va a corresponder con el proceso topológico de localización.

Dado un morfismo de anillos $j: A \to B$, cuando no cause confusión, seguiremos las siguientes notaciones: dado un ideal J de B, escribiremos $j^{-1}(J) = J \cap A$, dado un ideal I de A escribiremos $(j(I)) = j(I) \cdot B = I \cdot B$.

31. Teorema: *Consideremos el morfismo $j: A \to A_S$, $a \mapsto \frac{a}{1}$, de localización por S. La aplicación inducida $j^*: \operatorname{Spec} A_S \to \operatorname{Spec} A$ establece un homeomorfismo de $\operatorname{Spec} A_S$ con su imagen, que está formada por los puntos de $\operatorname{Spec} A$ donde no se anula ninguna función de S:*

$$\operatorname{Spec} A_S \underset{j^*}{=} \{\textit{ideales primos de } A \textit{ que no cortan a } S\}.$$

Demostración. Las asignaciones

$$\operatorname{Spec} A_S \longrightarrow \{\text{Ideales primos de } A \text{ que no cortan a } S\} \subseteq \operatorname{Spec} A$$

$$\mathfrak{p}' \longmapsto \mathfrak{p}' \cap A \qquad (j^*)$$

$$\mathfrak{p} \cdot A_S \longmapsto \mathfrak{p}$$

están bien definidas y son inversas entre sí, sin más que comprobar:

1. Si $\mathfrak{p}'$ es un ideal primo de A_S entonces $\mathfrak{p}' \cap A$ es un ideal primo de A que no corta con S y $(\mathfrak{p}' \cap A) \cdot A_S = \mathfrak{p}'$.

2. Si $\mathfrak{p}$ es un ideal primo de A que no corta con S entonces $\mathfrak{p} \cdot A_S$ es un ideal primo de A_S y $(\mathfrak{p} \cdot A_S) \cap A = \mathfrak{p}$.

Para ver que esta biyección es un homeomorfismo basta observar que $j^*((\frac{a}{s})_0) = j^*((\frac{a}{1})_0) = (a)_0 \cap \operatorname{Im} j^*$. □

32. Notación: Sea A un anillo. Si $f \in A$, denotaremos A_f la localización de A por el sistema multiplicativo $S = \{1, f, f^2, \ldots, f^n, \ldots\}$. Si x es un punto de $\operatorname{Spec} A$, denotaremos por A_x la localización de A por el sistema multiplicativo $S = A \setminus \mathfrak{p}_x$.

Dado $f \in A$, denotaremos $U_f = \operatorname{Spec} A \setminus (f)_0$ y diremos que es un abierto básico. Observemos que el conjunto de los abiertos básicos $\{U_f\}_{f \in A}$ es una base de abiertos de la topología de Zariski de $\operatorname{Spec} A$, porque el conjunto de los cerrados básicos $\{(f)_0\}_{f \in A}$ es es una base de cerrados de la topología de Zariski de $\operatorname{Spec} A$.

33. Corolario: *El espectro de A_f es igual a $\operatorname{Spec} A \setminus (f)_0$:*

$$\operatorname{Spec} A_f = U_f.$$

Demostración. Por el teorema anterior, $\mathrm{Spec}\, A_f$ se corresponde con los ideales primos $\mathfrak{p}_x$ de A que no cortan con $S = \{1, f, f^2, \ldots, f^n, \ldots\}$. Que equivale a decir que $\mathrm{Spec}\, A_f$ se corresponde con los ideales primos $\mathfrak{p}_x$ de A que no contienen a f, es decir, U_f. □

34. Ejercicio: Sea $C(\mathbb{R}^n)$ el anillo de funciones reales continuas sobre $\mathbb{R}^n$. Sea U un abierto de $\mathbb{R}^n$, $C(U)$ el anillo de funciones reales continuas sobre U y S el sistema multiplicativo formado por las funciones que no se anulan en ningún punto de U. Prueba que existe un isomorfismo natural $C(\mathbb{R}^n)_S = C(U)$. (Pista: Sea d la función distancia. Dada $h \in C(U)$, $s(x) = \frac{d(x,U^c)}{1+h^2(x)}$ no se anula en U, s y $f = h \cdot s$ son restricción de funciones continuas de $\mathbb{R}^n$ y $h = \frac{f}{s}$).

35. Corolario: *Los ideales primos de A_x se corresponden con los ideales primos de A contenidos en $\mathfrak{p}_x$. En particular, A_x tiene un único ideal maximal, que es $\mathfrak{p}_x \cdot A_x$.*

Demostración. $\mathrm{Spec}\, A_x$ se corresponde con los ideales primos de A que no cortan con $A \setminus \mathfrak{p}_x$. Es decir, con los ideales primos de A contenidos en $\mathfrak{p}_x$. □

36. Definición: Los anillos con un único ideal maximal se les denomina anillos locales.

"Podemos decir que el anillo de funciones que consideramos en $U_f = \mathrm{Spec}\, A_f$ es A_f. Si S es el sistema multiplicativo de las funciones de A que no se anulan en ningún punto de U_f, el lector puede probar que $A_f = A_S$. Como es de desear, estamos diciendo que las funciones de U_f, son los cocientes a/b de funciones de $\mathrm{Spec}\, A$, donde b es una función que no se anula en ningún punto de U_f. Dado un punto x, es usual no querer fijar la atención en un entorno dado de x, sino considerar un entorno lo suficientemente pequeño, luego las funciones que no se anulan en x pasan a ser invertibles y consideraremos por tanto el anillo A_x. Así pues, A_x recoge el concepto impreciso de funciones en un entorno suficientemente pequeño de x".

37. Proposición: *Sean $x_1, \ldots, x_n \in \mathrm{Spec}\, A$ e $I \subset A$ un ideal.. Entonces,*

1. *Si $I \subseteq \mathfrak{p}_{x_1} \cup \cdots \cup \mathfrak{p}_{x_n}$ entonces $I \subseteq \mathfrak{p}_{x_i}$, para algún i.*
2. *Sea $S = A \setminus \cup_i \mathfrak{p}_{x_i}$, entonces $\mathrm{Spec}\, A_S = \cup_i \mathrm{Spec}\, A_{x_i}$. Por tanto, A_S es un anillo semilocal[3] de ideales maximales $\mathfrak{p}_{x_i} \cdot A_S$ (siempre que $\mathfrak{p}_{x_i}$ no esté incluido en $\mathfrak{p}_{x_j}$, para algún $j \neq i$).*

Demostración. 1. Procedamos por reducción al absurdo. Desechando los ideales primos $\mathfrak{p}_{x_i}$ que convenga, podemos suponer que $I \not\subset \mathfrak{p}_{x_1} \cup \cdots \cup \widehat{\mathfrak{p}_{x_i}} \cup \cdots \cup \mathfrak{p}_{x_n}$, para todo i y que $\mathfrak{p}_{x_i} \not\subset \mathfrak{p}_{x_i}$ para todo $i \neq j$. Sea $f_i \in I$ tal que $f_i(x_j) \neq 0$ (y $f_i(x_i) = 0$). Entonces, $g_i = \prod_{j \neq i} f_j$

[3] Un anillo se dice que es semilocal si solo tiene un número finito de ideales maximales.

cumple que $g_i(x_j) \neq 0$ si y solo si $i = j$. Por tanto, $f = \sum_i g_i$ no se anula en ningún x_i y $f \in I$, lo que es contradictorio.

2. En efecto,

$$\begin{aligned}\operatorname{Spec} A_S &= \{x \in \operatorname{Spec} A : \mathfrak{p}_x \cap S = \emptyset\} = \{x \in \operatorname{Spec} A : \mathfrak{p}_x \subseteq \cup_i \mathfrak{p}_{x_i}\} \\ &\overset{1}{=} \{x \in \operatorname{Spec} A : \mathfrak{p}_x \subseteq \mathfrak{p}_{x_i}, \text{ para algún } i\} = \cup_i \operatorname{Spec} A_{x_i}.\end{aligned}$$

□

38. Definición: Dado un anillo A, llamaremos radical de A al ideal formado por el conjunto de los elementos nilpotentes de A, es decir, si denotamos por $\operatorname{rad} A$ al radical de A, entonces

$$\operatorname{rad} A = \{a \in A : a^n = 0, \text{ para algún } n \in \mathbb{N}\}.$$

Dados $a, b \in A$, si $a^n = 0$ y $b^m = 0$, entonces $(a+b)^{n+m} = 0$. Ahora es fácil demostrar que el radical de un anillo es un ideal.

39. Corolario: *El radical de un anillo coincide con la intersección de todos los ideales primos del anillo:*

$$\operatorname{rad} A = \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x.$$

Es decir, una función es nilpotente si y solo si se anula en todo punto del espectro.

Demostración. Si $f \in A$ es nilpotente, i.e., $f^n = 0$ para un $n \in \mathbb{N}$, entonces f ha de pertenecer a todo ideal primo de A. Luego $\operatorname{rad} A \subseteq \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$.

Sea ahora $f \in \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$. Por el corolario 0.5.33, $\operatorname{Spec} A_f = \emptyset$. Por tanto, $A_f = 0$, es decir, $\frac{1}{1} = \frac{0}{1}$. Luego existe un $f^n \in \{1, f, f^2, \ldots\}$, de modo que $f^n \cdot 1 = 0$. Entonces, f es nilpotente. En conclusión $\operatorname{rad} A \supseteq \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$ y hemos terminado. □

Observemos que $\operatorname{Spec} A = \operatorname{Spec}(A/\operatorname{rad} A)$.

40. Definición: Se dice que un anillo A es reducido si $\operatorname{rad} A = 0$.

Dado un anillo A se cumple que $A/\operatorname{rad} A$ es reducido: dado $\bar{a} \in (A/\operatorname{rad} A)$ si $\bar{a}^n = 0$, entonces $a^n \in \operatorname{rad} A$, luego $a \in \operatorname{rad} A$ y $\bar{a} = 0$.

41. Proposición: $\operatorname{Spec} A$ *es irreducible si y solo si* $A/\operatorname{rad} A$ *es un anillo íntegro.*

Demostración. Si $\operatorname{Spec} A$ es irreducible, es el cierre de un punto x, y $\mathfrak{p}_x$ es el único ideal primo minimal de A. Por tanto, $\operatorname{rad} A = \mathfrak{p}_x$ y $A/\operatorname{rad} A$ es un anillo íntegro. Si $A/\operatorname{rad} A$ es íntegro entonces $\operatorname{rad} A = \mathfrak{p}_x$ es un ideal primo y $\operatorname{Spec} A = \operatorname{Spec}(A/\operatorname{rad} A) = (\mathfrak{p}_x)_0 = \bar{x}$ es irreducible. □

42. Definición: Dado un ideal $I \subseteq A$, llamaremos radical de I, y lo denotaremos $r(I)$, a

$$r(I) = \{a \in A : a^n \in I \text{ para algún } n \in \mathbb{N}\}.$$

Observemos que si $\pi : A \to A/I$ es el morfismo de paso al cociente, entonces el radical de I es la antimagen por π del radical de A/I. Por tanto, el radical de un ideal es la intersección de los ideales primos que lo contienen. Por tanto, dados dos ideales I, I' de A si $(I)_0 = (I')_0$ entonces $r(I) = r(I')$ y recíprocamente. En conclusión, si denominamos ideales radicales a los ideales que coinciden con su radical tenemos que hay una correspondencia biunívoca entre los ideales radicales de un anillo y los cerrados del espectro primo del anillo.

Dado un morfismo de anillos $j : A \to B$ y un sistema multiplicativo S en A, escribiremos $B_{j(S)} = B_S$. Igualmente, dado un ideal primo $\mathfrak{p}_x$ de A, escribiremos $B_{j(A\setminus \mathfrak{p}_x)} = B_x$.

43. Fórmula de la fibra: *Sea $j : A \to B$ un morfismo de anillos y consideremos el morfismo inducido $j^* : \operatorname{Spec} B \to \operatorname{Spec} A$. Dado un punto $x \in \operatorname{Spec} A$ se verifica*

$$j^{*-1}(x) = \operatorname{Spec}(B_x/\mathfrak{p}_x \cdot B_x).$$

Si $\mathfrak{p}_x$ es un ideal primo minimal se verifica $j^{*-1}(x) = \operatorname{Spec} B_x$.
Si $\mathfrak{p}_x$ es un ideal primo maximal se verifica $j^{*-1}(x) = \operatorname{Spec}(B/\mathfrak{p}_x \cdot B)$.

Demostración.

$$\begin{aligned} j^{*-1}(x) &= \{y \in \operatorname{Spec} B : \mathfrak{p}_y \cap A = \mathfrak{p}_x\} \\ &= \{y \in \operatorname{Spec} B : \mathfrak{p}_y \cap A \subseteq \mathfrak{p}_x \text{ y } \mathfrak{p}_x \subseteq \mathfrak{p}_y \cap A\} \qquad (*) \\ &= \{y \in \operatorname{Spec} B : (\mathfrak{p}_y \cap A) \cap (A \setminus \mathfrak{p}_x) = \emptyset \text{ y } \mathfrak{p}_x \subseteq \mathfrak{p}_y \cap A\} \\ &= \{y \in \operatorname{Spec} B : \mathfrak{p}_y \cap j((A \setminus \mathfrak{p}_x)) = \emptyset \text{ y } j(\mathfrak{p}_x) \subseteq \mathfrak{p}_y\} \\ &= \{y \in \operatorname{Spec} B_x : j(\mathfrak{p}_x) \subseteq \mathfrak{p}_y\} = \operatorname{Spec}(B_x/\mathfrak{p}_x \cdot B_x). \end{aligned}$$

Las dos afirmaciones siguientes de la proposición, se deducen de que en $(*)$ podemos prescindir de una de las dos condiciones, en la primera afirmación de la segunda condición y en la segunda afirmación de la primera condición.

□

Observemos que las fibras pueden ser vacías, pues si un anillo $C = 0$ entonces $\operatorname{Spec} C = \emptyset$.

44. Ejemplo: Calculemos $\operatorname{Spec} \mathbb{C}[x, y]$ usando la fórmula de la fibra. Consideremos el morfismo $i : \mathbb{C}[x] \to \mathbb{C}[x, y], p(x) \mapsto p(x)$ y sea $i^* : \operatorname{Spec} \mathbb{C}[x, y] \to \operatorname{Spec} \mathbb{C}[x]$ el morfismo inducido en los espectros. Cada punto de $\operatorname{Spec} \mathbb{C}[x, y]$ está en la fibra de un único punto de $\operatorname{Spec} \mathbb{C}[x]$, así que vamos a calcular tales fibras.

Los ideales primos de $\mathbb{C}[x]$ son el ideal (0) y los ideales maximales $\mathfrak{m}_\alpha = (x-\alpha)$. Según la fórmula de la fibra

$$i^{*-1}(\alpha) = \operatorname{Spec}\mathbb{C}[x,y]/\mathfrak{m}_\alpha\mathbb{C}[x,y] = \operatorname{Spec}\mathbb{C}[x,y]/(x-\alpha).$$

Ahora bien, $\mathbb{C}[x,y]/(x-\alpha) \simeq \mathbb{C}[y]$, $x \mapsto \alpha, y \mapsto y$. Luego,

$$i^{*-1}(\alpha) = \operatorname{Spec}\mathbb{C}[y] = \{(0), (y-\beta)\ \forall\, \beta \in \mathbb{C}\}$$

que se corresponden con los ideales primos de $\mathbb{C}[x,y]$, $\{(x-\alpha), (x-\alpha, y-\beta)\ \forall\, \beta \in \mathbb{C}\}$.

Solo nos falta calcular la fibra de $(0) = \mathfrak{p}_g$

$$i^{*-1}(g) = \operatorname{Spec}\mathbb{C}[x,y]_{\mathbb{C}[x]-\setminus(0)} = \operatorname{Spec}\mathbb{C}(x)[y]$$

Los ideales primos no nulos de $\mathbb{C}(x)[y]$ están generados por un polinomio irreducible con coeficientes en $\mathbb{C}(x)$ de grado mayor o igual que 1 en y. Por el lema de Gauss se corresponden con los polinomios $p(x,y) \in \mathbb{C}[x,y]$ irreducibles de grado mayor o igual que 1 en y. Por tanto, $i^{*-1}(g)$ está formado por los ideales primos $(p(x,y))$, (0) (donde $p(x,y)$ es un polinomio irreducible de grado mayor o igual que 1 en y)

En resumen, los puntos de $\operatorname{Spec}\mathbb{C}[x,y] \underset{\text{Not}}{=} \mathbb{A}_2(\mathbb{C})$ son

1. Los puntos cerrados (α,β), es decir, los ideales primos $(x-\alpha, y-\beta)$.
2. Los puntos genéricos de las curvas irreducibles $(p(x,y))_0 \equiv p(x,y) = 0$, es decir, los ideales primos $(p(x,y))$, $p(x,y)$ irreducible.
3. El punto genérico del plano afín $(0)_0 \equiv \mathbb{A}_2(\mathbb{C})$, es decir, el ideal primo (0).

45. Ejemplo: Calculemos $\operatorname{Spec}\mathbb{C}[x,y]/(q(x,y))$. Consideremos la descomposición en producto de polinomios irreducibles $q(x,y) = q_1(x,y)^{n_1}\cdots q_r(x,y)^{n_r}$, que no difieran en factores constantes. Tenemos que

$$\operatorname{Spec}\mathbb{C}[x,y]/(q(x,y)) = (q(x,y))_0 = \bigcup_{i=1}^{r} (q_i(x,y))_0$$

que son:

1. Los ideales maximales $(x-\alpha, y-\beta)$ tales que $(q(x,y)) \subseteq (x-\alpha, y-\beta)$. Es decir, con otras notaciones, los puntos (α,β) tales que $q(\alpha,\beta) = 0$.
2. Los puntos genéricos de las curvas irreducibles $q_i(x,y) = 0$.

46. Proposición: *Sea $f: A \hookrightarrow B$ un morfismo inyectivo de anillos. Entonces, la imagen del morfismo $f^*:$ Spec$B \to$ Spec$A$ es densa.*

Demostración. Sea $x \in$ Spec$A$ el punto genérico de una componente irreducible de Spec$A$ (es decir, $\mathfrak{p}_x$ es un ideal primo minimal de A). Por la fórmula de la fibra $f^{*-1}(x) =$ Spec$B_x \neq \emptyset$, porque $B_x \neq 0$, ya que $1 \neq 0$ en B_x. En conclusión, $x \in \mathrm{Im} f^*$ y $\overline{\mathrm{Im} f^*} =$ Spec$A$. □

0.5.2. Espectro primo y soluciones de un sistema de ecuaciones algebraicas

47. Teorema : *Sea $A = k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ una k-álgebra de tipo finito y k' una k-extensión de cuerpos algebraicamente cerrada y de grado de trascendencia mayor o igual que n. Dadas $\alpha = (\alpha_1,\ldots,\alpha_n), \beta = (\beta_1,\ldots,\beta_n) \in k'^n$, diremos que $\alpha \sim \beta$ si existe $\tau \in Aut_{k-alg}k'$, tal que*

$$\tau(\alpha) := (\tau(\alpha_1),\ldots,\tau(\alpha_n)) = \beta.$$

Se cumple que

$$\boxed{\mathrm{Spec}A = \{\alpha \in k'^n : p_1(\alpha) = \cdots = p_r(\alpha) = 0\}/\sim}$$

Demostración. Dado $[\alpha] \in \{\alpha \in k'^n : p_i(\alpha) = 0, \forall i\}/\sim$ le asignamos el ideal primo

$$\mathfrak{p}_\alpha := \{\bar{p} \in k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) : p(\alpha) = 0\}.$$

Demos la asignación inversa.

Dado un ideal primo $\mathfrak{p}_y \subset A$, sea $k(y) := (A/\mathfrak{p}_y)_y$ el cuerpo residual de y. Existe un morfismo $g: k(y) \hookrightarrow k'$ porque el cierre algebraico de $k(y)$ es igual al cierre algebraico de un cuerpo de funciones racionales en s variables, con $s = \mathrm{gr\,tr}_k\, k(y) \leq n$ y k' es igual al cierre algebraico de un cuerpo de funciones racionales en $m \geq n$ variables.

Veamos que dado otro morfismo $g': k(y) \to k'$ entonces existe $\tau \in Aut_{k-alg}k'$ tal que $g' = \tau \circ g$. Pensemos g' como una inclusión y sea $z_1,\ldots,z_s \in k'$ una base de k-trascendencia de $k(y)$. Componiendo g con un automorfismo τ' de k' podemos suponer que $z_i' := g(z_i)$ es igual a z_i, para todo $1 \leq i \leq s$. En efecto, sean $z_{s+1},\ldots,z_m \in k'$ y $z_{s+1}',\ldots,z_m' \in k'$ de modo que $z_1,\ldots,z_m$ y $z_1',\ldots,z_m'$ sean bases de trascendencia de k'. Sea $\sigma: k(z_1',\ldots,z_m') \to k(z_1,\ldots,z_m)$, definido por $\sigma(z_i') = z_i$, para todo i. Por toma de cierres algebraicos, el morfismo σ extiende al automorfismo $\tau': k' \to k'$ buscado. Sea ahora $h: k(y)(z_{s+1},\ldots,z_m) \to k'$ el morfismo definido por $h = g$ sobre $k(y)$ y $h(z_t) = z_t$, para todo $0 < t \leq m - s$. Hemos obtenido el cierre algebraico de $k(y)(z_{s+1},\ldots,z_m)$ vía la inclusión natural en k' y vía h. Por tanto existe un morfismo $\tau: k' \to k'$ tal que $\tau \circ h$ es

la inclusión natural. En particular, $\tau \circ g$ es el morfismo de inclusión natural g' de $k(y)$ en k'.

Denotemos por $\pi\colon A \to k(y)$ el morfismo natural, y sea $f = g \circ \pi\colon A \to k'$. A $\mathfrak{p}_y$ le asignamos $[(f(\bar{x}_1), \ldots, f(\bar{x}_m))]$.

Ambas asignaciones son inversas entre sí.

□

0.6. Módulos

Los espacios vectoriales son el ejemplo más sencillo y usual de espacio geométrico. Muchos problemas se resuelven linealizándolos, lo que permite aplicarles además la intuición geométrica. Añadamos, que muchas de las estructuras usuales en Matemáticas son estructuras de espacios vectoriales.

Si I es un ideal de un anillo A, es un grupo conmutativo respecto de la suma de A y el producto de A define una aplicación $A \times I \to I$ que verifica todos los axiomas de espacio vectorial, salvo la condición de que los escalares formen un cuerpo; lo que resumiremos diciendo que I es un A-módulo. En esta sección iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (subespacios, cocientes, sumas y productos directos, producto tensorial, etc.) pueden generalizarse para los A-módulos; aunque la frecuente existencia de módulos que no admiten bases introduzca grandes modificaciones en la teoría de módulos. La posibilidad de efectuar muchas operaciones (cocientes, sumas directas, productos tensoriales, etc.) que carecen de sentido en los ideales hace que la teoría de módulos sea mucho más flexible y natural, que una teoría restringida únicamente a los ideales. Esta generalidad no complica las demostraciones, sino que la posibilidad de usar las operaciones básicas del Álgebra Lineal las aclara y simplifica.

Los módulos aparecen también con frecuencia en Matemáticas. Ya veremos que los grupos abelianos y los espacios vectoriales con un endomorfismo lineal son ejemplos de módulos, y que su clasificación es la clasificación de la estructura de módulos.

Dadas por conocidas nociones definidas más adelante, digamos que el estudio de los módulos equivale en topología, al estudio de los fibrados vectoriales $\pi\colon E \to X$, es decir, de los epimorfismos continuos, de fibras espacios vectoriales. El estudio de π será equivalente al estudio del $C(X)$-módulo de las secciones de π.

0.6.1. Módulos, submódulos y cocientes. Sistema de generadores

1. Definición: Sea A un anillo y sea M un conjunto. Diremos que una operación $M \times M \xrightarrow{+} M$, $(m, m') \mapsto m + m'$ y una aplicación $A \times M \dot{\to} M, (a, m) \mapsto a \cdot m$ definen en M una estructura de A-módulo cuando cumplen

1. $(M, +)$ es un grupo conmutativo.
2. $a \cdot (m + n) = a \cdot m + a \cdot n$, para todo $a \in A$ y $m, n \in M$.
3. $(a + b) \cdot m = a \cdot m + b \cdot m$, para todo $a, b \in A$ y $m \in M$.
4. $(ab) \cdot m = a \cdot (b \cdot m)$, para todo $a, b \in A$ y $m \in M$.
5. $1 \cdot m = m$, para todo $m \in M$.

La aplicación $A \times M \dot{\to} M$, $(a, m) \mapsto a \cdot m$ define para cada $a \in A$ una aplicación $a\cdot : M \to M$, $m \mapsto a \cdot m$. El segundo punto expresa que $a\cdot$ es morfismo de grupos. Los tres últimos puntos expresan que la aplicación $\phi : A \to \mathrm{End}(M)$, $\phi(a) = a\cdot$, es morfismo de anillos (donde $\mathrm{End}(M)$ el conjunto de morfismos de grupos del grupo conmutativo M en sí mismo). Recíprocamente, si M es un grupo conmutativo, cada morfismo de anillos $\phi : A \to \mathrm{End}(M)$ define una estructura de A-módulo en M tal que $a \cdot m := \phi(a)(m)$.

2. Ejemplos:

1. Todo ideal $I \subset A$ es un A-módulo, pues con la suma definida en A y con el producto por los elementos de A ya definido en A, I tiene estructura de A-módulo. En particular, A es un A-módulo.
2. Si A es un cuerpo, entonces los A-módulos son los A-espacios vectoriales.
3. Si G es un grupo abeliano, entonces es un $\mathbb{Z}$-módulo de modo natural: $n \cdot g := g + \overset{n}{\dots} + g$ si $n \in \mathbb{N}^+$, $n \cdot g := (-g) + \overset{-n}{\dots} + (-g)$ si $-n \in \mathbb{N}^+$, y definimos $0 \cdot g := 0$. Recíprocamente, si G es un $\mathbb{Z}$-módulo, en particular es un grupo abeliano.
4. Si $T : E \to E$ es un endomorfismo de k-espacios vectoriales entonces E tiene estructura natural de $k[x]$-módulo: $(\sum \lambda_i x^i) \cdot e := \sum \lambda_i T^i(e)$. Recíprocamente, dado un $k[x]$-módulo E, la aplicación $T : E \to E$ definida por $T(e) = x \cdot e$, es un endomorfismo de k-espacios vectoriales.
5. Sea $\{M_i\}_{i \in I}$ una familia de A-módulos con índices en un conjunto I. Su producto directo se denotará $\prod_{i \in I} M_i$, mientras que $\bigoplus_{i \in I} M_i$ denotará el subconjunto de $\prod_{i \in I} M_i$ formado por los elementos (m_i) que tienen todas sus componentes nulas salvo

un número finito de ellas, y se llamará suma directa de los $\{M_i\}_{i\in I}$. Tanto $\prod_{i\in I} M_i$ como $\oplus_{i\in I} M_i$ son A-módulos con la siguiente suma y producto por elementos de A:

$$(m_i)_{i\in I} + (m'_i)_{i\in I} := (m_i + m'_i)_{i\in I}$$
$$a\cdot(m_i)_{i\in I} := (a\cdot m_i)_{i\in I}$$

3. Notación: Alguna vez, escribiremos am en vez de $a\cdot m$ por sencillez de escritura.

4. Definición: Un subconjunto N de un A-módulo M, decimos que es un submódulo si con la operación + de M y con la multiplicación $\cdot$ por elementos de A, es un A-módulo.

Un subconjunto no vacío $N\subseteq M$ es un submódulo si y solo si para todo $n,n'\in N$ y $a\in A$ se cumple que $a\cdot n+n'\in N$.

5. Ejemplos: Los K-subespacios vectoriales de un K-espacio vectorial E son justamente los K-submódulos de E.

Los ideales de un anillo A son justamente los A-submódulos de A.

Los subgrupos de un grupo abelieano G son justamente los $\mathbb{Z}$-submódulos de G.

Dado un endomorfismo k-lineal $T: E\to E$, los subespacios vectoriales $E'\subseteq E$ estables por T ($T(E')\subseteq E'$) son justamente los $k[x]$-submódulos de E.

$\oplus_{i\in I} M_i$ es un submódulo de $\prod_{i\in I} M_i$.

6. Definición: Una aplicación $f: M\to M'$ entre A-módulos M,M', diremos que es un morfismo de A-módulos si cumple

1. $f(m+n)=f(m)+f(n)$, para todo $m,n\in M$.
2. $f(am)=af(m)$, para todo $a\in A$ y $m\in M$.

Cuando $f: M\to M'$ sea biyectiva diremos que f es un isomorfismo de A-módulos.

7. Ejemplos: 1. Sea M un A-módulo y $a\in A$. La aplicación $a\cdot M\to M$, $m\mapsto a\cdot m$ es un morfismo de A-módulos.

2. Sean G y G' dos grupos abelianos, es decir, dos $\mathbb{Z}$-módulos. Una aplicación $f: G\to G'$ es un morfismo de grupos si y solo si es un morfismo de $\mathbb{Z}$-módulos, y f es un isomorfismo de grupos si y solo si f es un isomorfismo de $\mathbb{Z}$-módulos.

3. Sean $T: E\to E$ y $T': E'\to E'$ dos endomorfismos k-lineales, es decir, E y E' son dos $k[x]$-módulos. Una aplicación lineal $\phi: E\to E'$ es un morfismo de $k[x]$-módulos si

y solo si $\phi \circ T = T' \circ \phi$, es decir, el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ E' & \xrightarrow[T']{} & E' \end{array}$$

es conmutativo. En efecto, si ϕ es morfismo de $k[x]$-módulos

$$(\phi \circ T)(e) = \phi(T(e)) = \phi(x \cdot e) = x \cdot \phi(e) = T'(\phi(e)) = (T' \circ \phi)(e)$$

para todo $e \in E$. Recíprocamente, si $\phi \circ T = T' \circ \phi$, entonces $\phi(x \cdot e) = \phi(T(e)) = T'(\phi(e)) = x \cdot \phi(e)$, para todo $e \in E$. Por tanto, $\phi(x^2 \cdot e) = x \cdot \phi(x \cdot e) = x^2 \cdot \phi(e)$, recurrentemente obtenemos que $\phi(x^n \cdot e) = x^n \cdot \phi(e)$ y por k-linealidad tenemos que $\phi(p(x) \cdot e) = p(x) \cdot \phi(e)$ para todo $p(x) \in k[x]$ y todo $e \in E$. Es decir, ϕ es un morfismo de $k[x]$-módulos.

Dado un isomorfismo k-lineal $\varphi : E \to V$, podemos definir un endomorfismo k-lineal (único) $S : V \to V$ tal que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\varphi}\downarrow\wr & & \wr\downarrow{\scriptstyle\varphi} \\ V & \xrightarrow[S]{} & V \end{array}$$

es conmutativo. En efecto, $S = \varphi \circ T \circ \varphi^{-1}$. Diremos que T y S son equivalentes.

Por tanto, T y T' son equivalentes si y solo si existe un isomorfismo de $k[x]$-módulos $\phi : E \to E'$.

Veamos que T y T' son equivalentes si y solo si existen bases $\{e_i\}$ en E y $\{e'_j\}$ en E' de modo que la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{e'_j\}$: Consideremos un isomorfismo k-lineal $\phi : E \to E'$, de modo que $\phi \circ T = T' \circ \phi$. Sea $\{e_i\}$ una base cualquiera de E. Entonces, $\{\phi(e_i)\}$ es una base de E' y la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{\phi(e_i)\}$. Sea $\{e_i\}_{i \in I}$ una base de E y $\{e'_j\}_{j \in J}$ una base de E' de modo que la matriz de T en la base $\{e_i\}_{i \in I}$ es igual a la matriz de T' en la base $\{e'_j\}_{j \in J}$. Implícitamente se está suponiendo que $I = J$. Entonces, el endomorfismo $\phi : E \to E'$ que cumple que $\phi(e_i) := e'_i$ es un isomorfismo k-lineal tal que $\phi \circ T = T' \circ \phi$.

8. Notación: Denotaremos por $\mathrm{Hom}_A(M,N)$ al conjunto de morfismos de A-módulos de M en N.

Con las definiciones de suma de morfismos y producto por elementos de A naturales:

$$(f+g)(m) := f(m) + g(m)$$
$$(af)(m) := a(f(m))$$

tenemos que $\mathrm{Hom}_A(M,N)$ es un A-módulo.

9. Definición: El conjunto de los elementos de un módulo M, que por un morfismo de A-módulos $f: M \to M'$ van al cero, se denomina núcleo de f y se denota por $\mathrm{Ker}\, f$.

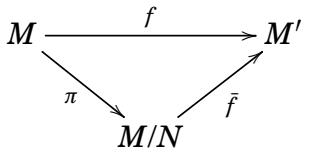
$\mathrm{Ker}\, f$ es un submódulo de M y $f(m_1) = f(m_2)$ si y solo si $m_2 \in m_1 + \mathrm{Ker}\, f$. Por tanto, f es inyectiva si y solo si $\mathrm{Ker}\, f = 0$. El conjunto de los elementos de la imagen, $\mathrm{Im}\, f$, forman un submódulo de M'.

Si N es un submódulo de M entonces es un subgrupo conmutativo de M. Por tanto, podemos considerar el grupo cociente M/N: Si denotamos $\bar{m} = m + N$, entonces

$$M/N = \{\bar{m},\ m \in M\}$$

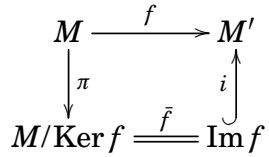
y $\bar{m} = \bar{m'} \iff m - m' \in N$. El producto $a \cdot \bar{m} := \overline{a \cdot m}$ dota a M/N de estructura de A-módulo (compruébese) y es la única estructura de A-módulo que podemos definir en M/N, de modo que el morfismo de paso al cociente $M \to M/N$, $m \mapsto \bar{m}$, sea un morfismo de módulos.

10. Teorema: *Sea $f: M \to M'$ un morfismo de A-módulos. Sea $N \subseteq \mathrm{Ker}\, f$ un A-submódulo. Existe un único morfismo $\bar{f}: M/N \to M'$ (que vendrá definido por $\bar{f}(\bar{m}) = f(m)$) de modo que el diagrama*



es conmutativo, siendo π el morfismo de paso al cociente.

11. Teorema de isomorfía: *Sea $f: M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*



donde $\pi(m) = \bar{m}$, $\bar{f}(\bar{m}) = f(m)$ (que está bien definida) e $i(m') = m'$, es conmutativo, $\bar{f}$ es un isomorfismo, π es epiyectiva e i inyectiva.

Demostración. Al lector. □

Dado un conjunto $\{M_i\}_{i \in I}$ de submódulos de M denotaremos

$$\sum_{i \in I} M_i = \{m \in M : m = \sum_{i \in I} m_i \text{ con } m_i \in M_i \text{ nulos para casi todo } i \in I\}$$

que es el menor submódulo de M que contiene a los submódulos M_i. Diremos que dos submódulos M_1, M_2 de M están en suma directa si $M_1 \cap M_2 = 0$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo. Se dice que M es la suma directa de dos submódulos M_1, M_2 si $M_1 \cap M_2 = 0$ y $M_1 + M_2 = M$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo.

Dado un conjunto $\{m_i\}_{i\in I}$ de elementos de un módulo M, denotaremos por

$$\langle m_i\rangle_{i\in I} = \{m \in M : m = \sum_{i\in I} a_i m_i, \text{ con } a_i = 0 \text{ para todo } i \text{ salvo un número finito}\}$$

que es el menor submódulo de M que contiene a $\{m_i\}_{i\in I}$. Diremos que $\{m_i\}_{i\in I}$ es un sistema generador de M si $\langle m_i\rangle_{i\in I} = M$. Evidentemente, todo módulo tiene sistemas generadores, por ejemplo el formado por todos los elementos de M. Si I es además finito diremos que el módulo es finito generado. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M, si es un sistema generador y si $\sum_i a_i m_i = 0$ entonces $a_i = 0$ para todo i.

Denotaremos $M^{(I)} = \bigoplus_{i\in I} M_i$, siendo $M_i = M$. Se dice que un módulo es libre si es isomorfo a $A^{(I)}$. Si denotamos $1_j = (a_i)_{i\in I} \in A^{(I)}$, donde $a_i = 0$ para todo $i \neq j$ y $a_j = 1$, entonces $\{1_j\}_{j\in I}$ forma una base de $A^{(I)}$. Los morfismos de $A^{(I)}$ en un A-módulo M se corresponden con conjuntos $\{m_i\}_{i\in I}$ de M: $\mathrm{Hom}_A(A^{(I)}, M) = \prod^I M$, $f \mapsto (f(1_i))_{i\in I}$. Sea $\{m_i\}_{i\in I}$ un conjunto de elementos de M, y definamos el morfismo

$$\phi : A^{(I)} \to M, (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i.$$

Se cumple que ϕ es epiyectivo si y solo si $\{m_i\}_{i\in I}$ es un sistema generador de M, ϕ es inyectivo si y solo si $\{m_i\}_{i\in I}$ son linealmente independientes. Por tanto, ϕ es isomorfismo si y solo si $\{m_i\}_{i\in I}$ es una base de M. En consecuencia, todo módulo es cociente de un libre y un módulo es libre si y solo si tiene bases.

Sea, pues, un epimorfismo $\pi : A^{(I)} \to M$. Igualmente, dado $\mathrm{Ker}\,\pi$ podemos definir un epimorfismo $A^{(J)} \to \mathrm{Ker}\,\pi$. Componiendo este último morfismo con la inclusión natural $\mathrm{Ker}\,\pi \hookrightarrow A^{(I)}$, tenemos un morfismo natural $s : A^{(J)} \to A^{(I)}$, y la sucesión de morfismos

$$A^{(J)} \xrightarrow{s} A^{(I)} \xrightarrow{\pi} M.$$

Por el teorema de isomorfía, $M \simeq A^{(I)}/\mathrm{Ker}\,\pi = A^{(I)}/\mathrm{Im}\,s$ Por tanto, el estudio de M se reduce al estudio de s, que es una aplicación A-lineal entre módulos libres.

El lema de Nakayama nos va a permitir calcular, mediante Álgebra Lineal, sistemas generadores.

Si M es un A-módulo e $I \subseteq A$ es un ideal, denotaremos por $I \cdot M = \{m \in M : m = \sum a_i m_i$, con $a_i \in I$ y $m_i \in M\}$, que es un A-submódulo de M. Se cumple que el A-módulo M/IM es de modo natural un A/I-módulo: $\bar{a} \cdot \bar{m} := a \cdot \bar{m}$. Es obvio que $M' \subseteq M/IM$ es un A-submódulo de M/IM, si y solo si es un A/I-submódulo, y que $\bar{m}_1, \ldots, \bar{m}_r \in M/IM$ es un sistema A-generador de M/IM si y solo si es un sistema A/I-generador de M/IM. En el caso de que $I = \mathfrak{m}$ sea un ideal maximal, tendremos que $\bar{m}_1, \ldots, \bar{m}_r \in M/\mathfrak{m}M$ es un sistema A-generador de $M/\mathfrak{m}M$ si y solo si es un sistema generador del $A/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}M$.

12. Lema de Nakayama: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y M un módulo finito generado. Se cumple que*

$$\mathfrak{m}M = M \iff M = 0$$

Como consecuencia se obtiene que $m_1, \ldots, m_n \in M$ es un sistema generador de M si sus clases $\bar{m}_1, \ldots, \bar{m}_n$ en $M/\mathfrak{m}M$ son un sistema generador.

Demostración. $\Rightarrow$) Sea $n_1, \ldots, n_r$ un sistema generador de M con el menor número posible de elementos. Si $\mathfrak{m}M = M$ tendremos que $n_1 = \sum_{i=1}^{r} a_i n_i$, con $a_i \in \mathfrak{m}$. Entonces $(1 - a_1)n_1 = \sum_{i=2}^{r} a_i n_i$. Como $(1 - a_1)$ no se anula en el único ideal maximal de $\mathcal{O}$, es invertible. Por tanto, $n_1 = \frac{\sum_{i=2}^{r} a_i n_i}{1 - a_1}$, y $\langle n_2, \ldots, n_r \rangle = M$, lo que es contradictorio salvo que $r = 0$, es decir, $M = 0$.

$\Leftarrow$) Es obvio.

Veamos la consecuencia. Si $\langle \bar{m}_1, \ldots, \bar{m}_n \rangle = M/\mathfrak{m}M$ entonces $M = \langle m_1, \ldots, m_n \rangle + \mathfrak{m}M$. Haciendo cociente por $\langle m_1, \ldots, m_n \rangle$ y denotando $\bar{M} = M/\langle m_1, \ldots, m_n \rangle$, tenemos $\bar{M} = 0 + \mathfrak{m}\bar{M}$. Por tanto, $\bar{M} = 0$, es decir, $M = \langle m_1, \ldots, m_n \rangle$.

□

13. Proposición: *Si $A^{(I)}$ es un A-módulo isomorfo a $A^{(J)}$ entonces I y J son conjuntos que tienen el mismo cardinal.*

Demostración. Si A fuese un cuerpo, este resultado sería conocido, porque el cardinal de I sería igual a la dimensión de $A^{(I)}$ que coincidiría con la dimensión de $A^{(J)}$, que sería igual al cardinal de J.

Sea $\mathfrak{m}$ un ideal maximal de A. Entonces, $A^{(I)}/\mathfrak{m} \cdot A^{(I)} = A^{(I)}/\mathfrak{m}^{(I)} = (A/\mathfrak{m})^{(I)}$ es un $A/\mathfrak{m}$-espacio vectorial de dimensión el cardinal I. Igualmente, $A^{(J)}/\mathfrak{m} \cdot A^{(J)}$ es un $A/\mathfrak{m}$-espacio vectorial de dimensión el cardinal J. Por último, observemos que $A^{(I)}/\mathfrak{m} \cdot A^{(I)}$ es isomorfo a $A^{(J)}/\mathfrak{m} \cdot A^{(J)}$.

□

0.6.2. Localización de módulos

Sea S un sistema multiplicativo de un anillo A y M un A-módulo. Podemos definir en el conjunto $M \times S$ la siguiente relación de equivalencia:

$$(m,s) \sim (m',s') \iff \text{ existen } s_1, s_2 \in S \text{ tales que } (s_1 m, s_1 s) = (s_2 m', s_2 s').$$

Denotaremos $\frac{m}{s}$ a la clase de equivalencia de (m,s). Observemos que $\frac{m}{s} = \frac{m'}{s'}$ si y solo si existen $s_1, s_2 \in S$ tales que $(s_1 m, s_1 s) = (s_2 m', s_2 s')$.

14. Definición: Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$M_S = \{\frac{m}{s},\ \forall\ m \in M, s \in S\}$$

y diremos que M_S es la localización de M por el sistema multiplicativo S.

Para definir una aplicación $f : M_S \to X$, tenemos que asignar a cada $\frac{m}{s} \in M_S$ un elemento $\phi(m,s)$, de modo que $\phi(tm,ts) = \phi(m,s)$, para todo $t \in S$.

Con las operaciones (bien definidas)

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$$
$$\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$$

M_S tiene estructura de A_S-módulo. La aplicación canónica

$$M \to M_S,\ m \mapsto \frac{m}{1}$$

es un morfismo de A-módulos y diremos que es el morfismo de localización.

15. Ejercicio: Pruébese que $\frac{m}{s} = 0$ si y solo sí existe un $t \in S$ de modo que $t \cdot m = 0$.

16. Ejercicio: Pruébese que $\frac{m}{s} = \frac{m'}{s'}$ si y solo si existe $t \in S$ tal que $t \cdot (s'm - sm') = 0$.

Todo morfismo $f : M \to N$ de A-módulos, induce la aplicación (bien definida)

$$f_S : M_S \to N_S, \frac{m}{s} \underset{\text{def}}{\mapsto} \frac{f(m)}{s},$$

que es morfismo de A_S-módulos. Es inmediato comprobar que la localización de morfismos es compatible con composiciones y combinaciones A-lineales:

$$(f \circ g)_S = f_S \circ g_S$$
$$(af + bg)_S = af_S + bg_S$$

17. Proposición: *Dado un morfismo $f : M \to N$ de A-módulos y S un sistema multiplicativo de A, se cumple que*

$$(\operatorname{Ker} f)_S = \operatorname{Ker} f_S \ \ y \ \ (\operatorname{Im} f)_S = \operatorname{Im} f_S.$$

Demostración. El morfismo $(\operatorname{Ker} f)_S \to M_S$, $\frac{m}{s} \mapsto \frac{m}{s}$ valora en $\operatorname{Ker} f_S$, pues $f_S(\frac{m}{s}) = \frac{f(m)}{s} = \frac{0}{s} = 0$ (para todo $m \in \operatorname{Ker} f$ y todo $s \in S$). Tenemos que comprobar que el morfismo $(\operatorname{Ker} f)_S \to \operatorname{Ker} f_S$, $\frac{m}{s} \mapsto \frac{m}{s}$ es un isomorfismo.

Inyectivo: si $\frac{m}{s} = 0$ en $\operatorname{Ker} f_S \subseteq M_S$ entonces existe un $s' \in S$ de modo que $s'm = 0$, luego $\frac{m}{s} = 0$ en $(\operatorname{Ker} f)_S$. Epiyectivo: Dado $\frac{m}{s}$ en $\operatorname{Ker} f_S$, entonces $f_S(\frac{m}{s}) = 0$, luego $\frac{f(m)}{s} = 0$. Por tanto, existe un $s' \in S$ de modo que $s'f(m) = 0$, es decir, $f(s'm) = 0$. Luego $\frac{m}{s} = \frac{s'm}{s's}$ con $s'm \in \operatorname{Ker} f$ y concluimos la epiyectividad.

Dejamos como ejercicio el probar que $(\operatorname{Im} f)_S = \operatorname{Im} f_S$. □

Una consecuencia de esta proposición es que la localización respeta los morfismos inyectivos y epiyectivos.

18. Definición: Diremos que una sucesión de morfismos de A-módulos

$$\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \cdots$$

es exacta cuando $\operatorname{Im} f_n = \operatorname{Ker} f_{n+1}$ para todo n.

Casos concretos:

1. $0 \to N \xrightarrow{i} M$ es una sucesión exacta si y solo si i es inyectiva.
2. $M \xrightarrow{\pi} M'' \to 0$ es una sucesión exacta si y solo si π es un epimorfismo.
3. $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ es exacta si y solo si i es inyectiva, π es epiyectiva y $\operatorname{Ker} \pi = \operatorname{Im} i$.

Observemos que $\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \cdots$ es exacta si y solo si las sucesiones $0 \to \operatorname{Im} f_{n-1} \to M_n \to \operatorname{Im} f_n \to 0$ son exactas, para todo n,

19. Proposición: *Sea S un sistema multiplicativo de A y sea*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

una sucesión exacta de A-módulos. Entonces es exacta la sucesión

$$M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$$

Demostración. Si $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión exacta de A-módulos entonces $\operatorname{Ker} g = \operatorname{Im} f$. Entonces $\operatorname{Ker} g_S = (\operatorname{Ker} g)_S = (\operatorname{Im} f)_S = \operatorname{Im} f_S$ (explícitamente, $\frac{m}{s} \mapsto \frac{m}{s}$) y por lo tanto ${M'}_S \xrightarrow{f_S} M_S \xrightarrow{g_S} {M''}_S$ es exacta. □

20. Ejercicio: Prueba las igualdades:

1. $(M/N)_S = M_S/N_S$.
2. $(M \oplus N)_S = M_S \oplus N_S$.
3. $(M+N)_S = M_S + N_S$.
4. $(M \cap N)_S = M_S \cap N_S$.

Uno de los procesos geométricos más básicos es el de localizar la atención en un entorno de un punto. Una propiedad es local cuando solo depende del comportamiento en un entorno de cada punto. Por ejemplo, la continuidad de las funciones consideradas en Topología, la derivabilidad de las funciones consideradas en Análisis, la conexión local o compacidad local de los espacios topológicos, etc., son propiedades locales. Por el contrario, una propiedad es global cuando no es local, es decir, depende de todo el espacio considerado. Por ejemplo el concepto de función acotada no es local, ni el de espacio compacto o conexo.

Un resultado central de esta subsección será demostrar que la anulación de un módulo es una cuestión local y que por tanto, también son locales todos los problemas que puedan reducirse a la anulación de un módulo.

21. Definición: Sea M un A-módulo, llamaremos anulador de M al ideal

$$\operatorname{Anul}(M) := \{a \in A : am = 0, \text{ para todo } m \in M\}.$$

Dicho de otro modo, el anulador de M es el núcleo del morfismo de estructura $A \to \operatorname{End}(M)$, $a \mapsto a\cdot$. Se dice que M es un A-módulo fiel si $\operatorname{Anul}(M) = 0$, es decir, si el morfismo $A \to \operatorname{End}(M)$ es inyectivo. Todo A-módulo M es de modo natural un $A/\operatorname{Anul}(M)$-módulo fiel (donde $\bar{a} \cdot m := am$).

Dado un elemento $m \in M$, llamaremos anulador de $m \in M$ al ideal anulador del módulo $\langle m \rangle = \{am, a \in A\}$. Es decir, el ideal anulador de m es

$$\operatorname{Anul}(m) = \{a \in A : am = 0\}.$$

El epimorfismo de A-módulos $A \to \langle m \rangle$, $a \mapsto am$, tiene de núcleo el ideal anulador de m. Por tanto, por el teorema de isomorfía $A/\operatorname{Anul}(m) \simeq \langle m \rangle$.

Igual que hacíamos para los anillos, dada $f \in A$ denotaremos M_f a la localización de M por el sistema multiplicativo $S = \{1, f, f^2, \ldots\}$. Dado un ideal primo $\mathfrak{p}_x \subset A$ denotaremos por M_x a la localización de M por el sistema multiplicativo $S = A \setminus \mathfrak{p}_x$.

22. Definición: Llamaremos soporte de un A-módulo M, al subespacio de $\operatorname{Spec} A$ formado por los puntos x donde $M_x \neq 0$ y lo denotaremos por $\operatorname{Sop}(M)$, i.e.,

$$\operatorname{Sop}(M) = \{x \in \operatorname{Spec} A : M_x \neq 0\}.$$

23. Teorema: *El soporte de un A-módulo finito generado coincide con los ceros de su ideal anulador, i.e.,*

$$\operatorname{Sop} M = (\operatorname{Anul} M)_0.$$

Como consecuencia se tiene que la condición necesaria y suficiente para que un módulo M (finito generado o no) sea cero es que $M_x = 0$, para todo punto cerrado $x \in \operatorname{Spec} A$.

Demostración. Empecemos probando que si $M = \langle m_1, \ldots, m_r \rangle$ es un A-módulo finito generado, entonces $M_S = 0$ si y solo si existe un $s \in S$ de modo que $sM = 0$: Si $M_S = 0$ entonces $\frac{m_i}{1} = 0$ para todo i, luego existen $s_i \in S$ de modo que $s_i m_i = 0$. Por tanto, $s = s_1 \cdots s_r \in S$ cumple que $sM = 0$. Recíprocamente, si existe $s \in S$ de modo que $sM = 0$, entonces $\frac{m}{s'} = 0$ para todo $\frac{m}{s'} \in M_S$ y $M_S = 0$.

Ahora ya, dado $x \in \operatorname{Spec} A$, tendremos que $M_x \neq 0$ si y solo si $\operatorname{Anul}(M) \cap (A \setminus \mathfrak{p}_x) = \emptyset$, es decir, $\operatorname{Anul}(M) \subseteq \mathfrak{p}_x$. Luego $\operatorname{Sop}(M) = (\operatorname{Anul} M)_0$.

Por último, veamos la consecuencia. Probemos solo la suficiencia. Si $M_x = 0$ para todo punto cerrado $x \in \operatorname{Spec} A$, entonces para todo submódulo $\langle m \rangle \subseteq M$ se cumple que $\langle m \rangle_x = 0$. Por tanto, el $(\operatorname{Anul}\langle m \rangle)_0$, no contiene ningún punto cerrado de $\operatorname{Spec} A$, es decir, $\operatorname{Anul}\langle m \rangle$ no está contenido en ningún ideal maximal. En conclusión, $\operatorname{Anul}(\langle m \rangle) = A$, luego $m = 1 \cdot m = 0$ y $M = 0$.

□

24. Proposición:

1. *Una inclusión $N \subseteq M$ de módulos es una igualdad si y solo si $N_x = M_x$, para todo punto cerrado $x \in \operatorname{Spec} A$.*

2. *Dos submódulos N, N' de un módulo M son iguales si y solo si $N_x = N'_x$, para todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración. 1. $N = M \iff M/N = 0 \iff (M/N)_x = 0$, para todo punto cerrado $x \in \operatorname{Spec} A \iff M_x/N_x = 0$ para todo punto cerrado $x \in \operatorname{Spec} A \iff M_x = N_x$, para todo punto cerrado $x \in \operatorname{Spec} A$.

2. Veamos solo que si $N_x = N'_x$, para todo punto cerrado $x \in \operatorname{Spec} A$, entonces $N = N'$. Tendremos que $N_x = N_x + N'_x = (N + N')_x$, para todo punto cerrado $x \in \operatorname{Spec} A$. Luego por el punto 1. $N = N + N'$, es decir, $N' \subseteq N$. Del mismo modo obtenemos la inclusión inversa y concluimos la igualdad.

□

25. Teorema : *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión de morfismos de A-módulos. Las siguientes condiciones son equivalentes*

1. *$M' \xrightarrow{f} M \xrightarrow{g} M''$ es una sucesión exacta.*
2. *$M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$ es exacta para todo punto $x \in \operatorname{Spec} A$.*
3. *$M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$ es exacta para todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración. La implicación 1 $\Rightarrow$ 2 es un caso particular de 0.6.19. La implicación 2 $\Rightarrow$ 3 es evidente.

Veamos que 3 $\Rightarrow$ 1. Si la sucesión es exacta en todo punto cerrado x entonces $\operatorname{Ker} g_x = \operatorname{Im} f_x$. Luego $(\operatorname{Ker} g)_x = (\operatorname{Im} f)_x$. Por tanto, por la proposición anterior, $\operatorname{Ker} g = \operatorname{Im} f$ y la sucesión del punto 1. es exacta. □

Como corolario, dado que los morfismos inyectivos y epiyectivos son casos concretos de sucesiones exactas, tendremos que un morfismo es inyectivo (o epiyectivo) si y solo si lo es localmente, para todo punto cerrado del espectro del anillo.

26. Proposición : *Sean S y S' dos sistemas multiplicativos de A y denotemos por $SS' = \{ss', \forall s \in S, \forall s' \in S'\}$. Entonces, $(A_S)_{S'} = A_{SS'}$ y $\operatorname{Spec}(A_S)_{S'} = \operatorname{Spec} A_S \cap \operatorname{Spec} A_{S'}$.*

Demostración. Los morfismos (bien definidos) $(A_S)_{S'} \to A_{SS'}$, $\frac{\frac{a}{s}}{s'} \mapsto \frac{a}{ss'}$, $A_{SS'} \to (A_S)_{S'}$, $\frac{a}{ss'} \mapsto \frac{\frac{a}{s}}{s'}$ son inversos entre sí.

Por último, $\operatorname{Spec}(A_S)_{S'} = \operatorname{Spec} A_{SS'} = \operatorname{Spec} A_S \cap \operatorname{Spec} A_{S'}$. □

27. Teorema: *Sea M un A-módulo finito generado cuyo soporte es igual a un número finto de puntos cerrados $\{x_1, \ldots, x_n\}$. Entonces, el morfismo natural*

$$M \to M_{x_1} \times \cdots \times M_{x_n}, m \mapsto (\frac{m}{1}, \ldots, \frac{m}{1})$$

es un isomorfismo.

Demostración. Sea $I = \mathrm{Anul}(M)$, entonces M es un A/I-módulo y $\mathrm{Spec}\, A/I = \{x_1, \ldots, x_n\}$. Observemos que si $S \subset A$ es un sistema multiplicativo y $\bar{S}$ es la imagen de S por el morfismo de paso al cociente $A \to A/I$, entonces el morfismo $M_S \to M_{\bar{S}}$, $\frac{m}{s} \mapsto \frac{m}{\bar{s}}$ es un isomorfismo. Por tanto, podemos suponer que $A = A/I$. Observemos que $(M_{x_i})_{x_j} = 0$ si $x_i \neq x_j$, porque $(A_{x_i})_{x_j} = 0$ ya que su espectro es vacío. Obviamente, $(M_{x_i})_{x_i} = M_{x_i}$. El morfismo del enunciado es un isomorfismo porque localmente lo es. □

Si U es un abierto de $\mathrm{Spec}\, A$, denotaremos por A_U la localización de A por el sistema multiplicativo de las funciones que no se anulan en ningún punto de U. Probemos el recíproco de 0.5.29.

28. Proposición: *Si* $\mathrm{Spec}\, A$ *es la unión disjunta de dos abiertos* U_1, U_2 *entonces* $A = A_{U_1} \times A_{U_2}$.

Demostración. Veamos que $\mathrm{Spec}\, A_{U_1} = U_1$ (igualmente $\mathrm{Spec}\, A_{U_2} = U_2$). $U_1 \subseteq \mathrm{Spec}\, A_{U_1}$, porque las funciones del sistema multiplicativo por las que localizamos no se anulan en ningún punto de U_1. Por otra parte, U_1 y U_2 son cerrados disjuntos. Si denotamos I_i al ideal de funciones que se anulan en U_i tenemos que $(I_1)_0 \cap (I_2)_0 = \emptyset$, por tanto $(I_1 + I_2)_0 = \emptyset$ y $I_1 + I_2 = A$. Así pues, existen $f_i \in I_i$, tales que $f_1 + f_2 = 1$. En conclusión, $f_2 = 1 - f_1$ es una función que se anula en todo los puntos de U_2 y no se anula en ningún punto de U_1, por tanto $\mathrm{Spec}\, A_{U_1} \subseteq U_1$ y $\mathrm{Spec}\, A_{U_1} = U_1$.

Consideremos el morfismo natural

$$A \to A_{U_1} \times A_{U_2}, \quad a \mapsto (\frac{a}{1}, \frac{a}{1})$$

Vamos a probar que este morfismo es isomorfismo. Por el teorema anterior, basta verlo localmente. Dado $x \in U_1$, tenemos que $(A_{U_1})_x = (A_x)_{U_1} = A_x$ porque el sistema multiplicativo de las funciones que no se anulan en U_1, está incluido en el sistema multiplicativo de las funciones que no se anulan en x. Por otra parte, $\mathrm{Spec}(A_{U_2})_x = \emptyset$, porque $U_2 \cap \{y \in \mathrm{Spec}\, A : \mathfrak{p}_y \subseteq \mathfrak{p}_x, i.e., x \in \bar{y}\} = \emptyset$, luego $(A_{U_2})_x = 0$. En conclusión, $A_x = (A_{U_1} \times A_{U_2})_x$ si $x \in U_1$, e igualmente si $x \in U_2$. Hemos terminado.

□

29. Definición: Llamamos radical de Jacobson de un anillo al ideal que es la intersección de todos los ideales primos maximales del anillo.

30. Corolario: *Sea* A *un anillo e* $I \subset A$ *un ideal incluido en el radical de Jacobson de* A. *Sea* M *un* A*-módulo finito generado. Se cumple que*

$$M = IM \iff M = 0.$$

Demostración. $M = IM \iff M_x = I_x M_x$ para todo punto cerrado $x \in \operatorname{Spec} A$, e igualmente $M = 0 \iff M_x = 0$ para todo punto cerrado $x \in \operatorname{Spec} A$. Ahora bien, $I_x \subseteq \mathfrak{p}_x A_x$ y por el lema de Nakayama concluimos trivialmente que $M_x = I_x M_x \iff M_x = 0$. Con todo, hemos terminado. □

0.6.3. Anillos y módulos noetherianos

En Geometría Algebraica, los espacios estudiados son objetos definidos por un número finito de ecuaciones (la finitud es una condición natural). Es decir, los ideales que se consideran son los generados por un número finito de funciones. Los anillos cuyos ideales son finito generados se denominan noetherianos. Como veremos los anillos que usualmente aparecen en Geometría Algebraica y la Aritmética son noetherianos, de forma que estos anillos proporcionan el marco natural para desarrollar su estudio.

La introducción de los módulos la justificábamos con diversas razones. La primera que dábamos es que los ideales son módulos. Decíamos además que las operaciones básicas como producto tensorial, cocientes etc., se realizan de un modo mucho más flexible y claro con los módulos, y que muchos de los objetos usuales en Matemáticas tienen estructura de módulo. De nuevo, será natural comenzar estudiando los módulos finito generados, cuyos submódulos sean finito generados, en vez de limitarnos simplemente a los anillos cuyos ideales son finito generados.

31. Definición: Un A-módulo M se dice que es un A-módulo noetheriano si todo submódulo suyo (propio o no) es finito generado.

32. Definición: Un A-módulo M se dice que es noetheriano si toda cadena ascendente de submódulos de M

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

estabiliza, es decir existe $r >> 0$ de modo que $M_r = M_{r+1} = \cdots$.

33. Proposición: *Las dos definiciones anteriores son equivalentes.*

Demostración. $\mathbf{def}^1 \Rightarrow \mathbf{def}^2$: Dada una cadena ascendente de submódulos de M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$, sea $M' = \bigcup_{i=1}^{\infty} M_i \subseteq M$. Como M' es un submódulo de M, es finito generado. Escribamos $M' = \langle m_1, \ldots, m_r \rangle$, con $m_j \in M_{i_j}$. Si r es el máximo de todos los i_j, $M' = M_r$, luego $M_r = M_{r+1} = \cdots$.

$\mathbf{def}^2 \Rightarrow \mathbf{def}^1$: Sea $M' \subseteq M$. Sea $m_1 \in M'$ y consideremos el submódulo de M, $M_1 = \langle m_1 \rangle$. Si $M_1 \neq M'$, sea $m_2 \in M' \backslash M_1$. Consideremos el submódulo de M, $M_2 = \langle m_1, m_2 \rangle$. Repitiendo el proceso, obtenemos una cadena de inclusiones estrictas

$$\langle m_1 \rangle \subset \langle m_1, m_2 \rangle \subset \cdots$$

que ha de ser finita, porque por la segunda definición toda cadena estabiliza. Por tanto, existe un $r \in \mathbb{N}$ tal que $\langle m_1, \ldots, m_r \rangle = M'$.

□

34. Ejemplo: Los k-espacios vectoriales de dimensión finita son k-módulos noetherianos.

35. Proposición: *Todo submódulo de un módulo noetheriano es noetheriano.*

36. Proposición: *Todo cociente de un módulo noetheriano es noetheriano.*

Demostración. Sea M noetheriano y $\pi\colon M \to M/N$ un cociente. Dado un submódulo $\bar{M} \subset M/N$, tenemos que $\pi^{-1}(\bar{M}) = \langle m_1, \ldots, m_r \rangle$. Por tanto, $\bar{M} = \langle \pi(m_1), \ldots, \pi(m_r) \rangle$. □

37. Proposición: *Sea*

$$0 \to M_1 \to M_2 \xrightarrow{\pi} M_3 \to 0$$

una sucesión exacta de A-módulos. Se verifica que M_2 es noetheriano $\Leftrightarrow$ M_1 y M_3 son noetherianos.

Demostración. $\Rightarrow$) Esto es lo que afirman las dos proposiciones anteriores.

$\Leftarrow$) Sea $M' \subseteq M_2$. El diagrama siguiente es conmutativo y las filas son exactas:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' \cap M_1 & \longrightarrow & M' & \longrightarrow & \pi(M') & \longrightarrow & 0 \\
 & & \cap & & \cap & & \cap & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \xrightarrow[\pi]{} & M_3 & \longrightarrow & 0
\end{array}$$

Tenemos que $M' \cap M_1 = \langle m_1, \ldots, m_r \rangle$ y que $\pi(M') = \langle \pi(n_1), \ldots, \pi(n_s) \rangle$, con $n_i \in M'$. De donde se sigue la igualdad $M' = \langle m_1, \ldots, m_r, n_1, \ldots, n_s \rangle$.

□

38. Ejercicio: Prueba que M y M' son noetherianos si y solo si $M \oplus M'$ es noetheriano.

39. Definición: Se dice que un anillo es noetheriano si como A-módulo es noetheriano, es decir si todo ideal es finito generado, o equivalentemente, si toda cadena ascendente de ideales estabiliza.

40. Ejemplo: Los cuerpos, los anillos de ideales principales, como $\mathbb{Z}$, $k[x]$, son noetherianos.

Un ejemplo de anillo no noetheriano, es el anillo de funciones diferenciales en la recta real: Sea I_n el ideal de las funciones que se anulan en $(-\frac{1}{n}, \frac{1}{n})$, $n \in \mathbb{N}$. Tenemos que $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ es una cadena ascendente estricta de ideales en el anillo, luego no estabiliza. Por tanto, el anillo no es noetheriano.

41. Proposición: *Si A es noetheriano, todo A-módulo finito generado es noetheriano.*

Demostración. Si A es noetheriano, A^n es un A-módulo noetheriano, por el ejercicio 0.6.38. Ahora bien, como todo módulo finito generado es cociente de un libre finito generado, concluimos que los módulos finito generados son noetherianos.

□

Por tanto, sobre los dominios de ideales principales todo módulo finito generado es noetheriano.

42. Ejercicio: Prueba que si A es noetheriano A_S es noetheriano

43. Ejercicio: Demuestra que $\mathbb{Q}[x, x_1, \ldots, x_n, \ldots]/((x-n)x_n)_{\{n\in\mathbb{N}\}}$ es localmente noetheriano pero no es noetheriano.

44. Definición: Se dice que un espacio topológico es noetheriano si toda cadena descendente de cerrados estabiliza.

45. Proposición:

1. *Todo espacio topológico noetheriano es compacto.*
2. *Todo subespacio de un espacio topológico noetheriano es noetheriano.*
3. *Todo espacio topológico noetheriano es unión de un número finito de cerrados irreducibles (hemos llamado cerrado irreducible a todo cerrado que no es unión de dos cerrados propios).*

Demostración. Probemos solo 3. Sea X el espacio topológico noetheriano. Supongamos que X no es unión de un número finito de cerrados irreducibles. En particular, X no es irreducible, luego es unión de dos cerrados propios, $X = C_1 \cup C_2$. C_1 y C_2 no pueden ser los dos a la vez unión de un número finito de cerrados irreducibles. Digamos que C_1 no es unión de un número finito de cerrados irreducibles. En particular, C_1 no es un cerrado irreducible, luego es unión de dos cerrados propios $C_1 = C_{11} \cup C_{12}$. C_{11} y C_{12} no pueden ser los dos a la vez unión de un número finito de cerrados irreducibles. Digamos que C_{11} no es unión de un número finito de cerrados irreducibles. En particular, C_{11} no es un cerrado irreducible, luego es unión de dos cerrados propios $C_{11} = C_{111} \cup C_{112}$. Así sucesivamente, vamos construyendo la cadena descendente de inclusiones estrictas

$$C_1 \supset C_{11} \supset C_{111} \supset \cdots$$

lo que contradice la noetherianidad de X. En conclusión, X es unión de un número finito de cerrados irreducibles.

□

46. Proposición: *Si A es un anillo noetheriano, entonces* Spec$A$ *es un espacio topológico noetheriano. En particular,* Spec$A$ *es unión de un número finito de componentes irreducibles y el número de ideales primos minimales de A es finito*

Demostración. Sea $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_n \supseteq \cdots$ una cadena descendente de cerrados. Sean I_i los ideales de funciones que se anulan en C_i. Luego $(I_i)_0 = C_i$ y tenemos la cadena

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

Cadena que estabiliza por ser A noetheriano. Es decir, existe $m \in \mathbb{N}$ de modo que $I_m = I_{m+1} = \cdots$. Luego, $C_m = C_{m+1} = \cdots$.

□

47. Corolario: *Sea A un anillo noetheriano e $I \subsetneq A$ un ideal radical. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos mínimos conteniendo a I (que se corresponden con los ideales primos mínimos de A/I), entonces*

$$I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n.$$

Demostración. Por ser I radical coincide con la intersección de todos los ideales primos que lo contienen, que coincide con la intersección de los ideales primos mínimos conteniendo a I.

□

48. Teorema de la base de Hilbert: *Si A es un anillo noetheriano entonces $A[x]$ es un anillo noetheriano.*

Demostración. Sea $I \subset A[x]$ un ideal. Tenemos que ver que es finito generado:

Sea $J \subseteq A$ el conjunto formado por los coeficientes de máximo grado de los $p(x) \in I$. J es un ideal de A: Si $p(x) = a_0x^n + \cdots + a_n, q(x) = b_0x^m + \cdots + b_m \in I$, entonces $x^m p(x) + x^n q(x) = (a_0 + b_0)x^{n+m} + \cdots \in I$, luego si $a_0, b_0 \in J$ entonces $a_0 + b_0 \in J$.

Por ser A noetheriano, $J = (b_1, \ldots, b_r)$ es finito generado. Así, existen $p_1, \ldots, p_r \in I$ cuyos coeficientes de grado máximo son $b_1, \ldots, b_r$, respectivamente. Además, multiplicando cada p_i por una potencia conveniente de x, podemos suponer que $\operatorname{gr} p_1 = \cdots = \operatorname{gr} p_r$. Escribamos $\operatorname{gr} p_i = m$, para todo i.

Dado $p(x) = a_0x^n + \cdots + a_n \in I$. Existen $\lambda_i \in A$ tales que $a_0 = \lambda_1 b_1 + \cdots + \lambda_r b_r$. Supongamos que $n \geq m$. Tenemos que $p(x) - \sum_i \lambda_i x^{n-m} p_i \in I$ y $\operatorname{gr}(p(x) - \sum_i \lambda_i x^{n-m} p_i) < \operatorname{gr} p(x)$.

Recurrentemente obtendré que

$$I = (p_1, \ldots, p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}.$$

Ahora bien, $I \cap \{A + Ax + \cdots + Ax^{m-1}\}$ es un A-módulo finito generado ya que es submódulo de $\{A + Ax + \cdots + Ax^{m-1}\}$, que es un A-módulo noetheriano. En conclusión, si escribimos $I \cap \{A + Ax + \cdots + Ax^{m-1}\} = \langle q_1, \ldots, q_s \rangle_A$, tenemos que $I = (p_1, \ldots, p_r, q_1, \ldots, q_s)$. □

49. Definición: Dado un morfismo de anillos $f : A \to B$ se dice que B es una A-álgebra.

50. Ejemplo: Todo anillo A es de modo natural (y único) $\mathbb{Z}$-álgebra: $\mathbb{Z} \to A$, $n \mapsto n$, es el único morfismo de anillos de $\mathbb{Z}$ en A.

51. Ejemplo: $A[x_1, \ldots, x_n]$ es una A-álgebra de modo natural: tenemos el morfismo de anillos $A \to A[x_1, \ldots, x_n]$, $a \mapsto a$.

52. Definición: Se dice que B es una A-álgebra de tipo finito si existen $\xi_1, \ldots, \xi_n \in B$ que generen A-algebraicamente B, es decir, si el morfismo

$$A[x_1, \ldots, x_n] \to B, \sum_{\alpha_1, \ldots, \alpha_n} a_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto \sum_{\alpha_1, \ldots, \alpha_n} f(a_{\alpha_1, \ldots, \alpha_n}) \xi_1^{\alpha_1} \cdots \xi_n^{\alpha_n}$$

es epiyectivo.

53. Corolario: *Sea k un cuerpo. Toda k-álgebra de tipo finito es noetheriana.*

Demostración. Todo cuerpo es un anillo noetheriano, luego k es noetheriano. Por el teorema de la base de Hilbert $k[x_1]$ es noetheriano. De nuevo, por el teorema de la base de Hilbert, $k[x_1, x_2]$ es noetheriano. En conclusión $k[x_1, \ldots, x_n]$ es noetheriano y todo cociente $k[x_1, \ldots, x_n]/I$ también. Luego toda k-álgebra de tipo finito es noetheriana. □

0.6.4. Módulos y anillos de longitud finita

Usualmente, se define la dimensión de un espacio vectorial, como el número de vectores de sus bases. El concepto de base de un espacio vectorial es elaborado, si bien es muy práctico. En los A-módulos libres se define el rango del A-módulo libre como el número de elementos de sus bases.

Si intuimos que $\mathbb{R}^3$ es de dimensión 3 es porque observamos la cadena de inclusiones irrefinable: punto, recta, plano, espacio. Puede definirse la dimensión de un espacio

vectorial, como la longitud de las cadenas irrefinables de subespacios vectoriales. En los A-módulos pueden no existir bases, pero si podemos hablar de la longitud de las cadenas irrefinables de submódulos de un módulo. En términos de éstas definiremos la longitud del módulo, concepto que no coincide con el de rango, en general.

54. Definición: Diremos que un A-módulo $M \neq 0$ es simple cuando sus únicos submódulos son los triviales: 0 y M.

Si M es un A-módulo simple entonces $M = \langle m \rangle$, luego $M \simeq A/\text{Anul}\langle m \rangle$. Ahora bien, los submódulos de $A/\text{Anul}\langle m \rangle$ se corresponden con los ideales de A que contienen a $\text{Anul}\langle m \rangle$. Por tanto, M es simple si y solo si $\text{Anul}\langle m \rangle$ es un ideal maximal, es decir, M es simple si y solo si $M \simeq A/\mathfrak{m}$, donde $\mathfrak{m}$ es un ideal maximal de A.

55. Definición: Diremos que una cadena finita $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ de submódulos es una serie de composición en M, si los cocientes sucesivos M_i/M_{i-1} son A-módulos simples. Diremos que la longitud de esta serie de composición es n.

Como los submódulos de M_i/M_{i-1} se corresponden biyectivamente con los submódulos de M_i que contienen a M_{i-1}, el que M_i/M_{i-1} sea simple equivale a que no existe una cadena $M_{i-1} \underset{\neq}{\subset} N \underset{\neq}{\subset} M_i$. Por tanto, que una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ sea una serie de composición equivale a decir que no podemos añadirle más "eslabones".

56. Definición: Llamaremos longitud de M a la mínima longitud de todas sus series de composición. Si no existe ninguna serie de composición diremos que la longitud de M es infinita. Denotaremos a la longitud de un módulo M por $l(M)$.

Sobre espacios vectoriales el concepto de longitud coincide con el de dimensión.

57. Proposición: *Todas las series de composición de un módulo tienen la misma longitud.*

Demostración. Si $l(M) = \infty$ la proposición es obvia. Supongamos que $l(M) = n < \infty$.

Probemos que dado un submódulo propio $N \subset M$ se cumple que $l(N) < l(M)$: Sea $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ una serie de composición de longitud mínima de M. Si en $0 = M_0 \cap N \subseteq M_1 \cap N \subseteq \cdots \subset M_n \cap N = N$ quitamos los términos repetidos obtenemos una serie de composición en N, porque como $M_i \cap N/M_{i-1} \cap N \hookrightarrow M_i/M_{i-1}$ y M_i/M_{i-1} es simple, entonces $M_i \cap N/M_{i-1} \cap N = M_i/M_{i-1}$. Por tanto, $l(N) \leq l(M)$. Si $l(N) = l(M)$ entonces $M_i \cap N/M_{i-1} \cap N \neq 0$ para todo i. Entonces, $M_1 \cap N$ contiene estrictamente a $M_0 \cap N = 0$ y está incluido en M_1, luego $M_1 \cap N = M_1$. Sigamos, $M_2 \cap N$ contiene estrictamente a $M_1 \cap N = M_1$ y está incluido en M_2 luego $M_2 \cap N = M_2$ Recurrentemente, $N = M_n \cap N = M_n = M$, lo que es contradictorio.

Así pues, dada una serie de composición $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_m = M$, tenemos que $l(M) > l(M'_{m-1}) > \cdots > l(M'_1)$, luego $l(M) \geq m$. Como $m \geq n = l(M)$, tenemos que $m = n$.

□

Observemos que hemos demostrado que si un módulo es de longitud finita todo submódulo suyo es de longitud finita. Si un módulo es de longitud finita todo cociente suyo también lo es, pues toda serie de composición define por paso al cociente una serie de composición (eliminando las igualdades que aparezcan en la serie, en el cociente).

58. Proposición : *La longitud es una función aditiva, es decir, dada una sucesión exacta* $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ *se cumple que* $l(M) = l(M') + l(M'')$.

Demostración. Si $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_{n'} = M'$ y $0 = M''_0 \subset M''_1 \subset \cdots \subset M''_{n''} = M''$ son series de composición de M' y M'' entonces

$$0 = i(M'_0) \subset i(M'_1) \subset \cdots \subset i(M'_{n'}) = i(M') = \pi^{-1}(M''_0) \subset \pi^{-1}(M''_1) \subset \cdots \subset \pi^{-1}(M''_{n''}) = M$$

es una serie de composición de M, luego $l(M) = n' + n'' = l(M') + l(M'')$. □

En particular, si consideramos la sucesión exacta

$$\begin{array}{ccccccccc} 0 & \to & M' & \to & M' \oplus M'' & \to & M'' & \to & 0 \\ & & m' & \mapsto & (m', 0) & & & & \\ & & & & (m', m'') & \mapsto & m'' & & \end{array}$$

tenemos que $l(M' \oplus M'') = l(M') + l(M'')$.

La sucesión de morfismos de módulos

$$0 \to M_0 \to \cdots \to M_{s-1} \xrightarrow{f_s} M_s \xrightarrow{f_{s+1}} M_{s+1} \to \cdots \to M_n \to 0 \qquad (*)$$

es exacta si y solo si son exactas las sucesiones $0 \to \operatorname{Im} f_s \to M_s \xrightarrow{f_{s+1}} \operatorname{Im} f_{s+1} \to 0$. Así, si la sucesión $(*)$ es exacta, tendremos que $l(\operatorname{Im} f_s) - l(M_s) + l(\operatorname{Im} f_{s+1}) = 0$ y haciendo el sumatorio para todo s tenemos

$$l(M_0) - l(M_1) + \cdots + (-1)^n l(M_n) = 0$$

59. Ejercicio : Sea $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n$ una cadena de A-submódulos de M. Prueba que $l(M/M_n) = \sum_{i=1}^{n} l(M_{i-1}/M_i)$.

60. Ejercicio : Sea $\mathcal{O}$ una k-álgebra local de ideal maximal $\mathfrak{m}$. Prueba que si M es un $\mathcal{O}$-módulo de longitud finita entonces $\dim_k M = l(M) \cdot \dim_k \mathcal{O}/\mathfrak{m}$.

61. Proposición: *M es de longitud finita $\Leftrightarrow$ M es noetheriano y* $\operatorname{Sop}(M)$ *es un número finito de puntos cerrados.*

Demostración. $\Rightarrow$) Si M es de longitud finita, sea

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

una cadena de composición. Entonces $M_i/M_{i-1} \simeq A/\mathfrak{m}_i$, con $\mathfrak{m}_i$ maximal. Como el soporte de M coincide con el soporte de $GM := \oplus_i M_i/M_{i-1}$, concluimos que el soporte de M es un número finito de puntos cerrados. Además, como GM es noetheriano, M también.

$\Leftarrow$) $M = \langle m_1, \ldots, m_n \rangle$ es finito generado porque es noetheriano. Sea $M_i := \langle m_1, \ldots, m_i \rangle$ y consideremos la cadena de submódulos

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M.$$

M es de longitud finita si y solo si $M_i/M_{i-1} = \langle \bar{m}_i \rangle$ es de longitud finita, para todo i. Además, M_i/M_{i-1} es noetheriano y de soporte incluido en el soporte de M, luego el soporte es un número finito de puntos cerrados. En conclusión, podemos suponer que M es monógeno, luego $M \simeq A/I$. El soporte de A/I es $(I)_0 = \mathrm{Spec}(A/I) = \{x_1, \ldots, x_r\}$. Por tanto, $A/I = A_1 \times \cdots \times A_n$, con $A_i = (A/I)_{x_i}$. Todo A_i-submódulo de A_i es un A-submódulo y viceversa, luego $l_A(A_i) = l_{A_i}(A_i)$, basta probar que $l_{A_i}(A_i) < \infty$. A_i es un anillo con un único ideal primo $\mathfrak{m}_i$, que es finito generado y que ha de coincidir con el radical de A. Luego, existe un $n_i \in \mathbb{N}$ tal que $\mathfrak{m}_i^{n_i} = 0$. A_i es un A_i-módulo de longitud finita, porque si consideremos la cadena

$$0 = \mathfrak{m}_i^{n_i} \subseteq \mathfrak{m}_i^{n_i - 1} \subseteq \cdots \subseteq \mathfrak{m}_i \subseteq A_i,$$

tenemos que $l_{A_i}(\mathfrak{m}_i^r/\mathfrak{m}_i^{r-1}) = \dim_{A_i/\mathfrak{m}_i}(\mathfrak{m}_i^r/\mathfrak{m}_i^{r-1}) < \infty$.

□

62. Definición: Se dice que un anillo A es de longitud finita si como A-módulo es de longitud finita. Se dice que un anillo es de dimensión de Krull nula si todos sus ideales primos son maximales.

Si un anillo noetheriano es de dimensión de Krull nula entonces su espectro primo es un número finito de ideales primos maximales, ya que el número de ideales primos minimales de todo anillo noetheriano es finito.

63. Corolario: *Un anillo es de longitud finita si y solo si es noetheriano de dimensión de Krull nula.*

Demostración. Es consecuencia inmediata de 0.6.61. □

64. Corolario: *Sea A un anillo de longitud finita. Entonces,* $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$*, donde $x_1, \ldots, x_n$ son puntos cerrados, y*

$$A = A_{x_1} \times \cdots \times A_{x_n}$$

Demostración. Es consecuencia inmediata de 0.6.27. □

65. Corolario: *Sea A un anillo de longitud finita. A es producto directo de cuerpos si y solo si es reducido.*

Demostración. $A = A_1 \times \cdots \times A_n$, con A_i locales (de ideales maximales $\mathfrak{p}_i$). Luego, $\operatorname{rad} A = \operatorname{rad} A_1 \times \cdots \times \operatorname{rad} A_n = \mathfrak{p}_1 \times \cdots \times \mathfrak{p}_n$. Si $\operatorname{rad} A = 0$, entonces $\mathfrak{p}_i = 0$ para todo i y A_i es un cuerpo para todo i. Si A es producto directo de cuerpos, obviamente es reducida. □

66. Corolario: *Sea A un anillo de longitud finita. A es íntegro si y solo si es un cuerpo.*

Demostración. Es consecuencia inmediata del corolario anterior.

□

67. Corolario: *Si $f : A \hookrightarrow B$ es un morfismo inyectivo y A es un anillo de longitud finita, entonces el morfismo inducido $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo.*

Demostración. Por 0.5.46, f^* es de imagen densa. Como $\operatorname{Spec} A$ es igual a un número finito de puntos cerrados, entonces f^* es epiyectiva.

□

68. Definición: Diremos que una k-álgebra A, es una k-álgebra finita, si A es un k-espacio vectorial de dimensión finita.

69. Proposición: *La k-álgebra $k[x]/(x^n + a_1 x^{n-1} + \ldots + a_n)$ es un k-espacio vectorial de base $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$.*

Demostración. Sea $q(x) = x^n + a_1 x^{n-1} + \ldots + a_n$. Dado un polinomio $p(x)$ existen dos polinomios únicos $c(x)$ y $r(x)$, de modo que $p(x) = c(x) \cdot q(x) + r(x)$ y que $\operatorname{gr} r(x) < \operatorname{gr} q(x)$. Por lo tanto, existe un único polinomio $r(x)$ de grado menor que n de modo que $\overline{r(x)} = \overline{p(x)}$ en $k[x]/(q(x))$.

Es decir, la aplicación $k \oplus k \cdot x \oplus \cdots \oplus k \cdot x^{n-1} \to k[x]/(q(x))$, $r(x) \mapsto \overline{r(x)}$ es un isomorfismo.

□

Obviamente las k-álgebras finitas son anillos de longitud finita. Por tanto, tenemos el siguiente teorema.

70. Teorema: *Sea A una k-álgebra finita. Se cumple*

1. $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ *es un número finito de puntos cerrados.*
2. $A = A_{x_1} \times \cdots \times A_{x_n}$.
3. *Si A es íntegra entonces es cuerpo.*
4. *A es reducida si y solo si es producto directo de un número finito de cuerpos.*
5. *Si $f : A \hookrightarrow B$ es un morfismo de anillos inyectivo, entonces $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo.*

71. Definiciones: Sea A un anillo de longitud finita, es decir, A es un anillo noetheriano y $X = \operatorname{Spec} A = \{x_1, \ldots, x_r\}$, es un número finito de puntos cerrados. Llamaremos multiplicidad con la que aparece x_i en X, que denotamos $m_{x_i}(X)$, a

$$m_{x_i}(X) := l_A(A_{x_i}).$$

Llamaremos número de puntos de X contando multiplicidades a $l_A(A)$. Observemos que $A = A_{x_1} \times \cdots \times A_{x_n}$, luego

$$\text{Número de puntos de } X \text{ contando multiplicidades} = l_A(A) = \sum_i l_A(A_{x_i}) = \sum_{x_i \in X} m_{x_i}(X).$$

Si A es una k-álgebra finita, llamaremos número de puntos de X contando multiplicidades y grados a $\dim_k A$. Llamaremos grado de $x \in X$ (sobre k), que denotaremos $\operatorname{gr}_k x$, a $\operatorname{gr}_k(x) := \dim_k A/\mathfrak{m}_x$. Observemos que

$$\begin{aligned} \text{Nº punt. de } X \text{ contando mult. y grad.} = \dim_k A &= \sum_i \dim_k A_{x_i} \\ &= \sum_i l_A(A_{x_i}) \cdot \dim_k A/\mathfrak{m}_{x_i} = \sum_{x_i \in X} m_{x_i}(X) \cdot \operatorname{gr}_k(x_i). \end{aligned}$$

72. Ejercicio: Sea $A = \mathbb{R}[x]/((x^2+1)^2(x-1)(x-2)^3)$. Calcula el espectro primo de A, el número de puntos de $\operatorname{Spec} A$, multiplicidades y grados.

0.6.5. Módulos sobre dominios de ideales principales

El objetivo de esta sección, es clasificar y determinar la estructura de los A-módulos finito generados sobre un dominio de ideales principales. En particular, obtendremos la clasificación de los grupos abelianos y la clasificación de los endomorfismos de un espacio vectorial de dimensión finita.

Empecemos con algunos ejemplos de módulos sobre dominios de ideales principales.

Todo grupo abeliano, G, tiene de modo natural estructura de $\mathbb{Z}$-módulo: La suma considerada es la suma del grupo abeliano y el producto por escalares se define

$$n \cdot g = \begin{cases} g + \overset{n}{\ldots} + g & \text{si } n \in \mathbb{N}^+ \\ (-g) + \overset{-n}{\ldots} + (-g) & \text{si } n \notin \mathbb{N} \\ 0 & \text{si } n = 0 \end{cases}$$

Recíprocamente, todo $\mathbb{Z}$-módulo es en particular un grupo abeliano. Así pues, hablar de grupos abelianos o de $\mathbb{Z}$-módulos es solo una diferencia en la terminología usada. Así, por ejemplo, un grupo abeliano es finito generado si y solo si es finito generado como $\mathbb{Z}$-módulo.

Un endomorfismo lineal $T\colon E \to E$ de un k-espacio vectorial E, induce una estructura de $k[x]$-módulos en E del siguiente modo

$$p(x) \cdot e := p(T)(e)$$

en particular $x \cdot e = T(e)$. Recíprocamente, si E es un $k[x]$-módulo, tenemos el endomorfismo $E \xrightarrow{x\cdot} E$, $e \mapsto x \cdot e$. Cuando pensemos E con la estructura de $k[x]$-módulo inducida por el endomorfismo T, lo escribiremos E_T.

73. Definición: Dos endomorfismos T, T' de E se dicen que son equivalentes si existe un automorfismo lineal τ de E tal que $T' = \tau \circ T \circ \tau^{-1}$. Esta igualdad significa la conmutatividad del cuadrado

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ E & \xrightarrow{T'} & E \end{array}$$

74. Proposición: *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y solo si existen una base para T y otra base para T' en las que T y T' tienen la misma matriz.*

Demostración. El endomorfismo τ es precisamente el que manda una base a la otra. □

75. Proposición: *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y solo si inducen estructuras de $k[x]$-módulos isomorfas.*

Demostración. Si T, T' son equivalentes existe un automorfismo lineal τ tal que $\tau \circ T = T' \circ \tau$. Veamos que $\tau : E_T \to E_{T'}$ es un isomorfismo de $k[x]$-módulos:

$$\tau(x \cdot e) = \tau(T(e)) = T'(\tau(e)) = x \cdot \tau(e).$$

Reiterativamente, probamos que $\tau(x^i \cdot e) = \tau(T^i(e)) = T'^i(\tau(e)) = x^i \cdot \tau(e)$ y por linealidad que $\tau(p(x) \cdot e) = p(x) \cdot \tau(e)$.

Recírpocamente, si $\tau : E_T \to E'_{T'}$ es un isomorfismo de $k[x]$-módulos, entonces tenemos $\tau(T(e)) = \tau(x \cdot e) = x \cdot \tau(e) = T'(\tau(e)$, luego $\tau \circ T = T' \circ T$ y T y T' son equivalentes.

□

Sigamos con la teoría general.

76. Definición: Sea A un anillo íntegro y M un A-módulo. Denotemos $\Sigma = A_{A\setminus\{0\}}$ y $M_\Sigma = M_{A\setminus\{0\}}$. Llamaremos rango de M al número $\dim_\Sigma M_\Sigma$.

Observemos que si $M = A \oplus \overset{n}{\ldots} \oplus A$ entonces el rango de M es n.

77. Definición: Sea A un anillo íntegro y M un A-módulo. Llamaremos torsión de M, que denotaremos $T(M)$, a

$$T(M) := \{m \in M : \text{existe } a \in A \text{ no nulo tal que } am = 0\}.$$

Es fácil comprobar que $T(M)$ coincide con el núcleo del morfismo de localización $M \to M_{A\setminus\{0\}} = M_\Sigma$, $m \mapsto \frac{m}{1}$, lo que prueba que $T(M)$ es un submódulo de M.

Se dice que un módulo M es libre de torsión si $T(M) = 0$, se dice que es de torsión si $T(M) = M$.

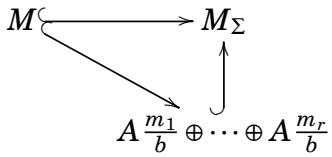
78. Ejemplo: Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})$.

$$\begin{aligned} T(\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})) &= \{(n, \bar{m}) \in \mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z}) \mid \text{Existe } r \in \mathbb{Z}\setminus\{0\}, \text{ tal que } r(n, \bar{m}) \\ &= (rn, \overline{r}m) = 0\} = \{(0, \bar{m}) \mid \bar{m} \in \mathbb{Z}/4\mathbb{Z}\} \simeq \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

79. Proposición: *Sea A un anillo íntegro. Si M es un A-módulo finito generado libre de torsión entonces es un submódulo de un A-módulo libre del mismo rango.*

Demostración. Tenemos que $M = \langle m_1, \ldots, m_n \rangle$ y el morfismo de localización $M \hookrightarrow M_\Sigma$ es inyectivo. Evidentemente $\frac{m_1}{1}, \ldots, \frac{m_n}{1}$ es un sistema generador del Σ-espacio vectorial M_Σ. Reordenado, podemos suponer que $\frac{m_1}{1}, \ldots, \frac{m_r}{1}$ es una base del Σ-espacio vectorial M_Σ, $(r \geq n)$. Por tanto, para cada m_j tendremos $\frac{m_j}{1} = \sum_{s=1}^{r} \frac{a_{js}}{b_{js}} \frac{m_s}{1}$. Denotemos $b = \prod_{i,j} b_{ij}$.

Con las notaciones obvias, tendremos el siguiente diagrama conmutativo de morfismos inyectivos



□

80. Ejercicio: Dado un epimorfismo $\pi\colon M\to M'$ de A-módulos, si π tiene sección (es decir, existe $s\colon M'\to M$ de modo que $\pi\circ s=\mathrm{Id}$) entonces $M\simeq \mathrm{Ker}\,\pi\oplus M'$. (Pista: Los morfismos $\mathrm{Ker}\,\pi\oplus M'\to M$, $(m,m')\mapsto (m+s(m'))$ y $M\to \mathrm{Ker}\,\pi\oplus M'$, $m\mapsto (m-s(\pi(m)),\pi(m))$ son inversos entre sí).

Dado un morfismo $i\colon N\to M$ inyectivo, si i tiene retracto (es decir, existe $r\colon M\to N$ de modo que $r\circ i=\mathrm{Id}$) entonces $M\simeq N\oplus M/N$. (Pista: Los morfismos $M\to N\oplus M/N$, $m\mapsto (r(m),\bar{m})$ y $N\oplus M/N\to M$, $(n,\bar{m})\mapsto n+(m-r(m))$ son inversos entre sí).

81. Proposición: *Sea A un dominio de ideales principales. Si M es un A-módulo finito generado libre de torsión entonces es un A-módulo libre.*

Demostración. Basta probar que los submódulos de un A-módulo libre son libres, por 0.6.79. Procederemos por inducción sobre el rango del módulo libre, que denotaremos L.

Si el rango de L es cero es obvio. Si el rango de L es uno entonces $L\simeq A$. Por tanto, todo submódulo M de L es isomorfo a un ideal de A, luego $M\simeq aA$. Si $a\neq 0$ entonces $A\simeq aA$, $b\mapsto ab$, luego M es libre de rango 1. Si $a=0$ entonces $M=0$.

Supongamos que el rango de L es $n>1$. Como $L\simeq A^n$ es fácil definir una sucesión exacta

$$0\to L'\to L\to L''\to 0$$

con L' libre de rango 1 y L'' libre de rango $n-1$. Dado $M\subseteq L$ consideremos el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L' & \longrightarrow & L & \xrightarrow{\pi} & L'' & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & L'\cap M & \longrightarrow & M & \longrightarrow & \pi(M) & \longrightarrow & 0 \end{array}$$

de filas exactas. Por inducción $L'\cap M$ y $\pi(M)$ son libres de rango finito. Por tanto, como $\pi(M)$ es libre, el epimorfismo $M\to\pi(M)$ tiene sección y por el ejercicio 0.6.80 $M=(L'\cap M)\oplus\pi(M)$. En conclusión, M es libre. □

82. Primer teorema de descomposición: *Sea A un dominio de ideales principales y M un A-módulo finito generado. Se cumple*

$$M \simeq T(M) \oplus (M/T(M))$$

donde $T(M)$ es un módulo finito generado de torsión y $M/T(M)$ es un módulo libre de rango el rango de M.

Se cumple además que si $M \simeq M' \oplus L$, siendo M' un A-módulo de torsión y L libre, entonces $M' \simeq T(M)$ y $L \simeq (M/T(M))$.

Demostración. $M/T(M)$ es un módulo finito libre de torsión: Si $\bar{m} \in T(M/T(M))$ entonces existe $a \in A$ no nulo tal que $a\bar{m} = 0$, luego $am \in T(M)$ y existe $b \in A$ no nulo tal que $bam = 0$. Por tanto, $m \in T(M)$ y $\bar{m} = 0$.

Por la proposición anterior $M/T(M)$ es un módulo libre. Luego, el epimorfismo de paso al cociente $M \to M/T(M)$ tiene sección, Entonces, $M \simeq T(M) \oplus (M/T(M))$. Sea g el punto genérico de $\operatorname{Spec} A$. Si localizamos en g obtenemos $M_g = (M/T(M))_g$, luego el rango de M es el de $M/T(M)$.

Si $M \simeq M' \oplus L$, entonces $T(M) \simeq T(M' \oplus L) = T(M') \oplus T(L) = M'$. Luego $(M/T(M)) \simeq (M' \oplus L)/M' = L$. Hemos concluido.

□

Observemos que $M_{A\setminus\{0\}} = (M/T(M))_{A\setminus\{0\}}$. Por tanto, el rango de $M/T(M)$ es el de M. Así pues, en el teorema anterior $M/T(M)$ es un módulo libre de rango el de M.

Clasificación de los módulos de torsion

Hemos reducido el problema de la clasificación de los módulos finito generados sobre dominios de ideales principales, a la clasificación de los módulos finito generados de torsión. Si M es un módulo finito generado de torsión, entonces $\operatorname{Anul}(M) \neq 0$. En efecto, si $M = \langle m_1, \ldots, m_n \rangle$, y $a_i \in A\setminus\{0\}$ cumplen que $a_i m_i = 0$, entonces $0 \neq a_1 \cdots a_n \in \operatorname{Anul}(M)$.

83. Lema: *Sea A un anillo y $p, q \in A$ tales que $(p, q) = A$. Sea M un A-módulo y dado $a \in A$ denotemos* $\operatorname{Ker} a = \{m \in M : a \cdot m = 0\}$. *Entonces,*

$$\operatorname{Ker} pq = \operatorname{Ker} p \oplus \operatorname{Ker} q.$$

Demostración. De acuerdo con la identidad de Bézout existen $\lambda, \mu \in A$ tales que

$$\lambda p + \mu q = 1$$

Por tanto, cada $m \in \operatorname{Ker} pq$ cumple $\lambda pm + \mu qm = m$, donde $\lambda pm \in \operatorname{Ker} q$ y $\mu qm \in \operatorname{Ker} p$. Por consiguiente $\operatorname{Ker} pq = \operatorname{Ker} p + \operatorname{Ker} q$.

Solo nos falta probar que $\operatorname{Ker} p \cap \operatorname{Ker} q = 0$. Si $m \in \operatorname{Ker} p \cap \operatorname{Ker} q$ entonces tenemos que $m = \lambda pm + \mu qm = 0 + 0 = 0$.

□

84. Segundo teorema de descomposición: Sea M un A-módulo y $a_1, \ldots, a_s \in A$, con $(a_i, a_j) = A$ para todo $i \neq j$. Entonces,

$$\operatorname{Ker}(a_1 \cdots a_s)\cdot = \operatorname{Ker} a_1 \cdot \oplus \cdots \oplus \operatorname{Ker} a_s \cdot .$$

En particular, si A es un dominio de ideales principales y M es un A-módulo finito generado de torsión, entonces $0 \neq \operatorname{Anul}_A(M) = (a)$ y si $a = p_1^{n_1} \cdots p_r^{n_r} \cdot inv$ es la descomposición en producto de potencias de irreducibles de a, entonces

$$M = \operatorname{Ker} p_1^{n_1} \cdot \oplus \cdots \oplus \operatorname{Ker} p_r^{n_r} \cdot .$$

Demostración. Primero observemos que si $(a,b) = A$ y $(a,c) = A$, entonces $(a,bc) = A$:

$$A = A \cdot A = (a,b) \cdot (a,c) = (a^2, ac, ab, bc) \subseteq (a,bc),$$

luego $(a,bc) = A$.

Recurrentemente, obtenemos que $(a_1, a_2 \cdots a_s) = A$. Por el lema anterior,

$$\operatorname{Ker}(a_1 \cdots a_s)\cdot = \operatorname{Ker} a_1 \cdot \oplus \operatorname{Ker}(a_2 \cdots a_s \cdot) = \cdots = \operatorname{Ker} a_1 \cdot \oplus \cdots \oplus \operatorname{Ker} a_s \cdot$$

□

85. Corolario: *Sea $T\colon E \to E$ un endomorfismo k-lineal. Sea $p(x) = p_1(x) \cdots p_r(x) \in k[x]$, con $p_i(x)$ primo con $p_j(x)$, para todo $i \neq j$. Entonces,*

$$\operatorname{Ker} p(T) = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

Demostración. E es un $k[x]$-módulo: $q(x) \cdot e = q(T)(e)$, para todo $q(x) \in k[x]$. Entonces,

$$\operatorname{Ker} p(T) = \operatorname{Ker} p(x)\cdot \overset{0.6.84}{=} \operatorname{Ker} p_1(x) \cdot \oplus \cdots \oplus \operatorname{Ker} p_r(x)\cdot = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

□

Aplicación a ecuaciones diferenciales lineales

Sea F el $\mathbb{C}$-espacio vectorial de todas las funciones reales con valores complejos infinitamente diferenciables. Sea

$$D : F \to F,\ D(f(x)) = f'(x)$$

el "operador derivada". Es claro que D es un endomorfismo $\mathbb{C}$-lineal de F. Dado $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, entonces $P(D)\colon F \to F$ es el endomorfismo definido por

$$P(D)(f) = a_n D^n(f) + a_{n-1}D^{n-1}(f) + \cdots + a_0 \cdot f, \text{ donde } D^r(f) \text{ es la derivada } r\text{-ésima de } f.$$

Queremos resolver ecuaciones diferenciales del tipo

$$a_n \cdot f^{n)} + \cdots + a_2 f'' + a_1 f' + a_o \cdot f = 0, \qquad \text{(donde los } a_i \text{ son constantes).}$$

Es decir, buscamos aquellas funciones $f \in F$. que cumplen que $P(D)(f) = 0$, donde $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Tenemos que calcular $\operatorname{Ker} P(D)$.

Veamos que

$$\operatorname{Ker} D^r = \{\text{Polinomios de grado estrictamente menor que } r\}.$$

En efecto,

$D(f) = 0 \iff f = cte$
$D^2(f) = 0 \iff D(D(f)) = 0 \iff D(f) = cte \iff f = cte \cdot x + cte'$
$D^3(f) = 0 \iff D^2(Df) = 0 \iff Df = cte \cdot x + cte' \iff f = \frac{cte}{2} \cdot x^2 + cte' \cdot x + cte''$
Etcétera.

86. Movimiento uniformemente acelerado: Supogamos que un objeto se mueve a lo largo de la recta (real) con una aceleración constante a. Digamos que $f(t)$ es la posición del móvil en el instante t. La velocidad del móvil es $f'(t)$ en cada instante t y la aceleración es $f''(t) = a$ en cada instante t. Por tanto, $f''' = 0$, es decir, $f(t) \in \operatorname{Ker} D^3$. Luego, $f(t) = \lambda + \mu t + \gamma t^2$. Observemos que $f(0) = \lambda$, $f'(0) = \mu$ y $f''(0) = 2 \cdot \gamma = a$. Por tanto,

$$f(t) = f(0) + f'(0) \cdot t + \frac{a}{2} \cdot t^2 \quad \text{y} \quad f'(t) = f'(0) + a \cdot t.$$

87. Fórmula de conmutación: *Sea $P(x) \in \mathbb{C}[x]$. Para toda $f \in F$ y $\alpha \in \mathbb{C}$, se cumple que*

$$P(D)(e^{\alpha x} \cdot f) = e^{\alpha x} \cdot P(D + \alpha \cdot \mathrm{Id})(f)$$

Demostración. $D(e^{\alpha x}\cdot f)=\alpha\cdot e^{\alpha x}\cdot f+e^{\alpha x}\cdot D(f)=e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})(f)$.

$D^2(e^{\alpha x}\cdot f)=D(D(e^{\alpha x}\cdot f))=D(e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})(f))=e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})((D+\alpha\cdot \mathrm{Id})(f))=e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})^2(f)$.

Así sucesivamente, $D^n(e^{\alpha x}\cdot f)=e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})^n(f)$. Para $P(D)=\sum_i a_i D^i$ tendremos que

$$P(D)(e^{\alpha x}\cdot f)=\sum_i a_i D^i(e^{\alpha x}\cdot f)=\sum_i a_i\cdot e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})^i(f)=e^{\alpha x}\cdot P(D+\alpha\cdot \mathrm{Id})(f)$$

□

88. Teorema: *Se cumple que*

1. $\mathrm{Ker}(D-\alpha\cdot \mathrm{Id})^r=e^{\alpha x}\cdot\{$*Polinomios de grado estrictamente menor que* $r\}$.

2. *Si* $p(x)=(x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}$ *, entonces*

$$\begin{aligned}\mathrm{Ker}\,p(D)&=\mathrm{Ker}(D-\alpha_1\cdot \mathrm{Id})^{n_1}\oplus\cdots\oplus\mathrm{Ker}(D-\alpha_r\cdot \mathrm{Id})^{n_r}\\&=e^{\alpha_1 x}\cdot\{\textit{Pol. de grado } <n_1\}\oplus\cdots\oplus e^{\alpha_r x}\cdot\{\textit{Pol. de grado } <n_r\}\end{aligned}$$

Demostración. 1. $(D-\alpha\cdot \mathrm{Id})^r f(x)=0\iff 0=(D-\alpha\cdot \mathrm{Id})^r(e^{\alpha x}\cdot e^{-\alpha x}\cdot f(x))=e^{\alpha x}\cdot D^r(e^{-\alpha x}\cdot f(x))\iff 0=D^r(e^{-\alpha x}\cdot f(x))\iff e^{-\alpha x}\cdot f(x)$ es un polinomio de grado menor que $r\iff f(x)$ es $e^{\alpha x}$ multiplicado por un polinomio de grado menor que r.

2. Es consecuencia de 1. y 0.6.85.

□

89. Nota: Sea $P(x)\in\mathbb{R}[x]$ y se $\alpha=a+bi$ es una raíz compleja de $P(x)$, con $b\neq 0$. Entonces $\bar\alpha=a-bi$ también es una raíz compleja de $P(x)$. Más aún, la multiplicidad con la que aparece α es la misma con la aparece $\bar\alpha$, es decir, $P(x)=(x-\alpha)^n\cdot(x-\bar\alpha)^n\cdot Q(x)$, con $Q(\alpha),Q(\bar\alpha)\neq 0$. Probemos que

$$\left\{\begin{array}{l} f\in\mathrm{Ker}(D-\alpha\,\mathrm{Id})^n\oplus\mathrm{Ker}(D-\bar\alpha\,\mathrm{Id})^n\\ \text{tales que } f(x)\in\mathbb{R}\text{ para todo } x\end{array}\right\}=e^{ax}\cdot\{q(x)\cdot\cos bx+r(x)\cdot\mathrm{sen}\,bx\}_{q(x),r(x)\in P_n}$$

donde P_n son todos los polinomios con coeficientes reales de grado $<n$: Por 0.6.88, tenemos que una base del $\mathbb{R}$-espacio vectorial $E=\mathrm{Ker}(D-\alpha\,\mathrm{Id})^n\oplus\mathrm{Ker}(D-\bar\alpha\,\mathrm{Id})^n$, es

$$\{e^{ax}\cdot e^{bix}\cdot x^r, ie^{ax}\cdot e^{bix}\cdot x^r, e^{ax}\cdot e^{-bix}\cdot x^r, ie^{ax}\cdot e^{-bix}\cdot x^r\}_{0\le r<n}.$$

Las funciones con valores en $\mathbb{R}$ de E, se obtienen sumando a cada función $f\in E$ su conjugada. Por tanto, una base de $\{f\in E:\ f(x)\in\mathbb{R},\ \forall x\in\mathbb{R}\}$ es

$$\{e^{ax}\cdot\cos bx\cdot x^r, e^{ax}\cdot\mathrm{sen}\,bx\cdot x^r,\}_{0\le r<n}.$$

90. Ley de desintegración radiactiva: Consideremos que tenemos una cierta cantidad $U(t)$ de gramos de uranio que permanece (sin desintegrar) en el tiempo t. Suponemos que la cantidad de uranio que se desintegra en un intervalo de tiempo (muy pequeño) t_1, $U(t)-U(t+t_1)$, es proporcional al tiempo t_1 transcurrrido y a la cantidad $U(t)$ de gramos que había en el instante t. Es decir, tenemos

$$U(t+t_1)-U(t) = -cte\cdot t_1\cdot U(t) \qquad (cte>0)$$

Por tanto,

$$\frac{U(t+t_1)-U(t)}{t_1} = -cte\cdot U(t)$$

Tomando límite $t_1 \to 0$, obtenemos

$$U'(t) = -cte\cdot U(t)$$

Es decir, $U(t)$ verifica la ecuación diferencial $U'+cte\cdot U=0$. Tenemos $(D+cte\cdot \mathrm{Id})(U)=0$, luego $U(t)=a\cdot e^{-cte\cdot t}$, para cierta constante a. Observemos que $U(0)=a\cdot e^0=a$. Luego,

$$\boxed{U(t)=U(0)\cdot e^{-cte\cdot t}}$$

Veamos cuál es la semivida del uranio, es decir, cuánto tiempo s ha de transcurrir para que se desintegre la mitad del uranio:

$$U(0)\cdot e^{-cte\cdot s} = U(s) = \frac{U(0)}{2}$$

Luego, $e^{-cte\cdot s}=\frac{-1}{2}$. Tomando logaritmo neperiano $-cte\cdot s=\ln 2^{-1}=-\ln 2$, luego

$$s=\frac{\ln 2}{cte} \quad \text{y} \quad U(t)=U(0)\cdot e^{-\frac{\ln 2}{s}\cdot t}=U(0)\cdot 2^{-\frac{t}{s}}.$$

El carbono 14 que hay en la atmósfera aunque se desintegra en carbono no radiactivo (carbono 12 y 13), también se crea continuamente debido a las colisiones de los neutrones generados por los rayos cósmicos con el nitrógeno de la atmósfera superior y, resulta que la proporción de carbono 14 y carbono no radiactivo permanece en un nivel casi constante en la atmósfera a lo largo del tiempo. Las plantas adquieren el carbono atmosférico mediante la fotosíntesis, y los animales, mediante el consumo de plantas y de otros animales. Cuando un organismo muere el carbono 14 existente va desintegrándose. La proporción de carbono 14 y carbono no radiactivo cuando se examinan los restos del organismo proporciona una indicación del tiempo transcurrido desde su muerte.

91. Presión atmosférica: Sea $P(h)$ la presión atmosférica a una altura h del suelo. La diferencia de presión $P(h+t)-P(h)$ es proporcional a t y a la densidad del aire en h (que es proporcional a $P(h)$). Entonces,

$$\frac{P(h+t)-P(h)}{t} = -K\cdot P(h), \text{ luego } P'(h) = -K\cdot P(h)$$

Es decir, $(D+K\cdot \mathrm{Id})(P)=0$ y $P(h)=a\cdot e^{-K\cdot h}$, donde $a=P(0)$. Puede medirse la altura en términos de la presión: $h=\frac{\ln P(0)-\ln P}{K}$.

92. Interés compuesto continuo: Supongamos que tenemos un capital de 10^6 euros invertidos en un banco. El banco nos por la inversión un interés del 2 por ciento anual y nos permite retirar el dinero en cualquier momento sin penalización y con el pago de los intereses del capital por el tiempo exacto transcurrido. Si retiramos el capital, con los intereses generados, al año y medio ¿cuánto dinero nos llevaremos?: Sea $f(t)$ el capital más los intereses generados que tenemos en el banco en el momento t. Observemos que $f(t+h)-f(t)$ es proporcional a $f(t)$ y al tiempo h transcurrido ("cuando h es muy pequeño"), es decir,

$$f(t+h)-f(t)=K\cdot h\cdot f(t), \quad \text{y} \quad \frac{f(t+h)-f(t)}{h}=K\cdot f(t)$$

Luego,

$$f'(t)=\lim_{h\to 0}\frac{f(t+h)-f(t)}{h}=K\cdot f(t)$$

Es decir, $(D-K\cdot \mathrm{Id})(f)=0$, luego $f(t)=a\cdot e^{Kt}$. Sabemos que $f(0)=10^6$, luego $a=10^6$; y $10^6\cdot e^K=f(1)=10^6\cdot(1+0'02)$, luego $e^K=1+0'02$. Por tanto,

$$f(t)=10^6\cdot(1+0'02)^t$$

y $f(1'5)=10^6\cdot(1+0'02)^{1'5}$.

93. Ejemplo: Resolvamos la ecuación diferencial: $f''''-2f'''+2f''=0$. Tenemos que resolver $(D^4-2D^3+2D^2)(f)=0$, es decir, calcular $\mathrm{Ker}(D^4-2D^3+2D^2)$. Observemos que $x^4-2x^3+2x^2=x^2(x^2-2x+2)=x^2(x-(1+i))(x-(1-i))$. Luego,

$$\begin{aligned}\mathrm{Ker}(D^4-2D^3+2D^2) &= \mathrm{Ker}\,D^2\oplus\mathrm{Ker}(D-(1+i)\cdot\mathrm{Id})\oplus\mathrm{Ker}(D-(1-i)\cdot\mathrm{Id})\\ &= \{a+bx+c\cdot e^{(1+i)\cdot x}+d\cdot e^{(1-i)\cdot x}\}\end{aligned}$$

Luego,

$$\left\{\begin{array}{l}\text{Las funciones con valores en } \mathbb{R} \text{ solución de}\\ \text{la ecuación diferencial } f''''-2f'''+2f''=0\end{array}\right\}=\{a+bx+e^x\cdot(\lambda\cos x+\mu\,\mathrm{sen}\,x)\}$$

94. Movimiento armónico simple: Consideremos un muelle cuyo extremo esté en el origen de la recta real. Denotemos por $f(t)$ la posición del extremo del muelle en el instante t. Si el extremo del muelle está en la posición $f(t)$ en el instante t, entonces el muelle ejerce una fuerza (luego aceleración) proporcional a $f(t)$ con sentido hacia el origen. Entonces,

$$f''(t) = -cte \cdot f(t), \qquad (cte > 0).$$

Es decir, $f(t)$ cumple la ecuación diferencial

$$(D^2 + cte)(f) = 0.$$

Como $x^2 + cte = (x - \sqrt{cte}\cdot i)(x + \sqrt{cte}\cdot i)$, tenemos que $f(t) = a\cos(cte\cdot t) + b\,\mathrm{sen}(cte\cdot t)$. Como $f(0) = 0$, entonces $a = 0$ y

$$f(t) = b \cdot \mathrm{sen}(cte \cdot t).$$

Observemos que b es la máxima elongación del muelle y $\frac{2\pi}{cte}$ el periodo del movimiento armónico.

95. Ejercicio: Resuelve la ecuación diferencial: $f'' + f = 0$.

Ecuaciones diferenciales lineales no homogéneas

Hasta ahora hemos resuelto ecuaciones diferenciales del tipo $P(D)(f) = 0$. Consideremos ahora una ecuación diferencial del tipo $P(D)(f) = g$, con $g \in F$. Sea f_0 una solución particular. Entonces, $f \in F$ cumple que $P(D)(f) = g$ si y sólo si

$$f = f_0 + f_1, \text{ con } f_1 \in \mathrm{Ker}\, P(D).$$

Dicho con palabras

$$\left[\begin{array}{l}\text{Todas las soluciones}\\ \text{de } P(D)(f) = g\end{array}\right] = \left[\begin{array}{l}\text{Una solución particu-}\\ \text{lar de } P(D)(f) = g\end{array}\right] + \left[\begin{array}{l}\text{Todas las soluciones de la}\\ \text{“homogénea” } P(D)(f) = 0\end{array}\right]$$

96. Ejemplo: Consideremos un objeto en caída libre. Supongamos que no hay más fuerza de rozamiento que la producida por el aire por causa de la velocidad del objeto. Supongamos que el rozamiento es proporcional a la velocidad. Planteemos la ecuación:

Sea $V(t)$ la velocidad del objeto. La aceleración del objeto será igual a la gravedad g menos una constante por la velocidad (debido a la fuerza de rozamiento). Luego,

$$V'(t) = g - R \cdot V(t) \quad (R > 0).$$

Es decir, $(D + R \cdot \mathrm{Id})V = g$. Una solución particular de esta ecuación es $V_0 = \frac{g}{R}$. Luego, todas las soluciones son $V = \frac{g}{R} + K' \cdot e^{-Rt}$. Si $V(0) = 0$, entonces $K' = \frac{-g}{R}$ y

$$V(t) = \frac{g}{R}(1 - e^{-Rt}).$$

Denotemos $S(t)$ los metros recorridos en el tiempo t, entonces $V(t) = S'(t)$ e integrando $S(t) = \int \frac{g}{R}(1 - e^{-Rt}) = a + \frac{g}{R}(t + \frac{e^{-Rt}}{R})$. Como $S(0) = 0$, entonces $a = \frac{-g}{R^2}$ y

$$S(t) = \frac{g}{R}t + \frac{g}{R^2}(-1 + e^{-Rt}).$$

97. Supongamos que tenemos una ecuación diferencial $P(D)f = g$, con $g \in F$, de la que sabemos que existe un polinomio $Q(x)$ primo con $P(x)$ tal que $Q(D)g = 0$. Veamos como resolverla:

Sean $\lambda(x)$ y $\mu(x)$ polinomios tales que $\lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = 1$. Por lo tanto, tenemos que $\lambda(D) \cdot P(D) + \mu(D) \cdot Q(D) = \mathrm{Id}$. Si aplicamos esta igualdad a g, obtenemos

$$g = \mathrm{Id}(g) = (\lambda(D) \cdot P(D) + \mu(D) \cdot Q(D))(g) = (\lambda(D) \cdot P(D))(g) = P(D)(\lambda(D)(g)).$$

Por tanto, una solución particular es $f = \lambda(D)(g)$.

De otro modo: $g \in \langle g, g', g'', \ldots, g^{n)}, \ldots \rangle \subseteq \mathrm{Ker}\, Q(D)$ que es un espacio vectorial de dimensión finita y $P(D)$: $E \to E$, $f \mapsto P(D)(f)$ es un isomorfismo (pues su inverso es $\lambda(D)$). Solo tenemos que calcular $f \in E$ tal que $P(D)(f) = g$.

98. Ejemplo: Resolvamos la ecuación diferencial $f''' - f = x^3$: Tenemos que resolver la ecuación $(D^3 - \mathrm{Id})(f) = x^3$. Observemos que $D^4(x^3) = 0$. Los polinomios $x^3 - 1$ y x^4 son primos entre sí. Tenemos

$$\begin{aligned} \underline{x^4} &= \underline{(x^3 - 1)} \cdot x + \underline{x} \\ \underline{x^3 - 1} &= \underline{x} \cdot x^2 - 1 \end{aligned}$$

Luego, $1 = \underline{x} \cdot x^2 - \underline{(x^3 - 1)} = (\underline{x^4} - \underline{(x^3 - 1)} \cdot x) \cdot x^2 - \underline{(x^3 - 1)} = x^2 \cdot \underline{x^4} + (-x^3 - 1) \cdot \underline{(x^3 - 1)}$. Por lo tanto,

$$\begin{aligned} x^3 &= (D^2 \cdot D^4 + (-D^3 - \mathrm{Id}) \cdot (D^3 - \mathrm{Id}))(x^3) = ((-D^3 - \mathrm{Id}) \cdot (D^3 - \mathrm{Id}))(x^3) \\ &= (D^3 - \mathrm{Id})((-D^3 - \mathrm{Id})(x^3)) = (D^3 - \mathrm{Id})(-6 - x^3). \end{aligned}$$

Luego una solución particular de la ecuación diferencial es $f_0 = -6 - x^3$. De otro modo: Sea $\operatorname{Ker} D^4 = \langle 1, x, x^2, x^3 \rangle$. El endomorfismo lineal $D^3 - \mathrm{Id} \colon \operatorname{Ker} D^4 \to \operatorname{Ker} D^4$, $p(x) \mapsto (D^3 - \mathrm{Id})(p(x))$ es un isomorfismo lineal y es fácil calcular el polinomio $ax^3 + bx^2 + cx + d$ que cumple que $(D^3 - \mathrm{Id})(ax^3 + bx^2 + cx + d) = x^3$.

Todas las soluciones son

$$\begin{aligned} f_0 + \operatorname{Ker}(D^3 - \mathrm{Id}) &= f_0 + \operatorname{Ker}(D - \mathrm{Id}) + \operatorname{Ker}(D - \frac{-1 - \sqrt{-3}}{2} \cdot \mathrm{Id}) + \operatorname{Ker}(D - \frac{-1 + \sqrt{-3}}{2} \cdot \mathrm{Id}) \\ &= -6 - x^3 + a \cdot e^x + b \cdot e^{\frac{-1-\sqrt{-3}}{2} \cdot x} + c \cdot e^{\frac{-1+\sqrt{-3}}{2} \cdot x}. \end{aligned}$$

Todas las soluciones que son funciones con valores reales son

$$-6 - x^3 + a \cdot e^x + e^{\frac{-1}{2}x} \cdot (c \cdot \cos \frac{\sqrt{3}}{2} x + d \cdot \operatorname{sen} \frac{\sqrt{3}}{2} x).$$

99. Ejercicio: Resuelve la ecuación diferencial $f'' - f = senx$.

100. Resolvamos la ecuación diferencial $f''' - 2f'' + f = xe^x$ siguiendo otro método: Tenemos $(D^3 - 2D^2 + \mathrm{Id})(f) = xe^x$, luego una solución particular es

$$\begin{aligned} f &= \frac{1}{D^3 - 2D^2 + \mathrm{Id}} xe^x = \frac{1}{(D^2 - D - \mathrm{Id})(D - \mathrm{Id})} xe^x = e^x \frac{1}{(D^2 + D - \mathrm{Id})D} x \\ &\overset{*}{=} e^x(-\mathrm{Id} - D - 2D^2)\frac{1}{D} x = e^x(\frac{-x^2}{2} + cte - x - 2) = e^x(\frac{-x^2}{2} - x + a) \end{aligned}$$

($*$ el desarrollo de Taylor de $\frac{1}{x^2+x-1}$ en $x = 0$ hasta orden tres es $-1 - x - 2x^2$).

101. Vamos a denotar $\int f = \frac{1}{D} f$ y en general $\int \overset{n}{\cdots} \int f = \frac{1}{D^n} f$.

Sea $P(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$. Existen polinomios $Q_1(x), \ldots, Q_r(x)$ tales que

$$\frac{1}{(x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}} = \frac{Q_1(x)}{(x - \alpha_1)^{n_1}} + \overset{r}{\cdots} + \frac{Q_r(x)}{(x - \alpha_r)^{n_r}}$$

Resolvamos la ecuación diferencial $P(D)f = g$.

$$\begin{aligned} f &= \frac{1}{P(D)} g = (\frac{Q_1(D)}{(D - \alpha_1 \mathrm{Id})^{n_1}} + \overset{r}{\cdots} + \frac{Q_r(D)}{(D - \alpha_r \mathrm{Id})^{n_r}}) g = \sum_i \frac{Q_i(D)}{(D - \alpha_i \mathrm{Id})^{n_i}} g \\ &\overset{0.6.87}{=} \sum_i e^{\alpha_i x} \cdot \frac{Q_i(D + \alpha_i \mathrm{Id})}{D^{n_i}} e^{-\alpha_i x} \cdot g = \sum_i e^{\alpha_i x} \cdot Q_i(D + \alpha_i \mathrm{Id}) \int \overset{n_i}{\cdots} \int e^{-\alpha_i x} \cdot g \end{aligned}$$

Ecuaciones en diferencias finitas

Sea $S = \{(a_n)_{n\in\mathbb{N}}\}$ el $\mathbb{C}$-espacio vectorial de las sucesiones de números complejos. La sucesión $(a_n)_{n\in\mathbb{N}}$ muchas veces la denotaremos simplemente (a_n). Consideremos el "operador siguiente" $\nabla\colon S \to S$ que es el endomorfismo $\mathbb{C}$-lineal definido por

$$\nabla(a_n) = (b_n), \text{ donde } b_n = a_{n+1}.$$

Diremos que $\Delta := \nabla - \mathrm{Id}$ es el "operador diferencia".

Como sabemos, dado un polinomio $P(x) = c_r x^r + c_{r-1}x^{r-1} + \cdots + c_0 \in \mathbb{C}[x]$, podemos considerar el endomorfismo lineal $P(\nabla)\colon S \to S$ definido por

$$\begin{aligned} P(\nabla)(a_n) &= (c_r\nabla^r + c_{r-1}\nabla^{r-1} + \cdots + c_0\,\mathrm{Id})(a_n) \\ &= (c_r a_{n+r} + c_{r-1}a_{n+r-1} + \cdots + c_0 a_n). \end{aligned}$$

Queremos resolver las ecuaciones en diferencias finitas (homogéneas)

$$c_r a_{n+r} + c_{r-1}a_{n+r-1} + \cdots + c_0 a_n = 0.$$

Queremos calcular a_n, es decir, queremos calcular $\mathrm{Ker}\,P(\nabla)$.

102. Proposición: *Se cumple que* $\{(1),(n),\ldots,(n^{r-1})\}$ *es una base de* $\mathrm{Ker}\,\Delta^r$

Demostración. Obviamente, $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Si $p(n)$ es un polinomio de grado s, es fácil ver que $\Delta(p(n))$ es un polinomio de grado $s-1$. Por tanto, $\{(1),(n),\ldots,(n^{r-1})\} \subseteq \mathrm{Ker}\,\Delta^r$. Consideremos la aplicación lineal

$$\Delta\colon \mathrm{Ker}\,\Delta^s \to \mathrm{Ker}\,\Delta^{s-1},\ (a_n) \mapsto \Delta(a_n),$$

cuyo núcleo es $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Por tanto, $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^s \le \dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^{s-1} + 1$. Recurrentemente, obtenemos que $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^r \le r$. Por dimensiones $\langle(1),(n),\ldots,(n^{r-1})\rangle = \mathrm{Ker}\,\Delta^r$. □

103. Fórmula de conmutación: Sea $p(x) \in \mathbb{C}[x]$ y (a_n) una sucesión de números complejos. Entonces,

$$p(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\nabla)(a_n).$$

Demostración. En efecto, $\nabla((\alpha^n)\cdot(a_n)) = \nabla(\alpha^n \cdot a_n) = (\alpha^{n+1}\cdot a_{n+1}) = (\alpha^n)\cdot(\alpha\cdot\nabla)(a_n)$. Por tanto, $\nabla^2((\alpha^n)\cdot(a_n)) = \nabla((\alpha^n)\cdot(\alpha\nabla)(a_n)) = (\alpha^n)\cdot(\alpha\cdot\nabla)^2(a_n)$. Recurrrentemente obtenemos $\nabla^r((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot(\alpha\nabla)^r(a_n)$ y $p(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\nabla)(a_n)$. □

Por lo tanto,

$$\boxed{p(\nabla - \alpha)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\cdot\Delta)(a_n)}$$

104. Teorema: *Se cumple que*

1. $\mathrm{Ker}(\nabla - \alpha\cdot \mathrm{Id})^r = (\alpha^n)\cdot\{$*(pol. $q(n)$ de grado menor que r)*$\}$ *(suponemos* $\alpha \neq 0$*).*

2. *Si* $p(x) = (x-\alpha_1)^{r_1}\cdots(x-\alpha_s)^{r_s}$*, con* $\alpha_i \neq 0$ *para todo* i*, entonces*

$$\mathrm{Ker}\, p(\nabla) = (\alpha_1{}^n)\cdot\{(\textit{Pol. } q(n) \textit{ de grado} < r_1)\} \oplus \overset{r}{\cdots} \oplus (\alpha_s^n)\cdot\{\textit{Pol. } q(n) \textit{ de grado} < r_s\}.$$

Demostración. 1. $(s(n)) \in \mathrm{Ker}(\nabla-\alpha)^r \iff 0 = (\nabla-\alpha)^r(s(n)) \iff 0 = (\nabla-\alpha)^r((\alpha^n)\cdot(\alpha^{-n})\cdot(s(n))) = (\alpha^n)\cdot(\alpha\Delta)^r((\alpha^{-n})\cdot(s(n))) \iff 0 = \Delta^r((\alpha^{-n})\cdot(s(n))) \iff$ existe un polinomio $q(n)$ de grado menor que r tal que $\alpha^{-n}\cdot s(n) = q(n)$, es decir, $s(n) = \alpha^n\cdot q(n)$.

2. Es consecuencia de que $\mathrm{Ker}\, p(\nabla) = \mathrm{Ker}(\nabla - \alpha_1\,\mathrm{Id})^{n_1} \oplus \cdots \oplus \mathrm{Ker}(\nabla - \alpha_r\,\mathrm{Id})^{n_r}$ y de 2. □

105. Nota: Supongamos $P(x) \in \mathbb{R}[x]$ y $\alpha = \rho\cdot(\cos\beta + i\cdot\mathrm{sen}\,\beta)$ es una raíz compleja de $P(x)$, con $\beta \neq 0, \pi$. Entonces, $P(x) = (x-\alpha)^r\cdot(x-\bar\alpha)^r\cdot Q(x)$, con $Q(\alpha), Q(\bar\alpha) \neq 0$. Es facil probar, a partir de 0.6.104, que

$$\left\{\begin{array}{l}(s(n)) \in \mathrm{Ker}(\nabla-\alpha\,\mathrm{Id})^n \oplus \mathrm{Ker}(\nabla-\bar\alpha\,\mathrm{Id})^r \\ \text{tales que } s(n)\in\mathbb{R} \text{ para todo } n\end{array}\right\} =$$

$$\rho^n\cdot\cos(\beta\cdot n)\cdot\left\{\begin{array}{l}\text{Pol. } p(n) \text{ con coef.}\\ \text{reales de grado } < r\end{array}\right\} + \rho^n\cdot\mathrm{sen}(\beta\cdot n)\cdot\left\{\begin{array}{l}\text{Pol. } p(n) \text{ con coef.}\\ \text{reales de grado } < r\end{array}\right\}.$$

106. Ejemplo: Resolvamos la ecuación $a_{n+2} = a_{n+1} + a_n$, con las condiciones iniciales $a_0 = 0, a_1 = 1$ (sucesión de Fibonacci). "Esta sucesión fue descrita por Leonardo de Pisa, matemático italiano del siglo XIII también conocido como Fibonacci. Tiene numerosas aplicaciones en ciencias de la computación, matemática y teoría de juegos. También aparece en configuraciones biológicas, como por ejemplo en las ramas de los árboles, en la disposición de las hojas en el tallo, en las flores de alcachofas y girasoles, en las inflorescencias del brécol romanesco, en la configuración de las piñas de las coníferas, en la reproducción de los conejos y en cómo el ADN codifica el crecimiento de formas orgánicas complejas. De igual manera, se encuentra en la estructura espiral del caparazón de algunos moluscos, como el nautilus." (Wikipedia). Tenemos que $a_{n+2} - a_{n+1} - a_n = 0$, luego

$$(\nabla^2 - \nabla - \mathrm{Id})(a_n) = (0).$$

Por tanto, $(a_n) \in \mathrm{Ker}(\nabla^2 - \nabla - \mathrm{Id})$. Observemos que $x^2 - x - 1 = (x - \frac{1+\sqrt{5}}{2})\cdot(x - \frac{1-\sqrt{5}}{2})$, luego

$$\mathrm{Ker}(\nabla^2 - \nabla - \mathrm{Id}) = \mathrm{Ker}(\nabla - \frac{1+\sqrt{5}}{2}\cdot\mathrm{Id}) \oplus (\nabla - \frac{1-\sqrt{5}}{2}\cdot\mathrm{Id}) = \{(a\cdot(\frac{1+\sqrt{5}}{2})^n + b\cdot(\frac{1-\sqrt{5}}{2})^n)\}.$$

Recordemos que

$$0 = a_0 = a + b$$
$$1 = a_1 = a \cdot (\tfrac{1+\sqrt{5}}{2}) + b \cdot (\tfrac{1-\sqrt{5}}{2})$$

Resulta que $a = \frac{1}{\sqrt{5}}$ y $b = -\frac{1}{\sqrt{5}}$. Luego,

$$a_n = \frac{1}{\sqrt{5}} \cdot (\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}} \cdot (\frac{1-\sqrt{5}}{2})^n.$$

107. Ejercicio: Calcula cuántos números de longitud n se pueden escribir con ceros y unos, de modo que nunca aparezcan dos ceros seguidos (ejemplo: los números de longitud tres cumpliendo lo dicho son $010, 011, 101, 110, 111$, que son cinco distintos).

108. Ejercicio: Calcula $\operatorname{Ker} \nabla^r$.

Ecuaciones en diferencias finitas no homogéneas

Consideremos una ecuación en diferencias $p(\nabla)(s(n)) = z(n)$. Sea $(s_0(n))$ una solución particular. Entonces, $(s(n))$ es una solución de la ecuación en diferencias si y sólo si

$$s(n) = s_0(n) + t(n), \text{ con } t(n) \in \operatorname{Ker} p(\nabla).$$

Con palabras

$$\left[\begin{array}{l}\text{Todas las soluciones}\\ \text{de } P(\nabla)(s(n)) = (z(n))\end{array}\right] = \left[\begin{array}{l}\text{Solución particular}\\ \text{de } P(\nabla)(s(n)) = (z(n))\end{array}\right] + \left[\begin{array}{l}\text{Todas las soluciones de la}\\ \text{“homogénea” } P(\nabla)(s(n)) = 0\end{array}\right]$$

109. Resolvamos la ecuación $p(\nabla)(s(n)) = z(n)$, suponiendo que existe un polinomio $q(x)$ primo con $p(x)$ de modo que $q(\nabla)(z(n)) = 0$:

Sean $\lambda(x)$ y $\mu(x)$ tales que $\lambda(x) \cdot p(x) + \mu(x) \cdot q(x) = 1$. Por tanto, $\lambda(\nabla) \cdot p(\nabla) + \mu(\nabla) \cdot q(\nabla) = \mathrm{Id}$. Si aplicamos esta igualdad a $(z(n))$, obtenemos

$$(z(n)) = \lambda(\nabla) \cdot p(\nabla)(z(n)) = p(\nabla)(\lambda(\nabla)(z(n))).$$

Por tanto, una solución particular es $s_0(n) = \lambda(\nabla)(z(n))$.

110. Ejemplo: Resolvamos $a_{n+2} + 2a_{n+1} - 6a_n = 2^n$: Tenemos que resolver

$$(\nabla^2 + 2\nabla - 6\,\mathrm{Id})(a_n) = (2^n).$$

Calculemos una solución particular. Observemos que $(\nabla - 2\,\mathrm{Id})(2^n) = (0)$ y que los polinomios x^2+2x-6 y $x-2$ son primos entre sí. Mediante el algoritmo de Euclides sabemos calcular $\lambda(x), \mu(x)$ de modo que $\lambda(x)\cdot(x^2+2x-6)+\mu(x)\cdot(x-2)=1$. En efecto,

$$x^2+2x-6 = (x+4)(x-2)+2.$$

Luego, $1 = \frac{1}{2}\cdot(x^2+2x-6) - \frac{x+4}{2}(x-2)$. Luego,

$$\begin{aligned}(2^n) &= (\frac{1}{2}\cdot(\nabla^2+2\nabla-6\,\mathrm{Id}) - \frac{\nabla+4\,\mathrm{Id}}{2}(\nabla-2\,\mathrm{Id}))(2^n) = \frac{1}{2}\cdot(\nabla^2+2\nabla-6\,\mathrm{Id})(2^n)\\ &= (\nabla^2+2\nabla-6\,\mathrm{Id})(\frac{1}{2}2^n)\end{aligned}$$

Luego, (2^{n-1}) es una solución particular. Procedamos de otro modo:

$$(a_n) = \frac{1}{\nabla^2+2\nabla-6\,\mathrm{Id}}(2^n) = \frac{1}{2^2+2\cdot 2-6}(2^n) = (2^{n-1}).$$

($(\nabla-2\,\mathrm{Id})(2^n)=0$ y el desarrollo de Taylor de $\frac{1}{x^2+2x-6}$ de orden 0 en $x=2$ es $\frac{1}{2^2+2\cdot 2-6}$).

Todas las soluciones son

$$\begin{aligned}a_n = 2^{n-1} + \mathrm{Ker}(\nabla^2+2\nabla-6\,\mathrm{Id}) &= 2^{n-1} + \mathrm{Ker}(\nabla-(-1+\sqrt{7})) + \mathrm{Ker}(\nabla-(-1-\sqrt{7}))\\ &= 2^{n-1} + a\cdot(-1+\sqrt{7})^n + b\cdot(-1-\sqrt{7})^n.\end{aligned}$$

111. Préstamos: Un banco nos presta un capital K, a devolver en N años, a un tipo de interés anual I. ¿Cuánto dinero D deberemos pagar al año, de modo que todos los años paguemos la misma cantidad y en los N años hayamos saldado nuestra deuda con el banco?

Resolución: Sea i_n el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n (por el capital K que nos han prestado). Entonces $D = a_n + i_n$. Además, $i_n = I\cdot(K - \sum_{r=1}^{n-1} a_r)$. Por tanto, $D = a_n + I\cdot(K-\sum_{r=1}^{n-1} a_r)$. Si aplicamos el operador diferencia Δ entonces

$$0 = \Delta(a_n) - I\cdot a_n = (\nabla - (1+I))(a_n).$$

Por tanto, $a_n = (1+I)^n\cdot\lambda$ y

$$D = a_1 + IK = (1+I)\cdot\lambda + IK. \qquad (*)$$

Tenemos que calcular λ. Nos falta decir que amortizamos el préstamo en N años, es decir, $K = \sum_{r=1}^{N} a_r$, que equivale a decir que $D = a_{N+1} = (1+I)^{N+1}\cdot\lambda$. Despejando λ y sustituyendo su valor en $(*)$ obtendremos que

$$D = \frac{IK}{1-\frac{1}{(1+I)^N}}.$$

112. Préstamos con gradiente lineal: Por la compra de un coche en un concesionario pagaremos cada año n un dinero d_n de modo que $d_n = A + G\cdot(n-1)$ (con $A = 1000$ y $G = 100$), durante $N = 20$ años. Se supone que el tipo de interés anual es $I = 5\%$. Calcula el valor K del coche (en la actualidad).

Resolución: Podemos decir que nos han prestado un capital K a un tipo de interés I a devolver en N años y que cada año n pagamos (por la amortización y los intereses) d_n. Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I\cdot(K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$A + G\cdot(n-1) = d_n = a_n + I\cdot(K - \sum_{r=1}^{n-1} a_r). \qquad (*)$$

Para $n = 1$, tenemos que

$$A = a_1 + I\cdot K \qquad (**)$$

Tenemos que determinar a_1. Aplicando Δ en $(*)$ obtenemos

$$G = \Delta(a_n) - I\cdot(a_n) = (\Delta - I)(a_n) = (\nabla - (1+I))(a_n)$$

Una solución particular, es $a_n = \frac{-G}{I}$ y todas las soluciones son $a_n = \frac{-G}{I} + cte\cdot(1+I)^n$. Luego, $a_1 = \frac{-G}{I} + cte\cdot(1+I)$. Tenemos que calcular cte. Nos falta imponer que $\sum_{i=1}^{N} a_n = K$, es decir, $A + GN = d_{N+1} = a_{N+1} = -\frac{G}{I} + cte\cdot(1+I)^{N+1}$. Luego, $cte = \frac{A+GN+\frac{G}{I}}{(1+I)^{N+1}}$. En conclusión

$$a_1 = -\frac{G}{I} + \frac{A+GN+\frac{G}{I}}{(1+I)^{N+1}}\cdot(1+I) = -\frac{G}{I} + \frac{A+GN+\frac{G}{I}}{(1+I)^N}$$

Sustituyendo el valor de a_1 en $(**)$, puede comprobarse que

$$K = \frac{A}{I}\cdot\frac{(1+I)^N - 1}{(1+I)^N} + \frac{G}{I^2}\cdot\frac{(1+I)^N - 1 - IN}{(1+I)^N} = 22311'1.$$

Supongamos que voy a un banco que me ofrece un interés anual $I = 1\%$ por mi dinero. Tendría que depositar $K = 34592$ euros para que el banco me fuese dando cada año lo que el concesionario me pide (y al final el banco quedase en paz conmigo). En fin, un coche de 22311 euros me ha costado 34592 euros.

113. Préstamos de gradiente exponencial: Un préstamo de $K = 10^5$ euros se quiere devolver durante $N = 20$ años, pagando cada año n una anualidad d_n de modo que $d_n = I' d_{n-1}$ ($I' = 1 + 2\%$). Se supone que nos prestan el dinero a un tipo de interés anual $I = 5\%$. Calculemos d_1.

Resolución: Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$d_n = a_n + I \cdot (K - \sum_{r=1}^{n-1} a_r).$$

Si aplicamos el operador diferencia Δ, entonces $\Delta(d_n) = \Delta(a_n) - I \cdot a_n = (\nabla - (1+I))(a_n)$. Por otra parte, $(\nabla - I')(d_n) = 0$ (luego $d_n = \lambda' I'^n$). Por tanto, si aplicamos $\nabla - I'$, obtenemos que

$$(\nabla - I')(\nabla - (1+I))(a_n) = 0$$

Por tanto, $a_n = \lambda I'^n + \mu(1+I)^n$. Sabemos que $d_{N+1} = a_{N+1}$, de lo que se deduce que $\lambda' = \lambda + \mu(\frac{1+I}{I'})^{N+1}$. De las ecuaciones

$$\lambda' I' = d_1 = a_1 + IK = \lambda I' + \mu(1+I) + IK$$
$$\lambda' I'^2 = d_2 = a_2 + I(K - a_1) = \lambda I'(I' - I) + \mu(1+I) + IK$$

se obtiene que $d_1 = \frac{K(1-I'+I)}{1-(\frac{I'}{1+I})^N}$.

114. Sumatorios: Dada una sucesión de números complejos (a_n), definamos la sucesión $s_n := \sum_{i=0}^{n-1} a_i$ (y $s_0 := 0$). Entonces, $\Delta(s_n) = (s_{n+1} - s_n) = (a_n)$. Denotaremos

$$\frac{1}{\Delta_0}(a_n) := (\sum_{i=0}^{n-1} a_i).$$

Como hemos dicho, $\Delta(\frac{1}{\Delta_0}(a_n)) = (a_n)$, luego $\Delta^{-1}(a_n) = \frac{1}{\Delta_0}(a_n) + \{(cte),\ \forall\, cte \in \mathbb{C}\}$.

Se define $\binom{n}{i} := \frac{n\cdot(n-1)\cdots(n-i+1)}{i\cdot(i-1)\cdots 2\cdot 1}$. Observemos que

$$\langle (1),(n),\ldots,(n^r)\rangle = \langle (\binom{n}{0}),(\binom{n}{1}),\ldots,(\binom{n}{r})\rangle.$$

Además, $\Delta(\binom{n}{r}) = (\binom{n}{r-1})$. Por tanto, $\frac{1}{\Delta_0}(\binom{n}{r}) = \binom{n}{r+1}$.

Si escribimos $p(n) = \sum_{i=0}^{r} \lambda_i \binom{n}{i}$, tendremos que

$$\lambda_0 = p(0), \ldots, \lambda_i = p(i) - \binom{i}{i-1}\lambda_{i-1} - \cdots - \binom{i}{0}\lambda_0,$$

y $\sum_{i=0}^{n-1} p(i) = \frac{1}{\Delta_0}(p(n)) = \sum_{i=0}^{r} \lambda_i \binom{n}{i+1}$. Finalmente, $\sum_{i=0}^{n} p(i) = \sum_{i=0}^{r} \lambda_i \binom{n+1}{i+1}$.

115. Ejercicio: Calcular $\sum_{i=0}^{n}(i^2+i-3)$.

116. Ejemplo: Calculemos $\sum_{i=0}^{n} i\cdot 2^i$: Recordemos que $(\nabla-2\,\mathrm{Id})^2(n2^n)=0$. Entonces,

$$\begin{aligned}\sum_{i=0}^{n-1} i\cdot 2^i &= \frac{1}{\Delta_0}(n2^n) = (\frac{1}{\nabla-\mathrm{Id}}(n2^n))+(cte) \overset{*}{=} (\mathrm{Id}-(\nabla-2\,\mathrm{Id}))(n2^n)+(cte)\\ &= (n2^n - n2^{n+1}+cte) = ((n-2)2^n+cte)\end{aligned}$$

($\overset{*}{=}$ el desarrollo de Taylor de $\frac{1}{x-1}$ de orden 2 en $x=2$, es $1-(x-2)+h(x)(x-2)^2$). Luego,

$$\sum_{i=0}^{n} i\cdot 2^i = (n-1)\cdot 2^{n+1}+2.$$

Teorema de clasificación de módulos sobre dominios de ideales principales

Sea M un A-módulo anulado por $\mathfrak{m}_x^n$, luego M es un $A/\mathfrak{m}_x^n$-módulo. Si $a\notin\mathfrak{m}_x$ entonces $\bar{a}$ es invertible en $A/\mathfrak{m}_x^n$, y por tanto, el morfismo $M \overset{a\cdot=\bar{a}\cdot}{\longrightarrow} M$ es un isomorfismo. En consecuencia, $M=M_x$ y es un A_x-módulo. En particular, $(A/\mathfrak{m}_x^n)=(A/\mathfrak{m}_x^n)_x = A_x/(\mathfrak{m}_x^n A_x)$. Por otra parte, si $x\neq y\in \operatorname{Spec} A$, entonces $M_y=0$.

Por tanto, si A es un dominio de ideales principales y M es un A-módulo finito generado de torsión, entonces (ver teorema 0.6.84)

$$M_x = (\operatorname{Ker} p_1^{n_1}\oplus\cdots\oplus\operatorname{Ker} p_s^{n_s})_x = \begin{cases} 0 & \text{si } \mathfrak{m}_x\neq(p_i), \text{ para todo } i.\\ \operatorname{Ker} p_i^{n_i} & \text{si } \mathfrak{m}_x=(p_i).\end{cases}$$

Luego si $\{x_1,\dots,x_r\}$ son los puntos cerrados del soporte de M, $M=M_{x_1}\oplus\cdots\oplus M_{x_r}$.

117. Proposición: *Dos módulos finito generados sobre un dominio de ideales principales son isomorfos si y solo si son localmente isomorfos.*

Demostración. Sean M y M' localmente isomorfos. Localizando en el punto genérico obtenemos que ambos tienen el mismo rango. Como la torsión de un módulo conmuta con localizaciones, entonces $T(M)$ y $T(M')$ son localmente isomorfos. Luego, como acabamos de ver $T(M)$ y $T(M')$ son isomorfos. Por el primer teorema de descomposición M y M' son isomorfos.

□

118. Definición: Un A-módulo M se dice que es de presentación finita si existe una sucesión exacta de la forma $A^m\to A^n\to M\to 0$ (con $n,m<\infty$). Con otras palabras, M es de presentación finita si es isomorfo al cociente de un módulo libre finito generado por un submódulo finito generado.

Seguimos la convención $A^0 = \{0\}$. Obviamente, los A-módulos libres finito generados son A-módulos de presentación finita.

Los A-módulos de presentación finita son finito generados.

119. Proposición: *Sea A un anillo noetheriano. Un A-módulo M es de presentación finita si y solo si M es finito generado.*

Demostración. Supongamos que $M = \langle m_1, \dots, m_n \rangle$ es un A-módulo finito generado. Consideremos el epimorfismo $\pi\colon A^n \to M$, $\pi((a_i)) := \sum_i a_i m_i$. $\operatorname{Ker}\pi = \langle n_1, \dots, n_m \rangle$ es finito generado porque es un submódulo del módulo noetheriano A^n, luego M es de presentación finita. □

120. Definición: Dada una sucesión exacta de A-módulos, $A^m \xrightarrow{\varphi} A^n \xrightarrow{\pi} M \to 0$, diremos que es una presentación libre de M.

Observemos que $M = \operatorname{Coker}\varphi := A^n/\operatorname{Im}\varphi$, luego, la clasificación y estudio de M equivale a la clasificación y estudio de la matriz asociada a φ.

121. Proposición: *Sea A un dominio de ideales principales local, de ideal maximal $\mathfrak{m} = (p)$. Sea $\phi\colon A^m \to A^n$ un morfismo de A-módulos. Se cumple que existen bases $\{e_1, \dots, e_m\}$, $\{e'_1, \dots, e'_n\}$ en A^m y A^n, de modo que $\phi(e_i) = \lambda_i e'_i$, para $1 \le i \le m$.*[4]

Demostración. Sea (a_{ij}) la matriz asociada a ϕ, en las bases estándar $\{u_1, \dots, u_m\}$, $\{u'_1, \dots, u'_n\}$ de A^m y A^n. Si en vez de $\{u_1, \dots, u_m\}$, consideramos la base que se obtiene permutando dos vectores de $\{u_1, \dots, u_m\}$, la matriz de ϕ en las nuevas bases, se obtiene permutando las correspondientes columnas de la matriz (a_{ij}). Igualmente, si permutamos dos vectores de $\{u'_1, \dots, u'_n\}$, la matriz de ϕ se obtiene permutando las correspondientes filas de (a_{ij}). Si en vez de $\{u_1, \dots, u_m\}$, consideramos la base $\{u_1, \dots, u_i \overset{i}{-} a_j u_j, \dots, u_m\}$, la matriz de ϕ en las nuevas bases, se obtiene cambiando la columna i, C_i de la matriz (a_{ij}) por la columna $C_i - a_j C_j$. Si en vez de la base $\{u'_1, \dots, u'_m\}$, consideramos la base $\{u'_1, \dots, u'_i \overset{i}{-} a_j u'_j, \dots, u'_n\}$, la matriz de ϕ en las nuevas bases, se obtiene cambiando la fila i, F_i de la matriz (a_{ij}) por la fila $F_j + a_j F_i$.

Este tipo de transformaciones de la matriz (a_{ij}) (o equivalentemente de las bases $\{u_i\}, \{u'_i\}$) las denominaremos transformaciones elementales. Vamos a probar que mediante transformaciones elementales la matriz de ϕ es "diagonal", es decir, $\phi(e_i) = \lambda_i e'_i$, para todo i.

Dado $a \in A$, tendremos que $a = p^i \cdot b$, con b no divisible por p, es decir, $b \notin \mathfrak{m} = (p)$, luego b invertible. Por tanto, $(a) = (p^i)$. Sea p^i el máximo común divisor de todos los a_{ij}. Existe un a_{rs}, tal que $(a_{rs}) = (p^i)$. Por tanto, a_{rs} divide a todos los coeficientes a_{ij}.

[4] Si $i > n$, decimos que $\phi(e_i) = 0$.

Permutando filas y columnas podemos suponer que $r = 1$ y $s = 1$. Transformando las columnas C_i por $C_i - \frac{a_{1i}}{a_{11}}C_1$ para $i > 1$, y posteriormente las filas F_i por $F_i - \frac{a_{i1}}{a_{11}}F_1$, obtendremos la matriz

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}$$

Procediendo del mismo modo reiteradamente, con la matriz (b_{ij}), "diagonalizaremos" ϕ.

□

122. Definición: Diremos que un A-módulo es monógeno si está generado por un elemento.

Si $M = \langle m \rangle$ entonces $M \simeq A/\mathrm{Anul}(m)$. Si A es dominio de ideales principales local, de ideal maximal $\mathfrak{m} = (p)$, entonces los únicos ideales son de la forma (p^i), y los módulos monógenos son isomorfos a $A/(p^i)$.

123. Tercer teorema de descomposición: *Sea A un dominio de ideales principales y M un A-módulo finito generado, de ideal anulador $p^n A$, siendo $p \in A$ irreducible. Se cumple que*

$$M \simeq A/p^{n_1}A \oplus \cdots \oplus A/p^{n_r}A$$

con $n_i \leq n$, determinados unívocamente por M. Es decir, M es suma directa de monógenos de modo único, salvo isomorfismos.

Demostración. Podemos suponer que A es local, de ideal maximal $\mathfrak{m} = (p)$. Sabemos que existe una sucesión exacta

$$A^m \xrightarrow{\phi} A^n \to M \to 0$$

y $M = \mathrm{Coker}\,\phi$. Por la proposición anterior, existen bases $\{e_1, \dots, e_m\}$, $\{e'_1, \dots, e'_n\}$ de A^m y A^n, de modo que $\phi(e_i) = \lambda_i e'_i$, para todo i. Luego,

$$\begin{aligned} M = \mathrm{Coker}\,\phi &= [Ae_1 \oplus \cdots \oplus Ae_n]/[(\lambda_1)e_1 \oplus \dots (\lambda_m)e_m \oplus 0 \oplus \cdots \oplus 0] \\ &= A/(\lambda_1) \oplus \cdots \oplus A/(\lambda_m) \oplus A \oplus \cdots \oplus A \end{aligned}$$

y fácilmente concluimos.

Veamos la unicidad de los n_i. Reordenando tenemos

$$M = (A/p^n A)^{m_n} \oplus (A/p^{n-1}A)^{m_{n-1}} \oplus \cdots \oplus (A/pA)^{m_1}$$

con $m_i \geq 0$. Tenemos que ver que M determina los m_i.

Sea $p^i : M \to M$, $m \mapsto p^i \cdot m$. Si $M = A/p^r A$ entonces $\operatorname{Ker} p^i = (\bar{p}^{r-i})$, para $i \leq r$, y $\operatorname{Ker} p^i = (\bar{1})$, para $i \geq r$. Por tanto, $\operatorname{Ker} p^i/(\operatorname{Ker} p^{i-1} + p \cdot \operatorname{Ker} p^{i+1}) = 0$ si $i \neq r$ y $\operatorname{Ker} p^r/(\operatorname{Ker} p^{r-1} + p \cdot \operatorname{Ker} p^{r+1}) = \langle \bar{1} \rangle$ (que es un A/pA espacio vectorial de dimensión 1).

Ahora en general, $m_i = \dim_{A/pA} \operatorname{Ker} p^i/(\operatorname{Ker} p^{i-1} + p \cdot \operatorname{Ker} p^{i+1})$. □

124. Teorema de clasificación: *Sea A un dominio de ideales principales y M un A-módulo finito generado. Existe un isomorfismo de A-módulos*

$$M \simeq (A \oplus \overset{r}{\ldots} \oplus A) \oplus (\underset{i,j}{\oplus} A/p_i^{n_{i,j}} A)$$

donde los $p_i \in A$ son irreducibles y $n_{i,j} > 0$, r y p_i están unívocamente determinados por M.

Demostración. Es un consecuencia directa de los tres teoremas de descomposición. □

125. Definición: A las potencias $p_i^{n_{i,j}}$ del teorema de clasificación se les denomina divisores elementales de M.

126. Corolario: *Dos módulos finito generados son isomorfos si y solo si tienen el mismo rango y los mismos divisores elementales.*

127. Ejercicio: Prueba que si $r = 0$ entonces $\operatorname{Anul}(M) = m.c.m.\{p_i^{n_{i,j}}\}_{i,j} A$.

Consideremos una presentación de un A-módulo M finito generado, es decir, una sucesión exacta

$$A^m \xrightarrow{\psi} A^n \longrightarrow M \longrightarrow 0$$

Consideremos sendas bases $\{e'_1, \ldots, e'_m\}$ y $\{e_1, \ldots, e_n\}$ de A^m y A^n. Escribamos $\psi(e'_i) = \sum_j a_{ij} e_j$, así que (a_{ij}) es la matriz de ψ. Definimos entonces los siguientes ideales:

128. Definición: Se llama i-ésimo *ideal de Fitting* de M al ideal $F_i(M)$ generado por los menores de orden $n - i$ de la matriz de ψ. Si $n - i \leq 0$ seguiremos la convención $F_i(M) = (1)$ y si $m < n - i$ seguiremos la convención $F_i(M) = (0)$.

Veamos que los ideales de Fitting de un módulo no dependen de las bases elegidas en la presentación (véase también el teorema 0.10.4). Consideremos otra base $\{\bar{e}_1, \ldots, \bar{e}_m\}$ de A^m y escribamos $\psi(\bar{e}_j) = \sum_i \bar{a}_{ij} e_i$, así que la nueva matriz de ψ es $(\bar{a}_{ij})$. Denotemos $F_i(M)$ y $\bar{F}_i(M)$ a los respectivos ideales i-ésimos de Fitting de las matrices (a_{ij}) y $(\bar{a}_{ij})$. Cada $\bar{e}_j$ es combinación lineal de la antigua base $\{e'_1, \ldots, e'_m\}$ y, por lo tanto, cada columna de $(\bar{a}_{ij})$ es combinación lineal de las columnas de (a_{ij}). En consecuencia, los menores de orden $n - i$ de $(\bar{a}_{ij})$ son combinación lineal de los menores de (a_{ij}), es

decir, $\bar{F}_i(M) \subseteq F_i(M)$. Por simetría también se cumple $F_i(M) \subseteq \bar{F}_i(M)$; luego en conclusión $F_i(M) = \bar{F}_i(M)$. Si la que cambiamos es la base de A^n se razona de modo similar (por filas en vez de por columnas).

Dada la sucesión exacta $A^m \xrightarrow{\psi} A^n \to M \to 0$ y $x \in \operatorname{Spec} A$, entonces localizando en x la sucesión $A_x^m \xrightarrow{\psi_x} A_x^n \to M_x \to 0$ es exacta. La matriz asociada a ψ, es la misma que la asociada a ψ_x, por tanto $(F_i(M))_x = F_i(M_x)$.

129. Definición: Denotemos c_i al generador del ideal de Fitting i-ésimo, $F_i(M)$. A los elementos $\phi_i = c_{i-1}/c_i$ se les llama *factores invariantes* del módulo M. Si $c_i = c_{i-1} = 0$ diremos que $\phi_i = 0$.

130. Teorema de clasificación (segunda versión): *Sea A un dominio de ideales principales y M un A-módulo finito generado. Se cumple que*

$$M \simeq A/(\phi_1) \oplus \cdots \oplus A/(\phi_n)$$

Luego, dos A-módulos finito generados son isomorfos si y solo si poseen los mismos factores invariantes.

Demostración. Los ideales de Fitting conmutan con localizaciones y dos módulos finito generados sobre un dominio de ideales principales son isomorfos si y solo si lo son localmente. Por tanto, el teorema es local y podemos suponer que A es local de ideal maximal $\mathfrak{m} = (p)$.

Por el teorema 0.6.121, podemos suponer que tenemos bases $\{e_1, \ldots, e_m\}$ de A^m y $\{e'_1, \ldots, e'_n\}$ de A^n, de modo que $\psi(e_1) = p^{n_1} \cdot e'_1, \ldots, \psi(e_r) = p^{n_r} \cdot e'_r$, $\psi(e_{r+1}) = e'_{r+1}, \ldots, \psi(e_{r+r'}) = e'_{r+r'}$, $\psi(e_{r+r'+1}) = \cdots = \phi(e_m) = 0$, con $n_1 \geq n_2 \geq \cdots \geq n_r > 0$.

Tanto para el cálculo de M como para el cálculo de los ideales de Fitting podemos suponer que $r' = 0$. Podemos suponer también que $m = r$. Tenemos que

$$M \simeq A^{n-r} \oplus A/(p^{n_1}) \oplus \cdots \oplus A/(p^{n_r})$$

Es una sencilla comprobación que $c_0 = \ldots = c_{n-r-1} = 0$, $c_{n-r} = p^{n_1} \cdots p^{n_r}$, $c_{n-r+1} = p^{n_2} \cdots p^{n_r}$, $c_{n-1} = p^{n_r}$, $c_n = 1$ para $i \leq n - r$, $\phi_i = p^{n_i}$, para $i > n - r$. Ahora es sencillo concluir. □

131. Observaciones:

1. Por el cálculo efectuado en la demostración del teorema anterior, ϕ_i es múltiplo de ϕ_{i+1}. Por tanto, (ϕ_1) es el ideal anulador de M.
2. Hemos probado, también, que los factores invariantes no dependen de la presentación por libres dada (véase por otra parte 0.10.7).

132. Teorema de clasificación de endomorfismos: *Dos endomorfismos de un k-espacio vectorial de dimensión finita E son equivalentes si y solo si poseen los mismos factores invariantes.*

Sea E un espacio vectorial de dimensión finita. Sea $T\colon E \to E$ un endomorfismo lineal. Tenemos que E es un $k[x]$-módulo finito generado. Construyamos una presentación finita del $k[x]$-módulo E. Sea $E[x]$ el conjunto de polinomios de coeficientes vectores de E. La extensión lineal del producto $x^n * (ex^m) := ex^{n+m}$, dota a $E[x]$ de estructura de $k[x]$-módulo. Obviamente, si $\{v_1,\dots,v_n\}$ es una base de E, entonces es una base del $k[x]$-módulo $E[x]$.

La sucesión de $k[x]$-módulos

$$E[x] \overset{(x*-T)}{\longrightarrow} E[x] \overset{\pi}{\to} E \to 0$$

donde $(x*-T)(ex^m) := ex^{m+1} - T(e)x^m$ y $\pi(ex^m) := T^m(e)$, es exacta: $\operatorname{Im}(x*-T) \subseteq \operatorname{Ker}\pi$, obviamente. Probemos la inclusión $\operatorname{Ker}\pi \subseteq \operatorname{Im}(x*-T)$. Dado $\sum_i e_i x^i \in \operatorname{Ker}\pi$, es fácil probar que módulo $\operatorname{Im}(x*-T)$ es equivalente a $\sum_i T^i(e_i)$, que es nulo por hipótesis, luego $\sum_i e_i x^i \in \operatorname{Im}(x*-T)$.

Si $\{v_1,\dots,v_n\}$ es una base de E y (a_{ij}) es la matriz asociada a T, entonces la matriz de $(x*-T)$ en la base $\{v_1,\dots,v_n\}$ es $x\cdot \mathrm{Id} - (a_{ij})$.

133. Teorema: *Sea (a_{ij}) la matriz $n\times n$ de un endomorfismo T. Sea $c_i(x)$ el máximo común divisor de los menores de orden $n-i$ de la matriz $xId-(a_{ij})$. Se verifica*

$$c_i(x) = \phi_{i+1}(x)\cdots\phi_n(x)$$
$$\phi_i(x) = c_{i-1}(x)/c_i(x)$$

siendo $\phi_1(x),\dots,\phi_n(x)$ los factores invariantes de T.

134. Teorema de Hamilton-Cayley: El polinomio $c_0(x) = \det\big(xId-(a_{ij})\big)$ se llama *polinomio característico* de T. Según el teorema anterior, el polinomio característico es igual al producto de los factores invariantes. Luego el polinomio característico es múltiplo del primer factor invariante (que es el polinomio anulador). Como todos los factores invariantes dividen al primer factor invariante, tenemos que el polinomio característico tiene las mismas raíces salvo multiplicidades que el polinomio anulador. Además,

$$\phi_1(x) = c_0(x)/c_1(x)$$

es decir, el polinomio anulador de T es igual al cociente del polinomio característico por el máximo común divisor de los menores de orden $n-1$ de la matriz $xId-(a_{ij})$.

0.7. Categorías. Funtor de homomorfismos

El estudiante de matemáticas una veces trata con los conjuntos y considera como transformaciones naturales entre ellos las aplicaciones de conjuntos, otras trata con los grupos y los morfismos de grupos, otras con anillos y los morfismos de anillos, otras con los espacios topológicos y las aplicaciones continuas, etc. Cada uno de estos "mundos" se les denomina categorías. Hablemos con mayor precisión.

Dar una categoría $\mathscr{C}$ es dar

1. Una familia arbitraria de elementos, que los llamaremos objetos de $\mathscr{C}$.
2. Unos conjuntos $\mathrm{Hom}_{\mathscr{C}}(M,N)$, para cada par de objetos M,N de $\mathscr{C}$, cuyos elementos f llamaremos morfismos de M en N y denotaremos por el símbolo $f: M \to N$.
3. Una aplicación

$$\mathrm{Hom}_{\mathscr{C}}(N,P) \times \mathrm{Hom}_{\mathscr{C}}(M,N) \to \mathrm{Hom}_{\mathscr{C}}(M,P), \ \ (f,g) \mapsto f \circ g$$

para cada terna M,N,P de objetos de $\mathscr{C}$. Satisfaciéndose

   a) $(f \circ g) \circ h = f \circ (g \circ h)$, para todo $f \in \mathrm{Hom}_{\mathscr{C}}(N,P)$, $g \in \mathrm{Hom}_{\mathscr{C}}(M,N)$ y $h \in \mathrm{Hom}_{\mathscr{C}}(L,M)$.

   b) Para cada objeto M de $\mathscr{C}$, existe un morfismo $\mathrm{Id}_M: M \to M$ de modo que $f \circ \mathrm{Id}_M = f$ e $\mathrm{Id}_M \circ g = g$ para todo morfismo $f: M \to N$ y $g: N \to M$.

Un morfismo $f: M \to N$ se dice que es un isomorfismo si existe $g: N \to M$ de modo que $f \circ g = \mathrm{Id}_N$ y $g \circ f = \mathrm{Id}_M$.

1. Ejemplos: 1. La categoría de conjuntos, $\mathscr{C}_{Conj}$, es la categoría cuyos objetos son los conjuntos y los morfismos entre los objetos son las aplicaciones de conjuntos.

2. Sea G un grupo. La categoría de G-conjuntos, C_{G-conj}, es la categoría cuyos objetos son los G-conjuntos y los morfismos entre los objetos son los morfismos de G-conjuntos.

3. La categoría de espacios topológicos, $\mathscr{C}_{Top}$, es la categoría cuyos objetos son los espacios topológicos y los morfismos entre los objetos son las aplicaciones continuas.

4. La categoría de A-módulos, $\mathscr{C}_{Mod}$, es la categoría cuyos objetos son los A-módulos y los morfismos entre los objetos son los morfismos de módulos.

2. Definición: Sean $\mathscr{C}$ y $\mathscr{C}'$ dos categorías. Dar un funtor covariante $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}'$ es asignar a cada objeto M de $\mathscr{C}$ un objeto $F(M)$ de $\mathscr{C}'$, y cada morfismo $f\colon M \to N$ de $\mathscr{C}$ un morfismo $F(f)\colon F(M) \to F(N)$ de $\mathscr{C}'$, de modo que se cumpla que $F(f \circ g) = F(f) \circ F(g)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Análogamente se definen los funtores contravariantes $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}'$, que asignan a cada objeto M de $\mathscr{C}$ un objeto $F(M)$ de $\mathscr{C}'$, y a cada morfismo $f\colon M \to N$ de $\mathscr{C}$ un morfismo $F(f)\colon F(N) \to F(M)$ de $\mathscr{C}'$, de modo que cumpla $F(f \circ g) = F(g) \circ F(f)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Un objeto $N \in \mathscr{C}$ induce para cada morfismo $f\colon M \to M'$, la aplicación

$$\mathrm{Hom}_{\mathscr{C}}(N,M) \xrightarrow{f_*} \mathrm{Hom}_{\mathscr{C}}(N,M'),\ g \mapsto f_*(g) := f \circ g$$

Estamos diciendo que

$$\begin{aligned} \mathrm{Hom}_{\mathscr{C}}(N,-)\colon \mathscr{C} &\rightsquigarrow \mathscr{C}_{Conj} \\ M &\rightsquigarrow \mathrm{Hom}_{\mathscr{C}}(N,M) \\ f &\rightsquigarrow f_* \\ (f \circ g) &\rightsquigarrow (f \circ g)_* = f_* \circ g_* \end{aligned}$$

es un funtor covariante de $\mathscr{C}$ en la categoría de los conjuntos $\mathscr{C}_{Conj}$.

Un objeto $N \in \mathscr{C}$ induce para cada morfismo $f\colon M \to M'$, la aplicación

$$\mathrm{Hom}_{\mathscr{C}}(M',N) \xrightarrow{f^*} \mathrm{Hom}_{\mathscr{C}}(M,N),\ g \mapsto f^*(g) := g \circ f$$

Luego,

$$\begin{aligned} \mathrm{Hom}_{\mathscr{C}}(-,N)\colon \mathscr{C} &\rightsquigarrow \mathscr{C}_{Conj} \\ M &\rightsquigarrow \mathrm{Hom}_{\mathscr{C}}(M,N) \\ f &\rightsquigarrow f^* \\ (f \circ g) &\rightsquigarrow (f \circ g)^* = g^* \circ f^* \end{aligned}$$

es un funtor contravariante.

3. Definición: Sean $F, F'\colon \mathscr{C} \rightsquigarrow \mathscr{C}'$ dos funtores covariantes (resp. contravariantes). Dar un morfismo (o transformación natural) $\theta\colon F \to F'$, es dar para cada objeto M de la categoría $\mathscr{C}$ un morfismo $\theta_M\colon F(M) \to F'(M)$, de modo que para cada morfismo $f\colon M \to N$ (resp. $f\colon N \to M$) el diagrama

$$\begin{array}{ccc} F(M) & \xrightarrow{F(f)} & F(N) \\ \downarrow{\scriptstyle \theta_M} & & \downarrow{\scriptstyle \theta_N} \\ F'(M) & \xrightarrow{F'(f)} & F'(N) \end{array}$$

es conmutativo. Diremos que θ es un isomorfismo si los θ_M son isomorfismos, para todo objeto M de $\mathscr{C}$.

$\mathrm{Hom}(F,F')$ denotará la familia de morfismos de F en F'.

4. Definición: Se dice que dos categorías $\mathscr{C}$ y $\mathscr{C}'$ son equivalentes (resp. antiequivalentes) si existen funtores covariantes (resp. contravariantes) $F\colon \mathscr{C}\rightsquigarrow\mathscr{C}'$ y $G\colon \mathscr{C}'\rightsquigarrow\mathscr{C}$, de modo que $F\circ G$ es isomorfo al funtor identidad de $\mathscr{C}'$ y $G\circ F$ es isomorfo al funtor identidad de $\mathscr{C}$.

5. Definición: Dada una categoría $\mathscr{C}$ se define la categoria dual de $\mathscr{C}$, que denotaremos $\mathscr{C}^\circ$, como la categoría cuyos objetos son los de $\mathscr{C}$, (dado $M\in\mathscr{C}$, cuando lo pensemos en $\mathscr{C}^\circ$ lo denotaremos M°), $\mathrm{Hom}_{\mathscr{C}^\circ}(M^\circ,N^\circ) := \mathrm{Hom}_{\mathscr{C}}(N,M)$ (dado $f\in\mathrm{Hom}_{\mathscr{C}}(N,M)$, cuando lo pensemos en $\mathrm{Hom}_{\mathscr{C}^\circ}(M^\circ,N^\circ)$ lo denotaremos f°) y por último $f^\circ\circ g^\circ := (g\circ f)^\circ$, para todo $f^\circ\in\mathrm{Hom}_{\mathscr{C}^\circ}(M^\circ,N^\circ)$ y $g^\circ\in\mathrm{Hom}_{\mathscr{C}^\circ}(P^\circ,M^\circ)$.

El funtor, $\mathscr{C}\rightsquigarrow\mathscr{C}^\circ$, $M\rightsquigarrow M^\circ$ y $f\rightsquigarrow f^\circ$ es un funtor contravariante, que establece una anti-equivalencia entre $\mathscr{C}$ y $\mathscr{C}^\circ$. Toda definición, teorema, etc., que se da en una categoría $\mathscr{C}$ tiene su correspondiente definición, teorema, etc., "dual" en $\mathscr{C}^\circ$.

6. Proposición: *Dado un objeto $M\in\mathscr{C}$, denotemos $M_\cdot = \mathrm{Hom}_{\mathscr{C}}(M,-)$. Sea un funtor covariante $F\colon \mathscr{C}\rightsquigarrow\mathscr{C}_{conj}$. Se cumple*

1. $\mathrm{Hom}(M_\cdot,F) = F(M)$.
2. $\mathrm{Hom}(M_\cdot,M'_\cdot) = \mathrm{Hom}_{\mathscr{C}}(M',M)$.
3. *$M_\cdot\simeq M'_\cdot$ si y solo si $M\simeq M'$.*

Demostración. 1. Todo morfismo $\mathrm{Hom}_{\mathscr{C}}(M,-)\xrightarrow{\theta}F$ queda determinado por $\theta_M(\mathrm{Id}_M) = g\in F(M)$: No es más que considerar, dado $f\in\mathrm{Hom}_{\mathscr{C}}(M,N)$, el diagrama

$$\begin{array}{ccc}\mathrm{Hom}_{\mathscr{C}}(M,M) & \xrightarrow{\theta_M} & F(M)\\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle F(f)}\\ \mathrm{Hom}_{\mathscr{C}}(M,N) & \xrightarrow{\theta_N} & F(N)\end{array}\qquad\qquad \begin{array}{ccc}\mathrm{Id}_M & \xmapsto{\theta_M} & g\\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle F(f)}\\ f & \xmapsto{\theta_N} & F(f)(g)\end{array}$$

2. Es consecuencia inmediata de 1.
3. es consecuencia inmediata de 2.

□

La proposición dual de la anterior es la siguiente.

7. Proposición: *Dado un objeto $M \in \mathscr{C}$, denotemos $M^{\cdot} = \mathrm{Hom}_{\mathscr{C}}(-,M)$. Sea un funtor contravariante $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{conj}$. Se cumple*

1. $\mathrm{Hom}(M^{\cdot},F) = F(M)$.
2. $\mathrm{Hom}(M^{\cdot},M'^{\cdot}) = \mathrm{Hom}_{\mathscr{C}}(M,M')$.
3. $M^{\cdot} \simeq M'^{\cdot}$ *si y solo si* $M \simeq M'$.

8. Teorema: *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ sea exacta es que para todo A-módulo N la sucesión*

$$0 \to \mathrm{Hom}_A(N,M') \xrightarrow{i_*} \mathrm{Hom}_A(N,M) \xrightarrow{p_*} \mathrm{Hom}_A(N,M'')$$

sea exacta. Se dice que "$\mathrm{Hom}_A(N,-)$ *es un funtor exacto por la izquierda".*

Demostración. Es sencillo comprobar la necesidad de la condición. En cuanto a la suficiencia, basta tomar $N = A$, pues para todo A-módulo M tenemos un isomorfismo natural $\mathrm{Hom}_A(A,M) = M$, $f \mapsto f(1)$. □

También se tiene el teorema "dual" del anterior:

9. Teorema: *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ sea exacta es que para todo A-módulo N la sucesión*

$$0 \to \mathrm{Hom}_A(M'',N) \xrightarrow{p^*} \mathrm{Hom}_A(M,N) \xrightarrow{i^*} \mathrm{Hom}_A(M',N)$$

sea exacta. "Se dice que $\mathrm{Hom}_A(-,N)$ *es un funtor exacto por la izquierda".*

Demostración. Es sencillo comprobar la necesidad de la condición. Veamos la suficiencia. Sea $N = M''/\mathrm{Im}\, p$, y $\pi\colon M'' \to N$ la proyección canónica. Tenemos que $p^*(\pi) = \pi \circ p = 0$, luego $\pi = 0$ y p es epiyectiva. Si tomamos ahora $N = M''$, entonces $0 = (p^* \circ i^*)(\mathrm{Id}) = p \circ i$, luego $\mathrm{Im}\, i \subseteq \mathrm{Ker}\, p$. Por último, si $N = M/\mathrm{Im}\, i$ y $\pi\colon M \to M/\mathrm{Im}\, i$ es la proyección canónica, entonces $i^*(\pi) = \pi \circ i = 0$. Luego existe un morfismo $f\colon M'' \to N$ tal que $f \circ p = p^*(f) = \pi$ y concluimos que $\mathrm{Ker}\, p = p^{-1}(0) \subseteq (f \circ p)^{-1}(0) = \pi^{-1}(0) = \mathrm{Im}\, i$. □

Funtor de puntos de una variedad

Sea $\mathscr{C}_{k-alg}$ la categoría de las k-álgebras de tipo finito, es decir, la categoría cuyos objetos son las k-álgebras de tipo finito y los morfismos son los morfismos de k-álgebras. Denotemos $\mathscr{C}_{Var}$ la categoría dual de $\mathscr{C}_{k-alg}$. A la k-álgebra A, cuando la pensemos como objeto de $\mathscr{C}_{Var}$, la escribiremos $\mathrm{Spec}A$. En conclusión, los objetos de $\mathscr{C}_{Var}$, son $\mathrm{Spec}A$, y los morfismos $\mathrm{Spec}B \to \mathrm{Spec}A$ son los morfismos de k-álgebras $A \to B$.

Dado $X = \mathrm{Spec}A$, denotaremos por $X^{\cdot}$ el funtor sobre $\mathscr{C}_{Var}$ en la categoría de conjuntos, definido para cada $Y = \mathrm{Spec}B \in \mathscr{C}_{Var}$, por

$$X^{\cdot}(Y) := \mathrm{Hom}_{\mathscr{C}_{Var}}(Y,X) = \mathrm{Hom}_{k-alg}(A,B)$$

Se dice que $X^{\cdot}$ es el funtor de puntos de X. $X^{\cdot}$ tiene una interpretación geométrica más clara que la del propio espacio topológico $\mathrm{Spec}A = X$: $X^{\cdot}(\mathrm{Spec}k) = \mathrm{Hom}_{k-alg}(A,k) =$ {puntos k-racionales de $\mathrm{Spec}A$}. Supongamos que

$$X = \mathrm{Spec}A, \quad A = k[x_1,\ldots,x_n]/(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$$

Entonces

$$\begin{aligned} X^{\cdot}(\mathrm{Spec}B) &= \mathrm{Hom}_{\mathscr{C}_{Var}}(\mathrm{Spec}B,X) = \mathrm{Hom}_{k-\text{álg.}}(A,B) \\ &= \left\{ \begin{array}{l} \text{Soluciones con valores en } B \text{ del sistema} \\ \text{de ecuaciones } p_1(x_1,\ldots,x_n) = \cdots = p_r(x_1,\ldots,x_n) = 0 \end{array} \right. \end{aligned}$$

que es la interpretación geométrica que queríamos dar a la variedad $X = \mathrm{Spec}A$. Sea $A' = k[x_1,\ldots,x_m]/(q_1(x_1,\ldots,x_m),\ldots,q_s(x_1,\ldots,x_m))$ y $X' = \mathrm{Spec}A'$. Entonces, tenemos que $\mathrm{Hom}_{\mathscr{C}_{Var}}(X,X') = \mathrm{Hom}(X^{\cdot},X'^{\cdot})$ y los morfismos entre variedades son las aplicaciones (funtoriales) entre conjuntos (de soluciones de sistemas de ecuaciones).

Categoría abeliana

La noción de categoría abeliana recoge las principales propiedades de la categoría de grupos abelianos, módulos, etc.

10. Definición: Una categoría $\mathscr{C}$ se dice que es una categoría aditiva si

1. Para cada par de objetos $A,B \in \mathscr{C}$, $\mathrm{Hom}_{\mathscr{C}}(A,B)$ es un grupo abeliano y para todo $f \in \mathrm{Hom}_{\mathscr{C}}(B,C)$, $i \in \mathrm{Hom}_{\mathscr{C}}(Z,A)$ y $g,h \in \mathrm{Hom}_{\mathscr{C}}(A,B)$ se cumple que $f \circ (g+h) = f \circ g + f \circ h$ y $(g+h) \circ i = g \circ i + h \circ i$.

2. Para cada par de objetos $A,B \in \mathscr{C}$ existe su producto directo $A \times B$, es decir, un objeto con dos morfismos $\pi_1 : A \times B \to A$, $\pi_2 : A \times B \to B$ de modo que

$$\mathrm{Hom}_{\mathscr{C}}(C, A \times B) \to \mathrm{Hom}_{\mathscr{C}}(C,A) \times \mathrm{Hom}_{\mathscr{C}}(C,B),\ f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$$

   es una biyección (funtorial en C).

3. Existe el objeto cero 0, es decir, un objeto que tienen un único morfismo en cada objeto de $\mathscr{C}$, y para cada objeto de $\mathscr{C}$ existe un único morfismo en él.

Un funtor $F : \mathscr{C} \rightsquigarrow \mathscr{C}'$ entre categorías aditivas, se dice que es aditivo si la aplicación $\mathrm{Hom}_{\mathscr{C}}(A,B) \to \mathrm{Hom}_{\mathscr{C}'}(F(A),F(B))$, $f \mapsto F(f)$ es un morfismo de grupos.

Puede probarse que en las categorías aditivas existe la suma directa de dos objetos y es isomorfo al producto directo. Si F es un funtor aditivo $F(A \times B) = F(A) \times F(B)$.

Una categoría abeliana es una categoría aditiva que cumple

1. Todo morfismo tiene núcleo y conúcleo. Es decir, dado $f : A \to B$ existen objetos, $\mathrm{Ker}\, f$ y $\mathrm{Coker}\, f$, y morfismos $\mathrm{Ker}\, f \to A$, $B \to \mathrm{Coker}\, f$, de modo que las sucesiones de morfismos $0 \to \mathrm{Hom}_{\mathscr{C}}(C, \mathrm{Ker}\, f) \to \mathrm{Hom}_{\mathscr{C}}(C,A) \to \mathrm{Hom}_{\mathscr{C}}(C,B)$ y $0 \to \mathrm{Hom}_{\mathscr{C}}(\mathrm{Coker}\, f, C) \to \mathrm{Hom}_{\mathscr{C}}(B,C) \to \mathrm{Hom}_{\mathscr{C}}(A,C)$ son exactas, para todo C.

2. Todo monomorfismo $f : A \to B$ es el núcleo de $B \to \mathrm{Coker}\, f$ ($f : A \to B$ se dice que es un monomorfismo si $\mathrm{Hom}_{\mathscr{C}}(C,A) \to \mathrm{Hom}_C(C,B)$ es una aplicación inyectiva para todo C).

3. Todo epimorfismo $f : A \to B$ es el conúcleo de $\mathrm{Ker}\, f \to A$ ($f : A \to B$ se dice que es un epimorfismo si $\mathrm{Hom}_{\mathscr{C}}(B,C) \to \mathrm{Hom}_C(A,C)$ es una aplicación inyectiva para todo C).

En las categorías abelianas como en la categoría de módulos se habla de sucesiones exactas (véase 0.6.18).

11. Definición: Diremos que un funtor covariante aditivo $F : \mathscr{C} \rightsquigarrow \mathscr{C}'$ entre categorías abelianas es exacto por la izquierda si para toda sucesión exacta $0 \to A \to B \to C$ en $\mathscr{C}$, se cumple que $0 \to F(A) \to F(B) \to F(C)$ es exacta. Se dice que es exacto por la derecha si si para toda sucesión exacta $A \to B \to C \to 0$ en $\mathscr{C}$, se cumple que $F(A) \to F(B) \to F(C) \to 0$ es exacta. Se dice que es exacto si es exacto por la derecha y la izquierda.

Se dice que un funtor contravariante aditivo $\mathscr{C} \overset{G}{\rightsquigarrow} \mathscr{C}'$ entre categorías abelianas es exacto por la izquierda si el funtor (covariante) composición $\mathscr{C}^\circ \rightsquigarrow \mathscr{C} \overset{G}{\rightsquigarrow} \mathscr{C}'$ es exacto por la izquierda. Se dice que es exacto por la derecha si el funtor composición $\mathscr{C}^\circ \rightsquigarrow \mathscr{C} \overset{G}{\rightsquigarrow} \mathscr{C}'$ es exacto por la derecha. Se dice que es exacto si es exacto por la derecha y la izquierda.

0.8. Producto tensorial de módulos y álgebras

Los dos procesos o técnicas fundamentales estudiados hasta aquí han sido el cociente y la localización de módulos. Como veremos éstos son casos particulares de la técnica de cambio de base, obtenida del producto tensorial. Geométricamente el producto tensorial de las álgebras de funciones de dos variedades algebraicas se corresponde con el álgebra de funciones del producto directo de las variedades.

Sean M y N dos A-módulos. Consideremos el A-módulo libre $A^{(M\times N)} = \overset{M\times N}{\oplus} A$. Sea $\{m\square n\}_{(m,n)\in M\times N}$ la base estándar de $A^{(M\times N)}$, es decir, $m\square n = (a_{(m',n')})_{(m',n')\in M\times N}$ es el elemento de $A^{(M\times N)}$ definido por $a_{(m',n')} = 0$ si $(m',n') \neq (m,n)$ y $a_{(m,n)} = 1$.

Sea R el submódulo de $A^{(M\times N)}$ generado por los elementos de la forma

$$\begin{array}{l}(m+m')\square n - m\square n - m'\square n\\ m\square(n+n') - m\square n - m\square n'\\ (am)\square n - a(m\square n)\\ m\square(an) - a(m\square n)\end{array} \qquad (*)$$

para todo $m,m' \in M$, $n \in N$ y $a \in A$.

1. Definición: Llamaremos producto tensorial de M y N sobre el anillo A, al A-módulo cociente $A^{(M\times N)}/R$ y lo denotaremos $M \otimes_A N$. Cada clase $\overline{m\square n} \in A^{(M\times N)}/R = M \otimes_A N$ la denotaremos $m \otimes n$.

De acuerdo con la definición de R tenemos que

$$\begin{array}{l}(m+m')\otimes n = m\otimes n + m'\otimes n\\ m\otimes(n+n') = m\otimes n + m\otimes n'\\ am\otimes n = a(m\otimes n)\\ m\otimes an = a(m\otimes n)\end{array}$$

propiedades que se expresan diciendo "el producto tensorial es A-bilineal". En realidad, el formalismo seguido, ha sido para llegar a definir "el producto" ($\otimes$) de elementos de M por N, con estas propiedades y sin más relaciones que las generadas por las relaciones de M y N y estas propiedades.

Dado que los elementos $\{m\square n\}_{(m,n)\in M\times N}$ forman una base de $A^{(M\times N)}$ entonces los elementos $\{m\otimes n\}_{(m,n)\in M\times N}$ forman un sistema generador de $M \otimes_A N$. Por las propiedades de bilinealidad recién escritas, si $\{m_i\}$ y $\{n_j\}$ son sistemas generadores de M y N, entonces $\{m_i \otimes n_j\}$ es un sistema generador de $M \otimes_A N$.

2. Definición: Sea P un A-módulo. Diremos que una aplicación $\beta\colon M\times N \to P$ es

A-bilineal si

$$\begin{aligned}\beta(m+m',n) &= \beta(m,n)+\beta(m',n)\\ \beta(m,n+n') &= \beta(m,n)+\beta(m,n')\\ \beta(am,n) &= a\beta(m,n)\\ \beta(m,an) &= a\beta(m,n)\end{aligned}$$

El conjunto de las aplicaciones A-bilineales de $M\times N$ en P se denota $\mathrm{Bil}_A(M,N;P)$.

Con mayor generalidad, el lector puede dar la definición de aplicación A-multilineal de $M_1\times\overset{n}{\cdots}\times M_n$ en P. El conjunto de las aplicaciones A-multilineales de $M_1\times\cdots\times M_n$ en P se denota $\mathrm{Multl}_A(M_1,\overset{n}{\ldots},M_n;P)$.

La condición de que una aplicación $\beta\colon M\times N\to P$ sea A-bilineal implica que la aplicación $\beta_m\colon N\to P$, $\beta_m(n)=\beta(m,n)$, es un morfismo de A-módulos para cada elemento $m\in M$. Tenemos así, un morfismo natural $\mathrm{Bil}_A(M,N;P)\to\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, $\beta\mapsto\tilde{\beta}$, donde $\tilde{\beta}(m):=\beta_m$.

3. Proposición: *Se cumple que* $\mathrm{Bil}_A(M,N;P)=\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, $\beta\mapsto\tilde{\beta}$.

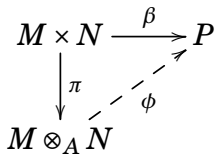
Demostración. Definamos la asignación inversa,

$$\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))\to\mathrm{Bil}_A(M,N;P), f\mapsto\beta_f,$$

donde $\beta_f(m,n):=f(m)(n)$. □

El morfismo natural $\pi\colon M\times N\to M\otimes N$, $(m,n)\mapsto m\otimes n$, es bilineal.

4. Propiedad universal del producto tensorial: *Una aplicación $\beta\colon M\times N\to P$ es A-bilineal si y solo si existe un único morfismo de A-módulos $\phi\colon M\otimes_A N\to P$, de modo que el siguiente diagrama*



es conmutativo. Con concisión,

$$\mathrm{Hom}_A(M\otimes_A N,P)=\mathrm{Bil}_A(M,N;P),\quad \phi\mapsto\phi\circ\pi$$

Por tanto, por la proposición 0.8.3,

$$\mathrm{Hom}_A(M\otimes_A N,P)=\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P)),\ f\mapsto\tilde{f},\ \textit{donde}\ \tilde{f}(m)(n):=f(m\otimes n)$$

Demostración. Sea $\beta\colon M\times N\to P$ una aplicación A-bilineal, entonces el morfismo de A-módulos

$$\varphi\colon A^{(M\times N)}\to P,\ \varphi(\sum_i a_i(m_i\square n_i))=\sum_i a_i\beta(m_i,n_i)$$

se anula sobre los generadores del submódulo R, anteriormente definido en $(*)$. Por lo tanto, induce el morfismo de A-módulos $\phi\colon M\otimes_A N\to P$, $m\otimes n\mapsto\beta(m,n)$. Este morfismo cumple que $\beta=\phi\circ\pi$ y si un morfismo ϕ' cumple esta igualdad entonces $\phi'(m\otimes n)=\beta(m,n)$ y coincide con ϕ, pues los elementos $m\otimes n$ generan $M\otimes N$.

Por último, es una simple comprobación ver que dado un morfismo de A-módulos $\phi\colon M\otimes N\to P$ entonces $\beta=\phi\circ\pi$ es una aplicación bilineal de $M\times N$ en P.

□

Este teorema nos dice que definir un morfismo de A-módulos $\phi\colon M\otimes N\to P$, es asignar a cada elemento $m\otimes n\in M\otimes_A N$ un elemento $\phi(m\otimes n)$ de P de modo que $\phi((am+m')\otimes n)=a\phi(m\otimes n)+\phi(m'\otimes n)$ y $\phi(m\otimes(an+n'))=a\phi(m\otimes n)+\phi(m\otimes n')$.

5. Observación: Análoga construcción puede hacerse para cualquier familia finita $M_1,\dots,M_n$ de A-módulos, obteniéndose un A-módulo $M_1\otimes_A\cdots\otimes_A M_n$ con la propiedad universal

$$\mathrm{Hom}_A(M_1\otimes_A\cdots\otimes_A M_n,P)=\mathrm{Multl}_A(M_1,\overset{n}{\dots},M_n;P).$$

Para definir un morfismo de A-módulos $f\colon M_1\otimes_A\cdots\otimes_A M_n\to P$, bastará definir las imágenes $f(m_1\otimes\cdots\otimes m_n)$ de modo que

$$f(m_1\otimes\cdots\otimes a_im_i+n_i\otimes\cdots\otimes m_n)=a_if(m_1\otimes\cdots\otimes m_i\otimes\cdots\otimes m_n)+f(m_1\otimes\cdots\otimes n_i\otimes\cdots\otimes m_n).$$

6. Teorema: *Existen isomorfismos naturales*

1. $(M\otimes_A N)\otimes_A P=M\otimes_A(N\otimes_A P)$, $(m\otimes n)\otimes p\mapsto m\otimes(n\otimes p)$.
2. $M\otimes_A N=N\otimes_A M$, $m\otimes n\mapsto n\otimes m$.
3. $A\otimes_A M=M$, $a\otimes m\mapsto am$.
4. $(\underset{i}{\oplus}M_i)\otimes_A N=\underset{i}{\oplus}(M_i\otimes N)$, $(m_i)\otimes n\mapsto(m_i\otimes n)$.

Demostración. Dejamos al lector que defina los morfismos inversos. Veamos, solo, que el morfismo de 1. está bien definido: Para cada elemento $p\in P$ el morfismo de A-módulos $M\otimes_A N\times p\to M\otimes_A(N\otimes_A P)$, $(m\otimes n)\times p\mapsto m\otimes(n\otimes p)$ está bien definido. Luego tenemos una aplicación $(M\otimes_A N)\times P\to M\otimes_A(N\otimes_A P)$, que es bilineal e induce el morfismo definido en 1. □

Sería formativo para el lector que intentase demostrar el teorema anterior usando la propiedad universal del producto tensorial. Por ejemplo,

$$\begin{aligned}\mathrm{Hom}_A((M\otimes_A N)\otimes_A P,R) &= \mathrm{Hom}_A((M\otimes_A N),\mathrm{Hom}_A(P,R))\\ &= \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,\mathrm{Hom}_A(P,R)))\\ &= \mathrm{Hom}_A(M,\mathrm{Hom}_A(N\otimes_A P,R)) = \mathrm{Hom}_A(M\otimes_A (N\otimes_A P),R)\end{aligned}$$

y por 0.7.6, $(M\otimes_A N)\otimes_A P = M\otimes_A (N\otimes_A P)$.

Si $f: A\to B$ es un morfismo de anillos, se dice que B es una A-álgebra. Si N es un B-módulo, entonces N es de modo natural un A-módulo. Sea M un A-módulo y N un B-módulo. Cada elemento $b\in B$ define un endomorfismo $1\otimes b: M\otimes_A N\to M\otimes_A N$, $m\otimes n \underset{\text{def}}{\mapsto} m\otimes bn$. Podemos definir así, una estructura de B-módulo en $M\otimes_A N$ que viene dada por el siguiente producto

$$b\cdot(\sum_i m_i\otimes n_i) := \sum_i m_i\otimes bn_i$$

7. Teorema : *Sea $A\to B$ un morfismo de anillos, M un A-módulo y N,P dos B-módulos. Existen isomorfismos naturales*

1. $\mathrm{Hom}_B(M\otimes_A N,P) = \mathrm{Hom}_A(M,\mathrm{Hom}_B(N,P))$.
2. $(M\otimes_A N)\otimes_B P = M\otimes_A (N\otimes_B P)$, $(m\otimes n)\otimes p\mapsto m\otimes(n\otimes p)$.
3. $M\otimes_A A_S = M_S$, $m\otimes\frac{a}{s}\mapsto\frac{am}{s}$.
4. $M\otimes_A A/I = M/IM$, $m\otimes\bar{a}\mapsto\overline{am}$.

Demostración. 1. Vía la igualdad $\mathrm{Hom}_A(M\otimes_A N,P) = \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, el submódulo $\mathrm{Hom}_B(M\otimes_A N,P)$ se corresponde con el submódulo $\mathrm{Hom}_A(M,\mathrm{Hom}_B(N,P))$. El resto al lector. □

8. Proposición : *Sea $M'\to M\to M''\to 0$ una sucesión exacta y N un A-módulo. Se cumple que*

$$M'\otimes_A N\to M\otimes_A N\to M''\otimes_A N\to 0$$

es una sucesión exacta. Es decir, "$-\otimes_A N$ es un funtor exacto por la derecha".

Demostración. Sea $M^\bullet$ la sucesión exacta inicial. De acuerdo con 0.7.9

$$\mathrm{Hom}_A(M^\bullet,\mathrm{Hom}_A(N,P)) = \mathrm{Bil}_A(M^\bullet,N;P) = \mathrm{Hom}_A(M^\bullet\otimes_A N,P)$$

es una sucesión exacta para todo A-módulo P. De nuevo 0.7.9 nos permite concluir que la sucesión $M^\bullet\otimes_A N$ es exacta. □

Sea $f: A \to B$ un morfismo de anillos. Se dice que $M \otimes_A B$ es el cambio de base de M por $A \to B$.

9. Notación: Denotaremos $M \otimes_A B = M_B$ y usualmente denotaremos $f(a) = a$.

10. Proposición: *Sean $A \to B$ y $B \to C$ morfismos de anillos, M y M' A-módulos. Existen isomorfismos naturales*

1. $(M \otimes_A M') \otimes_A B = M_B \otimes_B M'_B$, $(m \otimes m') \otimes b \mapsto (m \otimes b) \otimes (m' \otimes 1)$. *En particular, dado un sistema multiplicativo $S \subset A$, $(M \otimes_A N)_S = M_S \otimes_{A_S} N_S$.*

2. $(M_B)_C = M_C$, *(i.e.,* $(M \otimes_A B) \otimes_B C = M \otimes_A C$, $(m \otimes b) \otimes c \mapsto m \otimes bc$*).*

Demostración. Defínanse los morfismos inversos. □

Ahora, nuestro objetivo es definir el producto tensorial de A-álgebras.

Si B y C son A-álgebras, el A-módulo $B \otimes_A C$ tiene una estructura natural de A-álgebra: La aplicación $B \times C \times B \times C \to B \otimes_A C$, $(b, c, b', c') \mapsto bb' \otimes cc'$ induce el correspondiente morfismo $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$. Con este producto $B \otimes_A C$ es un anillo. Por último, el morfismo $A \to B \otimes_A C$, $a \mapsto a \otimes 1 = 1 \otimes a$ es un morfismo de anillos.

11. Proposición: *Sean B, C y D A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc} \mathrm{Hom}_{A-alg}(B \otimes_A C, D) & = & \mathrm{Hom}_{A-alg}(B, D) \times \mathrm{Hom}_{A-alg}(C, D) \\ \phi & \longmapsto & (\phi_1, \phi_2) \;\; \phi_1(b) = \phi(b \otimes 1), \phi_2(c) = \phi(1 \otimes c) \\ \phi : (b \otimes c) \mapsto \phi_1(b)\phi_2(c) & \longmapsto & (\phi_1, \phi_2) \end{array}$$

12. Proposición: *Sean A y B dos k-álgebras. Entonces,*

$$\mathrm{Spec}_{rac}(A \otimes_k B) = \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B$$

Demostración. En efecto,

$$\begin{aligned} \mathrm{Spec}_{rac}(A \otimes_k B) &= \mathrm{Hom}_{k-alg}(A \otimes_k B, k) = \mathrm{Hom}_{k-alg}(A, k) \times \mathrm{Hom}_{k-alg}(B, k) \\ &= \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B \end{aligned}$$

□

Este hecho justificará la definición $\operatorname{Spec} A \times \operatorname{Spec} A' := \operatorname{Spec}(A \otimes_{\mathbb{C}} A')$ (advertencia: $\operatorname{Spec} A \times \operatorname{Spec} A'$ no denota el producto cartesiano de los conjuntos $\operatorname{Spec} A$ y $\operatorname{Spec} A'$) y el producto tensorial de anillos "de funciones de variedades" se interpretará como el anillo del producto de las variedades.

El morfismo inducido en los espectros racionales por $i\colon A \to A \otimes_k B$, $i(a) = a \otimes 1$ es

$$\operatorname{Spec}_{rac} A \times \operatorname{Spec}_{rac} B = \operatorname{Spec}_{rac}(A \otimes_k B) \xrightarrow{i^*} \operatorname{Spec}_{rac} A$$

$$(\alpha, \beta) \longmapsto \alpha$$

En efecto, vía las aplicaciones

$$\operatorname{Hom}_{k-alg}(A,k) \times \operatorname{Hom}_{k-alg}(B,k) = \operatorname{Hom}_{k-alg}(A \otimes_k B, k) \xrightarrow{i^*} \operatorname{Hom}_{k-alg}(A,k),$$

(ϕ_1, ϕ_2) se aplica en $(\phi_1 \otimes \phi_2)_{|A\otimes 1} = \phi_1$.

El morfismo inducido en los espectros racionales por $f\colon A \otimes_k A \to A$, $f(a \otimes a') = aa'$ es

$$\begin{array}{rcl} \operatorname{Spec}_{rac} A & \to & \operatorname{Spec}_{rac} A \times \operatorname{Spec}_{rac} A = \operatorname{Spec}_{rac}(A \otimes_k A) \\ \alpha & \mapsto & (\alpha, \alpha) \end{array}$$

En efecto, vía las aplicaciones

$$\operatorname{Hom}_{k-alg}(A,k) \xrightarrow{f^*} \operatorname{Hom}_{k-alg}(A \otimes_k A, k) = \operatorname{Hom}_{k-alg}(A,k) \times \operatorname{Hom}_{k-alg}(A,k),$$

ϕ se aplica en $((\phi \circ f)_{|A\otimes 1}, (\phi \circ f)_{|1\otimes A}) = (\phi, \phi)$.

13. Proposición: *Sean B y C A-álgebras. Se cumple el isomorfismo*

$$\operatorname{Hom}_{A-alg}(B,C) = \operatorname{Hom}_{C-alg}(B_C, C)$$

$$\phi \longmapsto \phi' : \phi'(b \otimes c) = \phi(b) \cdot c$$

$$\phi'_{|B} \longmapsfrom \phi'$$

0.8.1. Álgebra tensorial, simétrica y exterior de un módulo

Dado un A-módulo M, diremos que

$$T^n M := M \otimes_A \overset{n}{\ldots} \otimes_A M$$

es el producto tensorial n-ésimo de M. Seguiremos las convenciones $T^0 M = A$ y $T^1 M = M$.

Si M es un A-módulo libre de base $\{e_i\}_{i\in I}$, entonces T^nM es un A-módulo libre de base $\{e_{i_1}\otimes\cdots\otimes e_{i_n}\}_{i_1,\ldots,i_n\in I}$ (por 0.8.6.4).

Podemos pensar los elementos de T^nM como ciertas aplicaciones multilineales. Con precisión, sea $M^*=\mathrm{Hom}_A(M,A)$, tenemos el morfismo natural

$$\phi\colon T^nM\to \mathrm{Multl}_A(M^*,\overset{n}{\ldots},M^*;A),\ \ \phi(m_1\otimes\overset{n}{\cdots}\otimes m_n)(w_1,\ldots,w_n):=w_1(m_1)\cdots w_n(m_n)$$

Si M es un A-módulo libre finito generado entonces $T^nM=\mathrm{Multl}_A(M^*,\overset{n}{\ldots},M^*;A)$.

14. Nota: En esta subsección las álgebras consideradas no serán necesariamente conmutativas.

15. Definición: Sea R una álgebra que es suma directa de subgrupos R_n (para la operación $+$), con $n\in\mathbb{Z}$. Diremos que $R=\underset{n\in\mathbb{Z}}{\oplus}R_n$ es un álgebra graduada, si dados $r_n\in R_n$, $r_m\in R_m$ entonces $r_n\cdot r_m\in R_{n+m}$. Además, diremos que R es una A-álgebra graduada si R_0 es una A-álgebra.[5]

16. Definición: Se dice que un álgebra graduada $R=\underset{n\in\mathbb{Z}}{\oplus}R_n$ es conmutativa si es un anillo conmutativo.

Los anillos de polinomios, $k[x_1,\ldots,x_n]$, son de modo obvio k-álgebras graduadas conmutativas.

17. Definición: Diremos que $T^{\cdot}M=\overset{\infty}{\underset{i=0}{\oplus}}T^iM$ es el álgebra tensorial de M. Denotaremos $T^{\cdot}M=T^{\cdot}_AM$ cuando queramos precisar quién es el anillo.

Dados $m_1\otimes\cdots\otimes m_n\in T^nM$ y $m'_1\otimes\cdots\otimes m'_r\in T^rM$ definimos

$$(m_1\otimes\cdots\otimes m_n)\cdot(m'_1\otimes\cdots\otimes m'_r)=m_1\otimes\cdots\otimes m_n\otimes m'_1\otimes\cdots\otimes m'_r\in T^{r+n}M$$

que extendido linealmente a $T^{\cdot}M$, define un producto, con el que es una A-álgebra graduada (no conmutativa).

18. Definición: Los morfismos de álgebras graduadas son morfismos de álgebras entre álgebras graduadas que conservan la graduación, es decir, aplican elementos de grado n en elementos de grado n. Si R y R' son A-álgebras graduadas denotaremos por $\mathrm{Hom}_{A-grd}(R,R')$ los morfismos de A-álgebras graduados.

19. Propiedad universal del álgebra tensorial: *Sea M un A-módulo y $R=\underset{n\in\mathbb{Z}}{\oplus}R_n$ un A-álgebra graduada Existe un isomorfismo natural*

$$\mathrm{Hom}_{A-grd}(T^{\cdot}M,R)=\mathrm{Hom}_A(M,R_1).$$

[5] Supondremos también que los elementos de A conmutan con todos los elementos de R.

Demostración. Cada morfismo de A-álgebras graduadas $\phi\colon T^{\cdot}M \to R$, induce por restricción un morfismo $\phi_{|M}\colon M \to R_1$ de A-módulos. Recíprocamente, dado un morfismo de A-módulos $\varphi\colon M \to R_1$, el morfismo $\phi\colon T^{\cdot}M \to R$, definido por

$$\phi(m_1 \otimes \cdots \otimes m_n) = \varphi(m_1)\cdots\varphi(m_n)$$

está bien definido. Ahora es fácil comprobar que las asignaciones definidas son inversas entre sí.

□

En particular, $\mathrm{Hom}_A(M,M') = \mathrm{Hom}_{A-grd}(T^{\cdot}M, T^{\cdot}M')$.

20. Proposición: *Se cumple:*

1. $(T^{\cdot}_A M) \otimes_A B = T^{\cdot}_B(M \otimes_A B)$.
2. $T^{\cdot}(M/N) = (T^{\cdot}M)/\langle N\rangle$, *donde* N *es un submódulo de* M *y denotamos por* $\langle N\rangle$ *al ideal bilátero de* $T^{\cdot}M$ *generado por* $N \subset T^{\cdot}M$, *es decir, un sistema generador de* $\langle N\rangle$ *como* A*-módulo es* $\{m_1 \otimes \ldots \otimes \overset{i}{n} \otimes \ldots \otimes m_r \mid n \in N, m_k \in M, i, r \in \mathbb{N}\}$.

Demostración. 1. Se deduce de las igualdades

$$\begin{aligned}\mathrm{Hom}_{B-grd}(T^{\cdot}_B(M \otimes_A B), R) &= \mathrm{Hom}_B(M \otimes_A B, R_1) = \mathrm{Hom}_A(M, R_1)\\ &= \mathrm{Hom}_{A-grd}(T^{\cdot}_A M, R) = \mathrm{Hom}_{B-grd}(T^{\cdot}_A M \otimes_A B, R).\end{aligned}$$

2. Sea $i\colon N \hookrightarrow M$ la inclusión e $i^*\colon \mathrm{Hom}_A(M,R_1) \to \mathrm{Hom}_A(N,R_1)$ el morfismo inducido. Por las igualdades

$$\begin{aligned}\mathrm{Hom}_{A-grd}(T^{\cdot}(M/N), R) &= \mathrm{Hom}_A(M/N, R_1) = \mathrm{Ker}\left[i^*\colon \mathrm{Hom}_A(M,R_1) \to \mathrm{Hom}_A(N,R_1)\right]\\ &= \mathrm{Ker}\left[i^*\colon \mathrm{Hom}_{A-grd}(T^{\cdot}M, R) \to \mathrm{Hom}_A(N,R_1)\right]\\ &= \mathrm{Hom}_{A-grd}((T^{\cdot}M)/\langle N\rangle, R)\end{aligned}$$

se concluye. □

Ahora, nuestro objetivo es definir el álgebra simétrica de un módulo. Consideremos en $T^n M$ el submódulo

$$M'_n = \langle m_1 \otimes \cdots \otimes \overset{i}{m_i} \otimes \cdots \otimes \overset{j}{m_j} \otimes \cdots \otimes m_n - m_1 \otimes \cdots \otimes \overset{i}{m_j} \otimes \cdots \otimes \overset{j}{m_i} \otimes \cdots \otimes m_n \mid m_1, \ldots, m_n \in M, \forall i, j\rangle$$

21. Definición: Diremos que $S^n M = T^n M/M'_n$ es el producto tensorial simétrico n-ésimo del A-módulo M. Diremos que $S^{\cdot}M = \overset{\infty}{\underset{i=0}{\oplus}} S^i M$ es el álgebra simétrica de M. Denotaremos $S^{\cdot}M = S^{\cdot}_A M$ cuando queramos precisar quién es el anillo.

Se dice que una aplicación multilineal $\beta\colon M\times \overset{n}{\dots} \times M \to M'$ es una aplicación multilineal simétrica de orden n de M en M' si

$$\beta(m_1,\dots,m_n)=\beta(m_{\sigma(1)},\dots,m_{\sigma(n)})$$

para todo $\sigma\in S_n$. Denotemos $\mathrm{Sim}_A(M,\overset{n}{\dots},M;M')$ el conjunto de las aplicaciones A-multilineales simétricas de orden n de M en M'.

22. Propiedad universal del producto tensorial simétrico de un A-módulo: *De la definición es inmediato que* $\mathrm{Hom}_A(S^nM,M')=\mathrm{Sim}_A(M,\overset{n}{\dots},M;M')$.

Es claro que $M'_n\cdot T^rM, T^rM\otimes M'_n\subseteq M'_{n+s}$. Por tanto el producto que tenemos definido en $T^{\cdot}M$, define por paso al cociente un producto en $S^{\cdot}M$. Luego $S^{\cdot}M$ es un álgebra graduada.

Se suele denotar $m_1\cdot\ldots\cdot m_n$ a la clase de $m_1\otimes\overset{n}{\dots}\otimes m_n$ en S^nM y $\cdot$ al producto que tenemos definido en $S^{\cdot}M$. Observemos que

$$m_1\cdot\ldots\cdot\overset{i}{m_i}\cdot\ldots\cdot\overset{j}{m_j}\cdot\ldots\cdot m_n=m_1\cdot\ldots\cdot\overset{i}{m_j}\cdot\ldots\cdot\overset{j}{m_i}\cdot\ldots\cdot m_n$$

De aquí es fácil concluir que dados $s_n\in S^nM$ y $s_r\in S^rM$, entonces $s_n\cdot s_r=s_r\cdot s_n$.

Por tanto, $S^{\cdot}M$ es una A-álgebra graduada conmutativa.

23. Propiedad universal del álgebra simétrica: *Sea M un A-módulo y $R=\bigoplus_{n\in\mathbb{Z}}R_n$ una A-álgebra graduada conmutativa. Existe un isomorfismo natural*

$$\mathrm{Hom}_{A-grd}(S^{\cdot}M,R)=\mathrm{Hom}_A(M,R_1).$$

Demostración. Es inmediato a partir de la definición del álgebra simétrica y la propiedad universal del álgebra tensorial de un módulo. □

24. Proposición: *Se cumple que $S^{\cdot}A^n\simeq A[x_1,\dots,x_n]$. Si E es un A-módulo libre de base $\{e_1,\dots,e_n\}$, entonces S^rE es un A-módulo libre de base $\{e_{i_1}\cdots e_{i_r}\}_{i_1\le\dots\le i_r}$.*

Demostración. Como

$$\mathrm{Hom}_{A-grd}(S^{\cdot}A^n,R)=\mathrm{Hom}_A(A^n,R_1)=(R_1)^n=\mathrm{Hom}_{A-grd}(A[x_1,\dots,x_n],M)$$

para toda A-álgebra graduada conmutativa, entonces $S^{\cdot}A^n\simeq A[x_1,\dots,x_n]$. Por tanto, S^rA^n es isomorfo al A-módulo formado por los polinomios homogéneos de grado r de $A[x_1,\dots,x_n]$, que es un A-módulo libre de base $\{x_{i_1}\cdots x_{i_r}\}_{i_1\le\dots\le i_r}$. Obviamente, $\{e_{i_1}\cdots e_{i_r}\}_{i_1\le\dots\le i_r}$ es un sistema generador de S^rE y es una base porque el rango de S^rE es igual al de $S^r(A^n)$. □

Si $R = \bigoplus_{n\in\mathbb{Z}} R_n$ y $R' = \bigoplus_{n\in\mathbb{Z}} R'_n$ son A-álgebras graduadas, entonces la A-álgebra $R\otimes_A R'$ es graduada con la graduación

$$(R\otimes_A R')_n = \bigoplus_{i+j=n} R_i \otimes_A R'_j$$

El producto tensorial $R\otimes_A R'$ de álgebras graduadas conmutativas es una álgebra graduada conmutativa.

25. Proposición: *Se cumple*

1. $S^\cdot(M\oplus N) = S^\cdot M\otimes_A S^\cdot N$. *Luego tenemos isomorfismos naturales* $S^n(M\oplus M') = \bigoplus_{i+j=n} S^i M\otimes_A S^j M'$.
2. $(S^\cdot_A M)\otimes_A B = S^\cdot_B(M\otimes_A B)$.
3. $S^\cdot(M/N) = (S^\cdot M)/\langle N\rangle$, *donde* N *es un submódulo de* M *y denotamos por* $\langle N\rangle$ *al ideal de* $S^\cdot M$ *generado por* $N\subset S^\cdot M$.

Demostración. 1. Se cumplen las igualdades

$$\begin{aligned}\mathrm{Hom}_{A-grd}(S^\cdot(M\oplus N),R) &= \mathrm{Hom}_A(M\oplus N,R_1) = \mathrm{Hom}_A(M,R_1)\times\mathrm{Hom}_A(N,R_1)\\ &= \mathrm{Hom}_{A-grd}(S^\cdot M,R)\times\mathrm{Hom}_{A-grd}(S^\cdot N,R) = \mathrm{Hom}_{A-grd}(S^\cdot M\otimes_A S^\cdot N,R),\end{aligned}$$

para toda álgebra graduada conmutativa R. Por tanto, $S^\cdot(M\oplus N) = S^\cdot M\otimes_A S^\cdot N$.

2. y 3. se demuestran igual que la proposición 0.8.20. □

La composición del morfismo $S^n M\to T^n M$, $m_1\cdots m_n\mapsto\sum_{\sigma\in S_n} m_{\sigma(1)}\otimes\cdots\otimes m_{\sigma(n)}$ con el epimorfismo natural $T^n M\to S^n M$ es una homotecia de factor $n!$. Podemos pensar los elementos de $S^n M$ como ciertas aplicaciones multilineales simétricas. Con precisión, sea $M^* = \mathrm{Hom}_A(M,A)$, tenemos el morfismo natural

$$\phi\colon S^n M\to \mathrm{Sim}_A(M^*,\overset{n}{\ldots},M^*,A),\ \phi(m_1\cdots m_n)(w_1,\ldots,w_n) := \sum_{\sigma\in S_n} w_{\sigma(1)}(m_1)\cdots w_{\sigma(n)}(m_n).$$

Si $n!$ es invertible en A y M es un A-módulo libre finito generado entonces $S^n M = \mathrm{Sim}_A(M^*,\overset{n}{\ldots};M^*;A)$.

Ahora, nuestro objetivo es definir el álgebra exterior de un módulo.

Consideremos en $T^n M$ el submódulo

$$M''_n = \langle m_1\otimes\overset{n}{\ldots}\otimes m_n\in T^n M \mid m_i = m_j \text{ para dos índices } i\neq j\rangle.$$

26. Definición: Diremos que $\Lambda^n M = T^n M/M''_n$ es la potencia exterior n-ésima del A-módulo M. Diremos que $\Lambda^{\cdot} M = \overset{\infty}{\underset{i=0}{\oplus}} \Lambda^i M$ es el álgebra exterior de M. Denotaremos $\Lambda^{\cdot} M = \Lambda^{\cdot}_A M$ cuando queramos precisar quién es el anillo.

Se dice que una aplicación multilineal $w_n : M \times \overset{n}{\ldots} \times M \to M'$ es una aplicación multilineal hemisimétrica de orden n de M en M' si

$$w_n(m_1, \ldots, m, \ldots, m, \ldots, m_n) = 0$$

Denotemos $\mathrm{Hem}_A(M, \overset{n}{\ldots}, M; M')$ el conjunto de las aplicaciones A-multilineales hemisimétricas de orden n de M en M'.

27. Propiedad universal de la potencia exterior n-ésima de un A-módulo: *De la definición es inmediato que* $\mathrm{Hom}_A(\Lambda^n M, M') = \mathrm{Hem}_A(M, \overset{n}{\ldots}, M; M')$.

28. Definición: Se dice que un álgebra graduada $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ es anticonmutativa si $r_i \cdot r_j = (-1)^{i\cdot j} r_j \cdot r_i$, para todo $r_i \in R_i$, $r_j \in R_j$.

Es claro que $M''_n \cdot T^r M, T^r M \cdot M''_n \subseteq M''_{n+s}$. Por tanto el producto que tenemos definido en $T^{\cdot} M$, define por paso al cociente un producto de $\Lambda^{\cdot} M$. Luego $\Lambda^{\cdot} M$ es un álgebra graduada.

Se suele denotar $m_1 \wedge \cdots \wedge m_n$ a la clase de $m_1 \otimes \overset{n}{\ldots} \otimes m_n$ en $\Lambda^n M$ y $\wedge$ al producto que tenemos definido en $\Lambda^{\cdot} M$. Observemos que

$$0 = \cdots \wedge m + m' \wedge \cdots \wedge m + m' \wedge \cdots = (\cdots \wedge m \wedge \cdots \wedge m' \wedge \ldots) + (\cdots \wedge m' \wedge \cdots \wedge m \wedge \ldots)$$

Luego $m_1 \wedge \cdots \wedge m \wedge \cdots \wedge m' \wedge \cdots \wedge m_n = -(m_1 \wedge \cdots \wedge m' \wedge \cdots \wedge m \wedge \cdots \wedge m_n)$. De aquí es fácil concluir que dados $w_n \in \Lambda^n M$ y $w_r \in \Lambda^r M$, entonces $w_n \wedge w_r = (-1)^{nr} w_r \wedge w_n$.

Por tanto, $\Lambda^{\cdot} M$ es una A-álgebra graduada anticonmutativa.

29. Propiedad universal del álgebra exterior: *Sea M un A-módulo y $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ un álgebra graduada anticonmutativa. Existe un isomorfismo natural*

$$\mathrm{Hom}_{A-grd}(\Lambda^{\cdot} M, R) = \mathrm{Hom}_A(M, R_1).$$

Demostración. Es inmediato a partir de la definición del álgebra exterior y la propiedad universal del álgebra tensorial de un módulo. □

El producto tensorial $R \otimes_A R'$ de álgebras graduadas anticonmutativas es una álgebra graduada anticonmutativa siguiendo la siguiente convención, con las notaciones obvias

$$(r_i \otimes r'_j) \cdot (s_n \otimes s'_m) = (-1)^{jn} r_i s_n \otimes r'_j s'_m$$

30. Proposición: *Se cumple*

1. $\Lambda^{\cdot}(M\oplus N)=\Lambda^{\cdot}M\otimes_A\Lambda^{\cdot}N$. *Luego tenemos isomorfismos naturales* $\Lambda^n(M\oplus M')=\bigoplus_{i+j=n}\Lambda^iM\otimes_A\Lambda^jM'$.

2. $(\Lambda^{\cdot}_AM)\otimes_AB=\Lambda^{\cdot}_B(M\otimes_AB)$.

3. $\Lambda^{\cdot}(M/N)=(\Lambda^{\cdot}M)/\langle N\rangle$, *donde* N *es un submódulo de* M *y denotamos por* $\langle N\rangle$ *al ideal bilátero de* $\Lambda^{\cdot}M$ *generado por* $N\subset\Lambda^{\cdot}M$, *que es el* A*-módulo generado por* $N\wedge\Lambda^{\cdot}M$.

Demostración. Se demuestra igual que la proposición 0.8.25. □

31. Proposición: *Sea* E *un* A*-módulo libre de base* $\{e_1,\dots,e_n\}$. *Entonces,* Λ^rE *es un* A*-módulo libre de rango* $\binom{n}{r}$, *de base* $\{e_{i_1}\wedge\overset{r}{\cdots}\wedge e_{i_r}\}_{i_1<\cdots<i_r}$, *para* $0\le r\le n$; *y* $\Lambda^rE=0$, *para* $r>n$.

Demostración. Si $n=1$, es claro que $\Lambda^{\cdot}E=\Lambda^{\cdot}Ae_1=A\oplus A\cdot e_1$. Por inducción sobre el rango de E, se cumple que

$$\begin{aligned}\Lambda^{\cdot}E&=\Lambda^{\cdot}(Ae_1\oplus\overset{r}{\cdots}\oplus Ae_n)=\Lambda^{\cdot}(Ae_1)\otimes\Lambda^{\cdot}(Ae_2\oplus\overset{r}{\cdots}\oplus Ae_n)=\Lambda^{\cdot}(Ae_1)\otimes\overset{r}{\cdots}\otimes\Lambda^{\cdot}Ae_n\\&=(A\oplus Ae_1)\otimes\overset{r}{\cdots}\otimes(A\oplus Ae_n)\end{aligned}$$

Luego, $\Lambda^rE=\oplus_{i_1<\cdots<i_r}A\cdot e_{i_1}\wedge\overset{r}{\cdots}\wedge e_{i_r}$, para $r\le n$ y $\Lambda^rE=0$, para $r>n$. □

El morfismo $\Lambda^nM\to T^nM$, $m_1\wedge\cdots\wedge m_n\mapsto\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot m_{\sigma(1)}\otimes\cdots\otimes m_{\sigma(n)}$ compuesto con el epimorfismo natural $T^nM\to\Lambda^nM$, es una homotecia de factor $n!$. Podemos pensar los elementos de Λ^nM como ciertas aplicaciones multilineales hemisimétricas. Con precisión, sea $M^*=\operatorname{Hom}_A(M,A)$, tenemos el morfismo natural

$$\phi\colon\Lambda^nM\to\operatorname{Hem}_A(M^*,\overset{n}{\dots},M^*;A),\ m_1\wedge\overset{n}{\cdots}\wedge m_n\mapsto\phi(m_1\wedge\overset{n}{\cdots}\wedge m_n),$$

donde $\phi(m_1\wedge\overset{n}{\cdots}\wedge m_n)(w_1,\dots,w_n):=\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot w_{\sigma(1)}(m_1)\cdots w_{\sigma(n)}(m_n)$. Si M es un A-módulo libre finito generado entonces

$$\Lambda^nM=\operatorname{Hem}_A(M^*,\overset{n}{\dots},M^*;A)=(\Lambda^nM^*)^*.$$

32. Definición: Sea E un A-módulo libre de rango n y $T\colon E \to E$ un endomorfismo A-lineal. Entonces, $\Lambda^n E \simeq A$ y el morfismo inducido

$$\Lambda^n T\colon \Lambda^n E \to \Lambda^n E,\ \Lambda^n T(e_1 \wedge \cdots \wedge e_n) = T(e_1) \wedge \cdots \wedge T(e_n),$$

es una homotecia por un escalar, que llamaremos determinante de T y denotaremos $\det(T)$. Es decir,

$$\Lambda^n T(e_1 \wedge \cdots \wedge e_n) = T(e_1) \wedge \cdots \wedge T(e_n) = \det(T) \cdot e_1 \wedge \cdots \wedge e_n.$$

33. Teorema: *Sea E un módulo libre de rango n y T, T' dos endomorfismos lineales. Entonces,*

$$\det(T \circ T') = \det(T) \cdot \det(T')$$

Demostración. Se cumple que que $\Lambda^n(T) \circ \Lambda^n(T') = \Lambda^n(T \circ T')$:

$$\begin{aligned}(\Lambda^n(T) \circ \Lambda^n(T'))(e_1 \wedge \cdots \wedge e_n) &= \Lambda^n(T)(T'(e_1) \wedge \cdots \wedge T'(e_n)) = (T \circ T')(e_1) \wedge \cdots \wedge (T \circ T')(e_n) \\ &= \Lambda^n(T \circ T')(e_1 \wedge \cdots \wedge e_n)\end{aligned}.$$

Por tanto, multiplicar (en $\Lambda^n E \simeq A$) por $\det(T')$ y después multiplicar por $\det(T)$ es igual a multiplicar por $\det(T \circ T')$. Es decir, $\det(T \circ T') = \det(T) \cdot \det(T')$. □

Sea E un módulo libre de rango n y base $\{e_1, \ldots, e_n\}$. Dada $\sigma \in S_n$, sea $\sigma\colon E \to E$ la aplicación lineal definida por $\sigma(e_i) := e_{\sigma(i)}$. Si $\sigma = (i, j)$ es una transposición, entonces

$$\det(\sigma) \cdot e_1 \wedge \overset{n}{\cdots} \wedge e_n = e_{\sigma(1)} \wedge \overset{n}{\cdots} \wedge e_{\sigma(n)} = -e_1 \wedge \overset{n}{\cdots} \wedge e_n = \operatorname{sign}(\sigma) \cdot e_1 \wedge \overset{n}{\cdots} \wedge e_n$$

Por lo tanto, $\operatorname{sign}(\sigma) = \det(\sigma)$. Por el teorema anterior, $\operatorname{sign}(\sigma) = \det(\sigma)$, para todo $\sigma \in S_n$.

Dados $v_1, \ldots, v_n \in E$, con $v_i = \sum_j \lambda_{ij} e_j$, tendremos que

$$\begin{aligned}&v_1 \wedge \cdots \wedge v_n = (\textstyle\sum_i \lambda_{1i} e_i) \wedge \cdots \wedge (\sum_i \lambda_{ni} e_i) = \sum_{i_1 \neq \cdots \neq i_n} \lambda_{1 i_1} \cdots \lambda_{n i_n} e_{i_1} \wedge \cdots \wedge e_{i_n} \\ &= \sum_{\sigma \in S_n} \lambda_{1\sigma(1)} \cdots \lambda_{n\sigma(n)} \cdot e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} = (\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \lambda_{1\sigma(1)} \cdots \lambda_{n\sigma(n)}) \cdot e_1 \wedge \cdots \wedge e_n.\end{aligned}$$

Sea $\{e_1, \ldots, e_n\}$ una base de E y (λ_{ij}) la matriz de T en esa base, entonces

$$T(e_1) \wedge \cdots \wedge T(e_n) = (\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \lambda_{1\sigma(1)} \cdots \lambda_{n\sigma(n)}) \cdot e_1 \wedge \cdots \wedge e_n,$$

luego $\det(T) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \lambda_{1\sigma(1)} \cdots \lambda_{n\sigma(n)}$.

34. Definición: Dada una matriz $A = (a_{ij})$ llamaremos menor pq de la matriz, que denotaremos por A_p^q, al determinante de la matriz que se obtiene suprimiendo en (a_{ij}) la columna p y la fila q.

35. Proposición: $\det(a_{ij}) = \sum_q (-1)^q a_{1q} A_1^q$.

Demostración. Sea $\{e_i\}$ una base. Entonces

$$\begin{aligned}
&\det(a_{ij}) \cdot e_1 \wedge \cdots \wedge e_n = (\sum_j a_{1j} e_j) \wedge \cdots \wedge (\sum_j a_{nj} e_j) = \sum_k a_{1k} e_k \wedge (\sum_j a_{2j} e_j) \wedge \cdots \wedge (\sum_j a_{nj} e_j) \\
&= a_{11} e_1 \wedge (\sum_{j \neq 1} a_{2j} e_j) \wedge \cdots \wedge (\sum_{j \neq 1} a_{nj} e_j) + \cdots + a_{1n} e_n \wedge (\sum_{j \neq n} a_{2j} e_j) \wedge \cdots \wedge (\sum_{j \neq n} a_{nj} e_j) \\
&= a_{11} A_1^1 \cdot e_1 \wedge \cdots \wedge e_n + \cdots + a_{1n} A_1^n \cdot e_n \wedge e_1 \wedge \cdots \wedge e_{n-1} \\
&= (\sum_j (-1)^j a_{1j} A_1^j) \cdot e_1 \wedge \cdots \wedge e_n
\end{aligned}$$

y hemos concluido. □

36. Sea $T\colon E \to E$ un isomorfismo lineal y sea $A = (a_{ij})$ la matriz de T en una base $\{e_j\}$ de E. Calculemos la matriz $B = (b_{ij})$ de T^{-1}: $T^{-1}(e_i) = \sum_j b_{ij} e_j$, luego

$$T^{-1}(e_i) \wedge e_1 \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge e_n = b_{ij} e_j \wedge e_1 \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge e_n = (-1)^j b_{ij} e_1 \wedge \cdots \wedge e_n$$

Aplicando $\Lambda^n T$, obtenemos

$$e_i \wedge T(e_1) \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge T(e_n) = b_{ij} (-1)^j \det(T) e_1 \wedge \cdots \wedge e_n$$

Como $e_i \wedge T(e_1) \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge T(e_n) = A_j^i \cdot (-1)^i e_1 \wedge \cdots \wedge e_n$, entonces

$$b_{ij} = (-1)^{i+j} \frac{A_j^i}{\det(a_{ij})}.$$

37. Probemos que $\det(T) = \det(T^*)$: $(\Lambda^n T)^* = \Lambda^n T^*$, es decir, el diagrama

$$\begin{array}{ccc}
\Lambda^n E^* & \xrightarrow{\Lambda^n T^*} & \Lambda^n E^* \\
\downarrow & & \downarrow \\
(\Lambda^n E)^* & \xrightarrow[(\Lambda^n T)^*]{} & (\Lambda^n E)^*
\end{array}$$

es conmutativo. $(\Lambda^n T)^*$ es una homotecia por $\det(T)$ y $\Lambda^n T^*$ es una homotecia por $\det(T^*)$, luego los determinantes coinciden.

0.9. Módulos planos y proyectivos

1. Definición: Diremos que un A-módulo P es plano, si para toda sucesión exacta $0 \to N' \to N \to N'' \to 0$, la sucesión $0 \to N' \otimes_A P \to N \otimes_A P \to N'' \otimes_A P \to 0$ es exacta. Es decir, "P es plano si el funtor $- \otimes_A P$ es exacto". Por la proposición 0.8.8, P es plano si para toda inyección $N \hookrightarrow M$ entonces el morfismo $N \otimes_A P \to M \otimes_A P$ también es inyectivo.

2. Ejemplo: Los módulos libres son planos, porque $N \otimes_A A^{(I)} = N^{(I)}$.

3. Proposición: *1. Si P es un A-módulo plano y $A \to B$ es un morfismo de anillos, entonces $P_B := P \otimes_A B$ es un B-módulo plano.*

2. La suma directa de módulos es plana si y solo si los sumandos son planos.

Demostración. 1. Para todo B-módulo M tenemos que $P_B \otimes_B M = P \otimes_A M$, así que la exactitud del funtor $P_B \otimes_B (-)$ es consecuencia de la exactitud del funtor $P \otimes_A (-)$.

2. Es consecuencia inmediata de que el producto tensorial conmuta con sumas directas. □

4. Proposición: *La condición necesaria y suficiente para que un A-módulo P sea plano, es que P_x sea un A_x-módulo plano, para todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración. Denotemos toda sucesión exacta $0 \to N' \to N$ de A-módulos por $N^\bullet$. P es plano $\iff$ para toda sucesión exacta $N^\bullet$ entonces $N^\bullet \otimes_A P$ es exacta $\iff$ para todo punto cerrado $x \in \operatorname{Spec} A$ la sucesión $(N^\bullet \otimes_A P)_x = N^\bullet_x \otimes_{A_x} P_x$ es exacta $\iff$ P_x es un A_x-módulo plano para todo punto cerrado $x \in \operatorname{Spec} A$ □

5. Lema: *Sea $\mathcal{O}$ un anillo local y M un $\mathcal{O}$-módulo finito generado. Si el morfismo natural $I \otimes_{\mathcal{O}} M \to M$, $i \otimes m \mapsto im$, es inyectivo para todo ideal finito generado $I \subseteq \mathcal{O}$, entonces M es un $\mathcal{O}$-módulo libre y por tanto plano.*

Demostración. Sea $m_1, \ldots, m_r$ un sistema de generadores de M, obtenido por el lema de Nakayama (es decir, de modo que $\bar{m}_1, \ldots, \bar{m}_r$ sea una base de $M/\mathfrak{m}M$, donde $\mathfrak{m}$ es el ideal maximal de $\mathcal{O}$). Dada una relación $a_1 m_1 + \cdots + a_r m_r = 0$, consideremos el ideal $I = (a_1, \ldots, a_r)$. Por hipótesis el morfismo natural $I \otimes_{\mathcal{O}} M \to M$ es inyectivo, así que $a_1 \otimes m_1 + \cdots + a_r \otimes m_r = 0$. En el $\mathcal{O}/\mathfrak{m}$-espacio vectorial

$$\begin{aligned}(I \otimes_{\mathcal{O}} M)/\mathfrak{m}(I \otimes_{\mathcal{O}} M) = (I \otimes_{\mathcal{O}} M) \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = (I \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}) \otimes_{\mathcal{O}/\mathfrak{m}} (M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}) \\ = I/\mathfrak{m}I \otimes_{\mathcal{O}/\mathfrak{m}} M/\mathfrak{m}M\end{aligned}$$

tendremos que $\overline{a_1 \otimes m_1 + \cdots + a_r m_r} = \bar{a}_1 \otimes \bar{m}_1 + \cdots + \bar{a}_r \otimes \bar{m}_r = 0$. Pero $\bar{m}_1, \ldots, \bar{m}_r$ es una base de $M/\mathfrak{m}M$, por tanto $\bar{a}_1 = \cdots = \bar{a}_r = 0$. Luego $I/\mathfrak{m}I = 0$ y por el lema de Nakayama $I = 0$. En conclusión, $m_1, \ldots, m_r$ es una base de M y M es libre. □

6. Teorema: *Un módulo finito generado es plano si y solo si es localmente libre.*

Demostración. Es consecuencia del lema y la proposición anteriores. □

7. Criterio del ideal de platitud: *Sea M un A-módulo finito generado. Si el morfismo natural $I \otimes_A M \to M$ es inyectivo para todo ideal $I \subseteq A$, entonces M es un A-módulo plano.*

Demostración. En cada punto cerrado $x \in \operatorname{Spec} A$ tenemos que el morfismo natural

$$I_x \otimes_{A_x} M_x = (I \otimes_A M)_x \to M_x$$

es inyectivo. Como cada ideal finito generado de A_x es localización de un ideal finito generado de A, el lema anterior permite concluir que M_x es un A_x-módulo plano. Luego, M es un A-módulo plano, por 0.9.4. □

8. Notación: Dado $x \in \operatorname{Spec} A$, denotemos a su cuerpo residual $k(x) := A_x/\mathfrak{p}_x A_x$.

9. Proposición: *Sea A un anillo reducido y M un A-módulo finito generado. Si $\dim_{k(x)} M \otimes_A k(x) = n$, para todo punto $x \in \operatorname{Spec} A$, entonces M es localmente libre de rango n, luego M es plano.*

Demostración. Sea $m_1, \ldots, m_n$ un sistema generador de M_x obtenido por Nakayama y $f : L = A_x^n \to M_x$ el epimorfismo definido por $f((a_i)) = \sum_i a_i m_i$. Sea $l \in \operatorname{Ker} f \subseteq L$. Dado $y \in \operatorname{Spec} A_x$, si $l \notin \mathfrak{p}_y \cdot L$, entonces $0 \neq \bar{l} \in (L/\mathfrak{p}_y \cdot L)_y = L \otimes_A k(y) = k(y)^n$ y pertenece al núcleo del epimorfismo $L \otimes_A k(y) \to M \otimes_A k(y)$, luego $\dim_{k(y)} M \otimes_A k(y) < n$ y llegamos a contradicción. Por tanto, $l \in \cap_{y \in \operatorname{Spec} A_x} \mathfrak{p}_y \cdot L = \prod_n (\cap_{y \in \operatorname{Spec} A_x} \mathfrak{p}_y) = 0$, porque A_x es reducido. En conclusión, $\operatorname{Ker} f = 0$ y M_x es libre.

□

10. Definición: Se dice que un módulo M es fielmente plano, si cumple que toda sucesión es exacta si y solo si lo es al tensarla por el módulo M.

11. Lema: *Sea M un A-módulo plano.*

1. *Sea* $f: N \to N'$ *es un morfismo de* A*-módulos y consideremos el morfismo inducido* $f \otimes \mathrm{Id}: N \otimes_A M \to N' \otimes_A M$, $f \otimes \mathrm{Id}(n \otimes m) := f(n) \otimes m$. *Entonces* $(\mathrm{Ker}\, f) \otimes_A M = \mathrm{Ker}(f \otimes \mathrm{Id})$ *e* $(\mathrm{Im}\, f) \otimes M = \mathrm{Im}(f \otimes \mathrm{Id})$

2. *Sean* $N, N' \subset P$ *dos submódulos. Entonces,* $(N \otimes_A M) + (N' \otimes M) = (N + N') \otimes_A M$.

Demostración. 1. Consideremos los morfismos $\mathrm{Ker}\, f \hookrightarrow N \twoheadrightarrow \mathrm{Im}\, f \hookrightarrow N'$ y tensemos por M, $\mathrm{Ker}\, f \otimes_A M \hookrightarrow N \otimes_A M \twoheadrightarrow \mathrm{Im}\, f \otimes_A M \hookrightarrow N' \otimes M$. Ahora es fácil concluir.

2. Consideremos la sucesión de morfismos $N \oplus N' \twoheadrightarrow N + N' \hookrightarrow P$ y tensemos por M, $(N \otimes_A M) \oplus (N' \otimes_A M) = (N \oplus N') \otimes_A M \twoheadrightarrow (N + N') \otimes_A M \hookrightarrow P \otimes_A M$. □

12. Proposición: *Las siguientes afirmaciones son equivalentes*

1. M *es un* A*-módulo fielmente plano.*

2. M *es un* A*-módulo plano y cumple que* $M \otimes_A N = 0 \iff N = 0$.

3. M *es un* A*-módulo plano y* $M/\mathfrak{m}_x M \neq 0$ *para todo punto cerrado* $x \in \mathrm{Spec}\, A$.

Demostración. 1. $\Rightarrow$ 2. Si M es fielmente plano, es obviamente plano. Además, la sucesión $0 \to N \to 0$ es exacta si y solo si $0 \to M \otimes_A N \to 0$ es exacta. Es decir, $N = 0 \iff M \otimes_A N = 0$.

2 $\Rightarrow$ 1. Sea

$$N \xrightarrow{f} N' \xrightarrow{f'} N'' \qquad (*)$$

una sucesión y consideremos la sucesión

$$N \otimes_A M \xrightarrow{f \otimes 1} N' \otimes_A M \xrightarrow{f' \otimes 1} N'' \otimes_A M \qquad (**)$$

Por tanto,

$$[(\mathrm{Ker}\, f' + \mathrm{Im}\, f)/\mathrm{Im}\, f] \otimes_A M = (\mathrm{Ker}(f' \otimes 1) + \mathrm{Im}(f \otimes 1))/\mathrm{Im}(f \otimes 1).$$

Así pues, $(\mathrm{Ker}\, f' + \mathrm{Im}\, f)/\mathrm{Im}\, f = 0$ si y solo si $(\mathrm{Ker}(f' \otimes 1) + \mathrm{Im}(f \otimes 1))/(\mathrm{Im}\, f \otimes 1) = 0$. Igualmente, $(\mathrm{Ker}\, f' + \mathrm{Im}\, f)/\mathrm{Ker}\, f' = 0$ si y solo si $(\mathrm{Ker}(f' \otimes 1) + \mathrm{Im}(f \otimes 1))/\mathrm{Ker}(f' \otimes 1) = 0$. En conclusión, $(*)$ es exacta si y solo si $(**)$ es exacta.

2 $\Rightarrow$ 3. $A/\mathfrak{m}_x \neq 0$, luego $A/\mathfrak{m}_x \otimes_A M = M/\mathfrak{m}_x M \neq 0$.

3 $\Rightarrow$ 2. Si $N \neq 0$, sea $0 \neq n \in N$. Se cumple que $\langle n \rangle \simeq A/\mathrm{Anul}(n)$. Sea $\mathfrak{m}_x \subset A$ un ideal maximal que contenga a $\mathrm{Anul}(n)$. El epimorfismo $A/\mathrm{Anul}(n) \to A/\mathfrak{m}_x$ induce el epimorfismo $A/\mathrm{Anul}(n) \otimes_A M \to A/\mathfrak{m}_x \otimes_A M$, es decir, un epimorfismo $\langle n \rangle \otimes_A M \to M/\mathfrak{m}_x M$. En conclusión, como $M/\mathfrak{m}_x M \neq 0$, entonces $\langle n \rangle \otimes_A M \neq 0$ y $N \otimes_A M$, que contiene a $\langle n \rangle \otimes_A M$, es distinto de cero. □

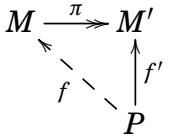
13. Definición: Diremos que un morfismo de anillos $f: A \to B$ es plano si B es un A-módulo plano. Diremos que un morfismo de anillos $f: A \to B$ es fielmente plano si B es un A-módulo fielmente plano.

14. Proposición: *Un morfismo $f: A \to B$ de anillos es fielmente plano si y solo si es plano y el morfismo inducido en los espectros es epiyectivo.*

Demostración. La fielplatitud es una propiedad local, por el punto 2 de 0.9.12.

Por la fórmula de la fibra, el morfismo $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo si y solo si $B_x/\mathfrak{p}_x B_x \neq 0$ para todo $x \in \operatorname{Spec} A$. Así pues, por la proposición 0.9.12, $f: A \to B$ es plano y el morfismo inducido en los espectros es epiyectivo si y solo si f es fielmente plano. □

15. Definición: Se dice que un A-módulo P es proyectivo, si para todo epimorfismo $\pi: M \to M'$ entonces $\pi_*: \operatorname{Hom}_A(P,M) \to \operatorname{Hom}_A(P,M')$ es un epimorfismo. Es decir, dado $f': P \to M'$, existe un morfismo $f: P \to M$ de modo que el diagrama



es conmutativo.

Por el teorema 0.7.8, P es un A-módulo proyectivo si el funtor $\operatorname{Hom}_A(P,-)$ conserva sucesiones exactas, es decir, "$\operatorname{Hom}_A(P,-)$ es un funtor exacto".

Como $\operatorname{Hom}_A(A^{(I)},M) = \prod_I M$ es fácil demostrar que los A-módulos libres son proyectivos.

16. Proposición: *Un A-módulo es proyectivo si y solo si es sumando directo de un libre.*

Demostración. Supongamos que P es un A-módulo proyectivo. Consideremos un epimorfismo de un A-módulo libre en P, $\pi: A^{(I)} \to P$. Si consideramos el morfismo $\mathrm{Id}: P \to P$ sabemos que levanta a un morfismo $s: P \to A^{(I)}$, tal que $\pi \circ s = \mathrm{Id}$, por ser P proyectivo. Por el ejercicio 0.6.80, $A^{(I)} = \operatorname{Ker}\pi \oplus P$.

Recíprocamente, sea M es un sumando directo de un libre, es decir, $A^{(I)} = M \oplus M'$. $A^{(I)}$ es un módulo proyectivo, por tanto $M \oplus M'$ es proyectivo. Ahora bien, como $\operatorname{Hom}_A(M \oplus M', -) = \operatorname{Hom}_A(M,-) \times \operatorname{Hom}_A(M',-)$ es fácil probar que una suma directa de módulos es un módulo proyectivo si y solo si lo es cada sumando. En conclusión, M es proyectivo. □

17. Proposición: *Los módulos proyectivos son planos.*

Demostración. Los módulos proyectivos son sumandos directos de un libre, que es plano, luego los módulos proyectivos son planos. □

18. Proposición: *Los módulos proyectivos finito generados son módulos de presentación finita.*

Demostración. Sea P un A-módulo proyectivo finito generado y $\pi: A^n \to P$ un epimorfismo. Entonces, $A^n = P \oplus \operatorname{Ker}\pi$ y $\operatorname{Ker}\pi \simeq A^n/P$. Luego, $\operatorname{Ker}\pi$ es un A-módulo finito generado y P es de presentación finita. □

19. Proposición: *Si P es un A-módulo proyectivo y $A \to B$ un morfismo de anillos, entonces P_B es un B-módulo proyectivo.*

Demostración. Si P es sumando directo de un A-módulo libre, entonces P_B es sumando directo de un B-módulo libre. □

20. Proposición: *Sea M un A-módulo de presentación finita y $S \subset A$ un sistema multiplicativo. Entonces para todo A-módulo N se cumple que*

$$\operatorname{Hom}_A(M,N)_S = \operatorname{Hom}_{A_S}(M_S,N_S)$$

Demostración. Si un A-módulo $L \simeq A^r$ es libre entonces $\operatorname{Hom}_A(L,N)_S = (N^r)_S = (N_S)^r = \operatorname{Hom}_{A_S}(L_S,N_S)$.

Por hipótesis existe una sucesión exacta $A^m \xrightarrow{\phi} A^n \to M \to 0$. Tomando $\operatorname{Hom}_A(-,N)$ obtenemos la sucesión exacta

$$0 \to \operatorname{Hom}_A(M,N) \to \operatorname{Hom}_A(A^n,N) \xrightarrow{\phi^*} \operatorname{Hom}_A(A^m,N)$$

Localizando por S tenemos la sucesión exacta

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}_A(M,N)_S & \longrightarrow & \operatorname{Hom}_A(A^n,N)_S & \longrightarrow & \operatorname{Hom}_A(A^m,N)_S \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & \operatorname{Ker}\phi_S^* & \longrightarrow & \operatorname{Hom}_{A_S}(A_S^n,N_S) & \xrightarrow{\phi_S^*} & \operatorname{Hom}_{A_S}(A_S^m,N_S)
\end{array}$$

Ahora bien, tomando $\operatorname{Hom}_{A_S}(-,N_S)$ en la sucesión exacta $A_S^m \to A_S^n \to M_S \to 0$, concluimos que $\operatorname{Ker}\phi_S^* = \operatorname{Hom}_{A_S}(M_S,N_S)$ y terminamos.

□

21. Teorema: *Un módulo P de presentación finita es proyectivo si y solo si es localmente proyectivo (es decir, para todo $x \in \operatorname{Spec} A$, M_x es un A_x-módulo proyectivo).*

Demostración. Denotemos la sucesión exacta $0 \to N' \to N \to N'' \to 0$ por $N^\bullet$. Digamos que un módulo P es proyectivo si y solo si para toda sucesión exacta $N^\bullet$ de A-módulos entonces la sucesión $\operatorname{Hom}_A(P, N^\bullet)$ es exacta. Con estas convenciones tenemos: P es proyectivo $\iff$ para toda sucesión exacta $N^\bullet$ de A-módulos $\operatorname{Hom}_A(P, N^\bullet)$ es exacta $\iff$ para toda sucesión exacta $N^\bullet$ de A-módulos $\operatorname{Hom}_A(P, N^\bullet)_x = \operatorname{Hom}_{A_x}(P_x, N_x^\bullet)$ es exacta para todo punto cerrado $x \in \operatorname{Spec} A \iff P_x$ es un A_x-módulo proyectivo (pues toda sucesión exacta de A_x-módulos $N'^\bullet$ es localización de una sucesión exacta de A-módulos, explícitamente $(N'^\bullet)_x = N'^\bullet$). □

22. Teorema: *Las condiciones de ser plano, localmente libre y proyectivo son equivalentes para los módulos de presentación finita.*

Demostración. Si M es plano, por 0.9.6, es localmente libre.

Si M es localmente libre entonces es localmente proyectivo. Como la propiedad de ser proyectivo es local M es proyectivo.

Si M es proyectivo, por 0.9.17, es plano. □

23. Proposición: *Un módulo M finito generado es proyectivo si y solo si existe un recubrimiento finito $\{U_{a_i}\}$ por abiertos básicos de $\operatorname{Spec} A$, de modo que M_{a_i} es un A_{a_i}-módulo libre.*

Demostración. Sea M proyectivo. Dado $x \in \operatorname{Spec} A$ existe un isomorfismo

$$A_x \oplus \cdots \oplus A_x \simeq M_x$$

Por tanto, existe un entorno $U_a = \operatorname{Spec} A_a$ de x, donde tenemos definido un morfismo $\pi_a : A_a \oplus \cdots \oplus A_a \to M_a$, que localizado en x es isomorfismo. $(\operatorname{Coker} \pi_a)_x = 0$, por tanto existe un entorno $U_{a'} \subset U_a$ de x, de modo que $(\operatorname{Coker} \pi_a)_{a'} = 0$. Es decir, podemos suponer que π_a es epiyectivo. Como M_a es un A_a-módulo proyectivo, π_a tiene sección, luego $\operatorname{Ker} \pi_a$ es un cociente de $A_a \oplus \cdots \oplus A_a$ y es finito generado. $(\operatorname{Ker} \pi_a)_x = 0$, por tanto existe un entorno $U_{a'} \subset U_a$ de x, de modo que $(\operatorname{Ker} \pi_a)_{a'} = 0$. Es decir, podemos suponer que π_a es un isomorfismo. Así podremos construir para cada punto $x \in \operatorname{Spec} A$ un entorno básico donde M es libre. Como $\operatorname{Spec} A$ es compacto, podremos construir el recubrimiento finito buscado.

Si existe un recubrimiento finito $\{U_{a_i}\}$ por abiertos básicos de $\operatorname{Spec} A$, de modo que M_{a_i} es un A_{a_i}-módulo libre, obviamente M es localmente libre. Solo nos falta probar que es de presentación finita. Sea

$$\pi : A \oplus \cdots \oplus A \to M$$

un epimorfismo. M_{a_i} es un A_{a_i}-módulo libre, luego proyectivo. Por tanto, al localizar por a_i, π tiene sección y $(\operatorname{Ker}\pi)_{a_i}$ es finito generado. Si escribimos $(\operatorname{Ker}\pi)_{a_i} = \langle \frac{m_{i_1}}{1}, \ldots, \frac{m_{i_{n_i}}}{1} \rangle$, con $m_{i_j} \in \operatorname{Ker}\pi$, entonces $\operatorname{Ker}\pi$ está generado por $\{m_{i_j}\}_{i_j}$, porque así es localmente. En conclusión, $\operatorname{Ker}\pi$ es finito generado y M es de presentación finita. □

0.10. Ideales de Fitting. Estratos de $\operatorname{Spec} A$ en los que un A-módulo M es libre

Como sabemos, en los módulos a diferencia de los espacios vectoriales, aunque existan sistemas de generadores no existen bases, en general. Los ideales de Fitting de un A-módulo miden la obstrucción por la que el módulo no es libre.

1. Notación: En esta sección, los módulos considerados serán de presentación finita.

Queremos probar que todas las presentaciones de M por libres

$$A^m \to A^n \to M \to 0$$

son "salvo elección de bases, esencialmente equivalentes".

2. Proposición: *Sea M un A-módulo de presentación finita. Si $\pi' \colon A^m \to M$ es un epimorfismo entonces $\operatorname{Ker}\pi'$ es un A-módulo finito generado.*

Demostración. Sabemos que tenemos un epimorfismo $\pi \colon A^n \to M$, tal que $\operatorname{Ker}\pi$ es un A-módulo finito generado. Sea $f \colon A^n \to A^m$ un morfismo de A-módulos, tal que $\pi' \circ f = \pi$. Obviamente, $f(\operatorname{Ker}\pi) \subseteq \operatorname{Ker}\pi'$. Tenemos el diagrama de fila superior exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\operatorname{Ker}\pi'/f(\operatorname{Ker}\pi)) & \longrightarrow & (A^m/f(\operatorname{Ker}\pi)) & \xrightarrow{\bar{\pi}'} & M & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle \bar{f}} & \nearrow_{\bar{\pi}} & & & \\ & & & & A^n/\operatorname{Ker}\pi & & & & \end{array}$$

Luego, $A^m/f(\operatorname{Ker}\pi) \simeq M \oplus (\operatorname{Ker}\pi'/f(\operatorname{Ker}\pi))$. Por tanto, $\operatorname{Ker}\pi'/f(\operatorname{Ker}\pi)$ es finito generado y $\operatorname{Ker}\pi'$ es finito generado. □

Sea A un anillo local, de ideal maximal $\mathfrak{m}$ y M un A-módulo de presentación finita. Sea $\{m_1, \ldots, m_r\}$ un sistema generador mínimo de M (que equivale a decir que $\{\bar{m}_1, \ldots, \bar{m}_r\}$ es una base de $M/\mathfrak{m}M$). Consideremos el epimorfismo $\pi \colon A^r \to M$, $\pi(a_i) = \sum_i a_i m_i$. Sea $\{n_1, \ldots, n_s\}$ un sistema generador mínimo de $\operatorname{Ker}\pi$ y $A^s \to \operatorname{Ker}\pi$ el epimorfismo inducido. Con todo, tenemos una presentación por libres

$$A^s \xrightarrow{\varphi} A^r \xrightarrow{\pi} M \to 0$$

que denominaremos presentación libre minimal de M. Denotaremos por (φ) a la matriz asociada a φ en las bases estándar de los módulos libres.

3. Lema: *Sea A un anillo local de ideal maximal $\mathfrak{m}$. Sea L un A-módulo libre finito generado. Se cumple que $\{e_1,\dots,e_n\}\subset L$ es una base de L si y solo si $\{\bar{e}_1,\dots,\bar{e}_n\}$ es una base del $A/\mathfrak{m}$-espacio vectorial $L/\mathfrak{m}L$.*

Demostración. Obviamente, si $\{u_1,\dots,u_n\}\subset L$ es una base de L entonces $\{\bar{u}_1,\dots,\bar{u}_n\}$ es una base de $L/\mathfrak{m}L$.

Consideremos en L una base $\{u_1,\dots,u_n\}$. Escribamos $e_i=\sum_j a_{ij}u_j$. La matriz (a_{ij}) es invertible si y solo si su determinante es invertible. Como A es local, $a\in A$ es invertible si y solo si $\bar{a}\in A/\mathfrak{m}$ es invertible. Por tanto, la matriz (a_{ij}) es invertible si y solo si la matriz de sus clases $(\bar{a}_{ij})$ es invertible. En conclusión, $\{e_1,\dots,e_n\}\subset L$ es una base de L si y solo si $\{\bar{e}_1,\dots,\bar{e}_n\}$ es una base de $L/\mathfrak{m}L$. □

4. Teorema: *Sea A un anillo local y M un A-módulo de presentación finita. Dada una presentación por libres $A^m \xrightarrow{\phi} A^n \xrightarrow{\pi'} M\to 0$, escogiendo apropiadamente bases de los libres, la matriz asociada a ϕ es*

$$(\phi)=\begin{pmatrix}(\varphi) & 0 & 0\\ 0 & (\mathrm{Id}) & 0\end{pmatrix}$$

Demostración. Siguiendo las notaciones precedentes sea $m_1,\dots,m_r$ un sistema generador mínimo de M. Sea $e_1,\dots,e_n$ una base de A^n de modo que $\pi'(e_i)=m_i$, para $i\le r$. Escribamos $\pi'(e_j)=\sum_i a_{ji}m_i$, para $j>r$. Sea $e'_j=e_j-\sum_i a_{ji}e_i$, para $j>r$. Tenemos que $\{e_1,\dots,e_r,e'_{r+1},\dots,e'_n\}$ es una base de A^n de modo que $\pi'(e_i)=m_i$ y $\pi'(e'_j)=0$. Descompongamos del modo obvio $A^n=A^r\oplus A^{n-r}$, tenemos que $\operatorname{Ker}\pi'=\operatorname{Ker}\pi\oplus A^{n-r}$. Sabemos que $\operatorname{Im}\phi=\operatorname{Ker}\pi'$. Por tanto, tenemos el epimorfismo $A^m\xrightarrow{\phi}\operatorname{Ker}\pi'=\operatorname{Ker}\pi\oplus A^{n-r}$. De nuevo, tenemos una base $v_1,\dots,v_m$ en A^m, de modo que $\phi(v_i)=n_i$, para $i\le s$ (recordemos que denotamos por $n_1,\dots,n_s$ a un sistema generador minimal de $\operatorname{Ker}\pi$), $\phi(v_{s+i})=e'_{r+i}$, para $i\le n-r$ y $\phi(v_i)=0$, para $i\ge s+n-r$. En las bases, $\{v_1,\dots,v_m\}$, $\{e_1,\dots,e_r,e'_{r+1},\dots,e'_n\}$, la matriz asociada a ϕ es

$$(\phi)=\begin{pmatrix}(\varphi) & 0 & 0\\ 0 & (\mathrm{Id}) & 0\end{pmatrix}$$

□

Sea $A^m \xrightarrow{\phi} A^n \xrightarrow{\pi'} M \to 0$ una presentación libre de M.

5. Definición: Llamaremos ideal de Fitting i-ésimo de M, $F_i^{\phi}(M)$, al ideal de A generado por los menores de orden $n-i$ de ϕ.

Si $n-i \leq 0$ seguiremos la convención $F_i^{\phi}(M) = A$. Si $n-i > m$ seguiremos la convención $F_i^{\phi}(M) = 0$.

Dicho de otro modo, $F_i^{\phi}(M)$ es el ideal generado por los coeficientes de la matriz $\Lambda^{n-i}\phi\colon \Lambda^{n-i}A^m \to \Lambda^{n-i}A^n$, es decir, es el ideal $I \subset A$ mínimo tal que el morfismo $\Lambda^{n-i}\phi \otimes 1\colon (\Lambda^{n-i}A^m)\otimes A/I \to (\Lambda^{n-i}A^n)\otimes A/I$ es nulo.

Sea $A \to B$ un morfismo de anillos y tensando por $\otimes_A B$ obtenemos la presentación libre

$$B^m \xrightarrow{\phi\otimes 1} B^n \xrightarrow{\pi\otimes 1} M\otimes_A B \to 0$$

6. Proposición: $F_i^{\phi\otimes 1}(M\otimes_A B) = F_i^{\phi}(M)\cdot B$. *"Los ideales de Fitting conmutan con cambios de anillo base".*

Demostración. Es una consecuencia directa de que la matriz asociada a ϕ es la misma que la de $\phi\otimes 1$. □

7. Proposición: *Los ideales de Fitting de M no dependen de la presentación libre de M considerada.*

Demostración. Dos ideales son iguales si y solo si son iguales localmente. Por la proposición anterior podemos suponer que A es local. Es una sencilla comprobación, usando el teorema anterior, que $F_i^{\phi}(M) = F_i^{\varphi}(M)$. □

8. Notación: Escribiremos simplemente $F_i^{\phi}(M) = F_i(M)$. Cuando sea necesario precisar cuál es el anillo escribiremos $F_i(M) = F_i^A(M)$.

9. Proposición: $F_0(M) \subseteq F_1(M) \subseteq \cdots \subseteq F_n(M) = A$.

Demostración. Los menores de orden $n-i$ de una matriz son combinación lineal de los menores de orden $n-i-1$ de la matriz. Por tanto, $F_i(M) \subseteq F_{i+1}(M)$. □

10. Proposición: *Sea M un A-módulo de presentación finita. Entonces,*

$$(F_i(M))_0 = \{x \in \operatorname{Spec} A :\ \dim_{k(x)}(M\otimes_A k(x)) > i\}$$

donde $k(x) := A_x/\mathfrak{p}_x A_x$ es el cuerpo residual de x. Por tanto, la función $\operatorname{Spec} A \to \mathbb{N}$, que asigna a cada x el número natural $\dim_{k(x)}(M_x/\mathfrak{p}_x M_x)$ es superiormente continua.

Demostración. Observemos que $x \in (F_i(M))_0$ si y solo si $F_i(M)\cdot(A/\mathfrak{p}_x) = 0$, que equivale a $F_i(M)\cdot k(x) = 0$. Por la proposición 0.10.6, $F_i(M)\cdot k(x) = F_i^{k(x)}(M_x/\mathfrak{p}_x M_x)$, $k(x)$ es un cuerpo, y $F_i^{k(x)}(M_x/\mathfrak{p}_x M_x) = 0$ si y solo si $\dim_{k(x)}(M_x/\mathfrak{p}_x M_x) > i$. □

11. Corolario: *Sea M un A-módulo de presentación finita. Entonces,*

$$\operatorname{Sop} M = (F_0(M))_0$$

Demostración. Es consecuencia del lema de Nakayama y de la proposición anterior. □

Estudiemos la relación entre $\operatorname{Anul} M$ y $F_0(M)$.

12. Proposición: *Sea $I \subset A$ un ideal finito generado. Entonces,*

$$F_i^A(M/IM) = F_i^A(M) + I\cdot F_{i+1}^A(M) + \cdots + I^{n-i}F_n^A(M).$$

Demostración. Dar la presentación libre

$$A^m \xrightarrow{\phi} A^n \to M \to 0$$

equivale a decir que $M = A^n/\langle v_1,\ldots,v_m\rangle$, donde los vectores $\{v_i\}$, son la imagen por ϕ de la base estándar de A^m. La matriz asociada a ϕ es la matriz formada por los vectores v_i. $F_i(M)$ es el ideal generado por los menores de orden $n-i$ de la matriz formada por los vectores $\{v_i\}$. Tenemos que

$$M/IM = (A^n/\langle v_1,\ldots,v_m\rangle)/I(A^n/\langle v_1,\ldots,v_m\rangle) = A^n/(\langle v_1,\ldots,v_m\rangle + I\cdot A^n)$$

Si $I = \langle i_1,\ldots,i_r\rangle$, $F_i(M/IM)$ es el ideal generado por los menores de orden $n-i$, de la matriz formada por los vectores $\{v_i\}$ y los vectores $\{(0,\ldots,\overset{j}{i_k},\ldots,0)\}_{j,k}$. Ahora, mediante un sencillo cálculo se obtiene la proposición. □

13. Corolario: *Se cumple que* $\operatorname{Anul}(M)\cdot F_{i+1}(M) \subseteq F_i(M)$*, luego* $\operatorname{Anul}^n(M) \subseteq F_0(M)$.

Demostración. Para todo ideal $I \subset \operatorname{Anul}(M)$ finito generado, se cumple que $F_i(M) = F_i(M/I\cdot M)$. Por la proposición anterior, $F_i(M) = F_i(M) + I\cdot F_{i+1}(M) + \cdots + I^{n-i}\cdot F_n(M)$, luego $I\cdot F_{i+1}(M) \subseteq F_i(M)$. Por tanto, $\operatorname{Anul}(M)\cdot F_{i+1}(M) \subseteq F_i(M)$.

□

14. Proposición: *Se cumple que* $F_0(M) \subseteq \operatorname{Anul}(M)$.

Demostración. Tenemos que $M = A^n/\langle v_1,\dots,v_m\rangle$. Podemos suponer, añadiendo ceros, que $m \geq n$. Sabemos que una matriz cuadrada (a_{ij}), multiplicada por la matriz de sus adjuntas es la matriz $\det(a_{ij})\cdot \mathrm{Id}$. Consideremos la matriz cuadrada (a_{ij}) definida por n vectores $v_1,\dots,v_n$. Sea Ad_{kl} el menor complementario del coeficiente kl de la matriz (a_{ij}), afectado del signo $(-1)^{i+j}$. Se cumple que

$$(0,\dots,\overset{k}{\det(a_{ij})},\dots,0) = \sum_{l=1}^{n} Ad_{kl}v_l.$$

Como consecuencia, $\det(a_{ij})\cdot M = 0$. En conclusión, $F_0(M)\cdot M = 0$.

□

15. Notación: Dado un cerrado $C = (I)_0 = \mathrm{Spec}A/I \overset{i}{\hookrightarrow} \mathrm{Spec}A$, denotaremos $M_{|C} = M/IM$.

16. Proposición: *M es un A-módulo localmente libre de rango $i+1$ si y solo si $F_i(M) = 0$ y $F_{i+1}(M) = A$.*

En particular, $M_{|(F_i(M))_0}$ es un $A_{|(F_i(M))_0}$-módulo localmente libre de rango $i+1$ en los puntos del abierto $U_{i+1} := (F_i(M))_0 \setminus (F_{i+1}(M))_0$ de $(F_i(M))_0$.

Demostración. Los ideales de Fitting conmutan con localizaciones. Por tanto, podemos suponer que el anillo es local, de ideal maximal $\mathfrak{m}$.

Obviamente, si M es libre de rango $i+1$, $F_i(M) = 0$ y $F_{i+1}(M) = A$.

Recíprocamente, supongamos que $F_i(M) = 0$ y $F_{i+1}(M) = A$. Tenemos que $M/\mathfrak{m}M$ es un $A/\mathfrak{m}A$-espacio vectorial, digamos de dimensión r. Luego, $F_s^{A/\mathfrak{m}A}(M/\mathfrak{m}M) = 0$ si $s < r$ y $F_s^{A/\mathfrak{m}A}(M/\mathfrak{m}M) = A/\mathfrak{m}$ si $s \geq r$. Ahora bien, $F_i^{A/\mathfrak{m}A}(M/\mathfrak{m}M) = F_i(M)\cdot A/\mathfrak{m} = 0$ y $F_{i+1}^{A/\mathfrak{m}A}(M/\mathfrak{m}M) = F_{i+1}(M)\cdot A/\mathfrak{m} = A/\mathfrak{m}$. En conclusión, $r = i+1$. Consideremos la presentación por libres minimal de M

$$A^s \overset{\varphi}{\to} A^{i+1} \to M \to 0$$

Sabemos que $F_i(M) = 0$, luego $\varphi = 0$ y M es libre de rango $i+1$.

Por último, $F_i^{A_{|(F_i(M))_0}}(M_{|(F_i(M))_0}) = 0$ y para todo $x \notin (F_{i+1}(M))_0$, $(F_{i+1}(M))_x = A_x$. Luego, $M_{|(F_i(M))_0}$ es localmente libre de rango $i+1$ en los puntos del abierto U_{i+1}.

□

Observemos que $\mathrm{Spec}A = U_0 \coprod (F_0(M))_0 = U_0 \coprod U_1 \coprod (F_1(M))_0$ y recurrentemente tenemos

$$\boxed{\mathrm{Spec}A = U_0 \coprod \dots \coprod U_n}$$

Los conjuntos U_i son abiertos en su cierre $\overline{U_i}$. Por abuso de notación, a falta del concepto de esquema, diremos "$M_{|U_i}$ es localmente libre", si $M_{|\overline{U_i}}$ es localmente libre en los puntos del abierto U_i. Observemos que $M_{|U_i}$ es localmente libre de rango i, para cada i.

17. Proposición: *Sea $f: A \to B$ un morfismo de anillos y $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido en espectros. Se cumple que $f^*M := M \otimes_A B$ es un B-módulo localmente libre de rango $i+1$, si y solo si f^* valora en $U_{i+1} = (F_i(M))_0 \setminus (F_{i+1}(M))_0$, con precisión, f factoriza a través $A \to A/F_i(M)$ e $\operatorname{Im} f^* \subseteq U_{i+1}$.*

Demostración. Por la proposición anterior, $f^*M = M \otimes_A B$ es localmente libre de rango $i+1$ si y solo si $0 = F_i^B(M \otimes_A B) = F_i^A(M) \cdot B$ y $B = F_{i+1}^B(M \otimes_A B) = F_{i+1}^A(M) \cdot B$. Que equivale a decir, que tenemos la factorización $A \to A/F_i(M) \to B$ e $\operatorname{Im} f^* \cap (F_{i+1}(M))_0 = \emptyset$.

□

18. Ejercicio: Prueba que si $M \to M'$ es epiyectivo, entonces $F_i(M) \subseteq F_i(M')$.

19. Ejercicio: Prueba que si $M = M' \oplus M''$, entonces $F_i(M) = \sum_{l'+l''=i} F_{l'}(M') \cdot F_{l''}(M'')$.

20. Ejercicio: Sea $\pi: A^n \to M$ un epimorfismo de A-módulos. Prueba que $F_0(\Lambda^n M) = F_{n-1}(M)$.

0.11. Límites proyectivos e inductivos

Sea I un conjunto ordenado, diremos que es filtrante decreciente si para cada par $i, j \in I$ existe algún $k \in I$ que cumple que $k \leq i$ y $k \leq j$.

1. Definición: Sea I un conjunto filtrante decreciente. Un conjunto de objetos $\{M_i\}_{i \in I}$ de una categoría $\mathscr{C}$, junto con morfismos $f_{ij}: M_i \to M_j$, para cada $i \leq j$, diremos que es un sistema proyectivo de objetos de $\mathscr{C}$ si satisface las siguientes condiciones

1. $f_{ii} = \mathrm{Id}$, para todo i.
2. $f_{jk} f_{ij} = f_{ik}$ siempre que $i \leq j \leq k$.

Sin tanto formalismo, un sistema proyectivo de objetos $\{M_i\}_{i \in I}$ es un "río de flechas"

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M_r & \longrightarrow & M_l & \longrightarrow & M_k & \longrightarrow & M_i \\ & & & \searrow & & & & \searrow & \\ & & & & M_m & & & & M_j \\ & & & & & \searrow & & & \\ & & & & & & M_n & & \end{array}$$

2. Definición: Sea $\{M_i\}_{i\in I}$ un sistema proyectivo de objetos. Diremos que M (si existe) es el límite proyectivo de $\{M_i\}_{i\in I}$, y lo denotaremos $\varprojlim_i M_i$, si cumple una igualdad funtorial

$$\mathrm{Hom}_{\mathscr{C}}(N, \varprojlim_i M_i) = \{(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(N, M_i) \mid f_j = f_{ij} f_i \text{ para todo } i \leq j\}$$

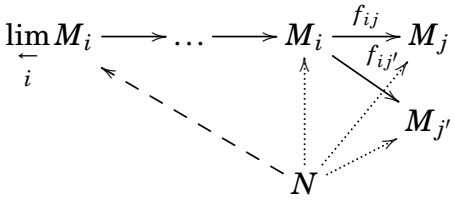
para todo objeto N de la categoría $\mathscr{C}$.

Si $\varprojlim_i M_i$ existe, entonces el morfismo $\mathrm{Id} \in \mathrm{Hom}_{\mathscr{C}}(\varprojlim_i M_i, \varprojlim_i M_i)$ define morfismos $\phi_i \colon \varprojlim_i M_i \to M_i$, de modo que

1. $\phi_j = f_{ij}\phi_i$
2. Dados $(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(N, M_i)$ tales que $f_j = f_{ij} f_i$, para todo $i \leq j$, entonces existe un único morfismo $f : N \to \varprojlim_i M_i$, de modo que $f_i = \phi_i f$, para todo objeto N.

Se tiene también el recíproco, si existe un objeto M, y morfismos $\phi_i \colon M \to M_i$, cumpliendo estas dos condiciones, entonces $M = \varprojlim_i M_i$.

Intuitivamente $\varprojlim_i M_i$ es "la fuente del río de flechas, la cota inferior máxima"



3. Teorema: *En la categoría de conjuntos los límites proyectivos existen, explícitamente*

$$\varprojlim_i M_i = \{(m_i) \in \prod_i M_i \mid f_{ij}(m_i) = m_j \text{ para todo } i \leq j\}$$

y $\phi_i \colon \varprojlim_i M_i \to M_i$, $\phi_i((m_j)) = m_i$.

Demostración. Denotemos $M = \{(m_i) \in \prod_i M_i \mid f_{ij}(m_i) = m_j \text{ para todo } i \leq j\}$. Obviamente, $\phi_j = f_{ij}\phi_i$ pues $\phi_j((m_k)) = m_j = f_{ij}(m_i) = f_{ij}\phi_i((m_k))$. Dado $\{(f_i) \in \prod_i \mathrm{Hom}(N, M_i) \mid$

$f_j = f_{ij}f_i$ para todo $i \leq j\}$, entonces $f : N \to M$, $f(n) := (f_i(n))$ es la única aplicación (bien definida) que cumple que $f_i = \phi_i f$. □

4. Teorema: *En la categoría de A-módulos los límites proyectivos existen, explícitamente*

$$\varprojlim_i M_i = \{(m_i) \in \prod_i M_i \mid f_{ij}(m_i) = m_j \text{ para todo } i \leq j\}$$

y $\phi_i : \varprojlim_i M_i \to M_i$, $\phi_i((m_j)) = m_i$.

Demostración. Repítase la demostración anterior. □

Dado un sistema proyectivo $\{M_i, f_{ij}\}_{i\in I}$ de objetos de una categoría $\mathscr{C}$ y un objeto $N \in \mathscr{C}$, entonces $\{\mathrm{Hom}_{\mathscr{C}}(N, M_i), f_{ij_*}\}_{i\in I}$ forma un sistema proyectivo de conjuntos.

5. Proposición: $\mathrm{Hom}_{\mathscr{C}}(N, \varprojlim_i M_i) = \varprojlim_i \mathrm{Hom}_{\mathscr{C}}(N, M_i)$

Demostración. Tenemos

$$\begin{aligned}\mathrm{Hom}_{\mathscr{C}}(N, \varprojlim_i M_i) &= \{(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(N, M_i) \mid f_j = f_{ij}f_i \text{ para todo } i \leq j\} \\ &= \varprojlim_i \mathrm{Hom}_{\mathscr{C}}(N, M_i)\end{aligned}$$

donde la primera igualdad es por la definición de límite proyectivo, y la segunda igualdad por la construcción del límite proyectivo de conjuntos. □

6. Definición: Un morfismo f entre dos sistemas proyectivos de objetos $\{M_i, f_{ij}\}$ y $\{N_i, g_{ij}\}$, con el mismo conjunto ordenado de índices, es una familia de morfismos $f_i : M_i \to N_i$ tales que $f_j f_{ij} = g_{ij} f_i$, cuando $i \leq j$.

Todo morfismo f entre dos sistemas proyectivos induce morfismos $\varprojlim_i M_i \to M_j \to N_j$, que induce un morfismo $\hat{f} : \varprojlim_i M_i \to \varprojlim_i N_i$. Explícitamente, en la categoría de conjuntos o de módulos, está definido por $\hat{f}((m_i)) := (f_i(m_i))$.

7. Definición: Diremos que una sucesión de morfismos de sistemas proyectivos de módulos $\{M'_i\} \to \{M_i\} \to \{M''_i\}$ es exacta, si lo es la sucesión $M'_i \to M_i \to M''_i$, para todo i.

8. Proposición: *La toma de límites proyectivos es exacta por la izquierda. Es decir, si* $0 \to \{M_i'\} \to \{M_i\} \to \{M_i''\}$ *son sucesiones exactas de sistemas proyectivos de A-módulos, entonces la sucesión de A-módulos*

$$0 \to \varprojlim_i M_i' \to \varprojlim_i M_i \to \varprojlim_i M_i''$$

es exacta

Demostración. Es una sencilla comprobación, conocida la construcción explícita de los límites proyectivos de módulos. □

9. Ejercicio: Sea $\{k[x]/(x^n)\}$ el sistema proyectivo de $k[x]$-módulos, cuyos morfismos $k[x]/(x^{n+1}) \to k[x](x^n)$ son los morfismos naturales de paso al cociente. Prueba que $\varprojlim_i k[x]/(x^n) = k[[x]]$.

Pasemos ahora a la definición del límite inductivo, que es el concepto dual de límite proyectivo.

Sea I un conjunto ordenado, diremos que es filtrante creciente si para cada par $i, j \in I$ existe algún $k \in I$ que cumple que $k \geq i$ y $k \geq j$.

10. Definición: Sea I un conjunto filtrante creciente. Un conjunto de objetos $\{M_i\}_{i \in I}$ de una categoría $\mathscr{C}$, junto con morfismos $f_{ij} \colon M_i \to M_j$, para cada $i \leq j$, diremos que es un sistema inductivo de objetos de $\mathscr{C}$ si satisface las siguientes condiciones

1. $f_{ii} = \mathrm{Id}$, para todo i.
2. $f_{jk} f_{ij} = f_{ik}$ siempre que $i \leq j \leq k$.

11. Definición: Sea $\{M_i\}_{i \in I}$ un sistema inductivo de objetos. Diremos que M (si existe) es el límite inductivo de este sistema inductivo, y lo denotaremos $\varinjlim_i M_i$, si cumple una igualdad funtorial

$$\mathrm{Hom}_{\mathscr{C}}(\varinjlim_i M_i, N) = \{(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(M_i, N) \mid f_i = f_j f_{ij} \text{ para todo } i \leq j\}$$

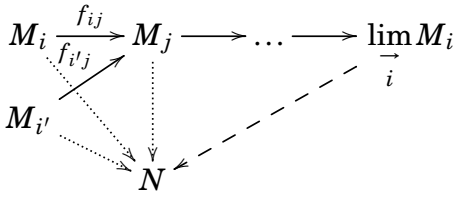
Si $\varinjlim_i M_i$ existe, entonces el morfismo $\mathrm{Id} \in \mathrm{Hom}_{\mathscr{C}}(\varinjlim_i M_i, \varinjlim_i M_i)$ define morfismos $\phi_i \colon M_i \to \varinjlim_i M_i$, de modo que

1. $\phi_i = \phi_j f_{ij}$

2. Dados $(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(M_i, N)$ tales que $f_i = f_j f_{ij}$ para todo $i \leq j$, entonces existe un único morfismo $f : \varinjlim_i M_i \to N$, de modo que $f_i = f\phi_i$, para todo objeto N.

Se tiene también el recíproco, si existe un objeto M, y morfismos $\phi_i : M_i \to M$, verificando estas dos condiciones, entonces $M = \varinjlim_i M_i$.

Intuitivamente $\varinjlim_i M_i$ es "la desembocadura del río de flechas, la cota superior mínima"



12. Teorema : *En la categoría de conjuntos los límites inductivos existen, explícitamente*

$$\varinjlim_i M_i = \{\coprod_i M_i/\sim : m_i \sim m_j \text{ si existe un índice } k \geq i, j \text{ de modo que } f_{ik}(m_i) = f_{jk}(m_j)\}$$

y $\phi_j : M_j \to \varinjlim_i M_i$, $\phi_j(m_j) = \bar{m}_j$.

Demostración. Se cumple que $\phi_j f_{ij} = \phi_i$, pues $\phi_j f_{ij}(m_i) = \overline{f_{ij}(m_i)} = \bar{m}_i = \phi_i(m_i)$. Denotemos $M = \coprod_i M_i/\sim$. Dado $\{(f_i) \in \prod_i \mathrm{Hom}(M_i, N) \mid f_i = f_j f_{ij}, \text{ para todo } i \leq j\}$, entonces la aplicación $f : M \to N$, $f(\bar{m}_i) := f_i(m_i)$ está bien definida y es la única que cumple que $f_i = f\phi_i$. □

13. Teorema : *En la categoría de A-módulos los límites inductivos existen, explícitamente*

$$\varinjlim_i M_i = \{\coprod_i M_i/\sim : m_i \sim m_j \text{ si existe un índice } k \text{ de modo que } f_{ik}(m_i) = f_{jk}(m_j)\}$$

y $\phi_j : M_j \to \varinjlim_i M_i$, $\phi_j(m_j) = \bar{m}_j$.

Demostración. Repítase la demostración anterior y pruébese que los conjuntos definidos son A-módulos y los morfismos de A-módulos. □

Dado un sistema inductivo $\{M_i, f_{ij}\}_{i\in I}$ de objetos de $\mathscr{C}$ y dado un objeto N de $\mathscr{C}$, entonces $\{\mathrm{Hom}_{\mathscr{C}}(M_i,N), {f_{ij}}^*\}_{i\in I}$ forma un sistema proyectivo de conjuntos.

14. Proposición: $\mathrm{Hom}_{\mathscr{C}}(\varinjlim_i M_i, N) = \varprojlim_i \mathrm{Hom}_{\mathscr{C}}(N, M_i)$

Demostración. Tenemos

$$\begin{aligned}\mathrm{Hom}_{\mathscr{C}}(\varinjlim_i M_i, N) &= \{(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(M_i,N) \mid f_i = f_j f_{ij} \text{ para todo } i \le j\} \\ &= \varprojlim_i \mathrm{Hom}_{\mathscr{C}}(M_i,N)\end{aligned}$$

donde la primera igualdad es por la definición de límite inductivo, y la segunda igualdad por la construcción del límite proyectivo de conjuntos. □

15. Definición: Un morfismo f entre dos sistemas inductivo de objetos $\{M_i, f_{ij}\}$ y $\{N_i, g_{ij}\}$, con el mismo conjunto ordenado de índices, es una familia de morfismos $f_i : M_i \to N_i$ tales que $f_j f_{ij} = g_{ij} f_i$, cuando $i \le j$.

Todo morfismo f entre dos sistemas inductivos de objetos induce, para cada j, morfismos $M_j \to N_j \to \varinjlim_i N_i$, que induce un morfismo $f : \varinjlim_i M_i \to \varinjlim_i N_i$, que explícitamente, en la categoría de conjuntos o de módulos, está definido por $f(\bar{m}_i) = \overline{f_i(m_i)}$.

16. Definición: Diremos que una sucesión de morfismos de sistemas inductivos de módulos $\{M'_i\} \to \{M_i\} \to \{M''_i\}$ es exacta, si lo es la sucesión $M'_i \to M_i \to M''_i$, para todo i.

17. Proposición: *La toma de límites inductivos es exacta. Es decir, si*

$$0 \to \{M'_i\} \xrightarrow{f_i} \{M_i\} \xrightarrow{g_i} \{M''_i\} \to 0$$

son sucesiones exactas de sistemas inductivos de A-módulos, entonces la sucesión de A-módulos

$$0 \to \varinjlim_i M'_i \xrightarrow{f} \varinjlim_i M_i \xrightarrow{g} \varinjlim_i M''_i \to 0$$

es exacta

Demostración. 1. $(gf)(\overline{m'}_i) = g(\overline{f_i(m'_i)}) = \overline{g_i(f_i(m'_i))} = 0.$

2. Si $g(\bar{m}_i) = 0$ entonces $\overline{g_i(m_i)} = 0$. Luego existe un k, de modo que $0 = f''_{ik}(g_i(m_i)) = g_k(f_{ik}(m_i))$. Por lo tanto, $f_{ik}(m_i) = f_k(m'_k)$, para cierto $m'_k \in M'_k$. Entonces, $\bar{m}_i = \overline{f_k(m'_k)} = f(\overline{m'}_k)$.

3. Obviamente g es epiyectiva: Dado $\overline{m''}_j \in \varinjlim M''_i$, entonces existe m_j tal que $g_j(m_j) = m''_j$ y $g(\bar{m}_j) = \overline{m''}_j$.

4. Por último, f es inyectiva: si $0 = f(\overline{m'}_i) = \overline{f_i(m'_i)}$ entonces existe un k, tal que $f_{ik}(f_i(m'_i)) = 0$. Por tanto, $f_k(f'_{ik}(m'_i)) = 0$ y $f'_{ik}(m'_i) = 0$, porque f_k es inyectiva. Luego $\overline{m'}_i = 0$.

□

18. Proposición: *El límite inductivo conmuta con el producto tensorial. Es decir,*

$$(\varinjlim M_i) \otimes_A N = \varinjlim (M_i \otimes_A N)$$

Demostración.

$$\begin{aligned}\mathrm{Hom}_A((\varinjlim M_i) \otimes_A N, R) &= \mathrm{Hom}_A(\varinjlim M_i, \mathrm{Hom}_A(N,R)) = \varprojlim \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(N,R)) \\ &= \varprojlim \mathrm{Hom}_A(M_i \otimes_A N, R) = \mathrm{Hom}_A(\varinjlim (M_i \otimes_A N), R)\end{aligned}$$

□

El límite inductivo de módulos planos es plano. En particular, el límite inductivo de módulos libres es plano. Queremos probar que todo módulo plano es límite inductivo de libres.

19. Proposición: *Todo módulo es límite inductivo de módulos de presentación finita.*

Demostración. Sea M un A-módulo. Consideremos un epimorfismo $\pi\colon \oplus_I A \to M$. Para cada subconjunto finito $J \subseteq I$ denotemos π_J la composición de los morfismos obvios $\oplus_J A \hookrightarrow \oplus_I A \to M$. Sea K el conjunto de parejas (J,N), donde J es un subconjunto finito de I y N es un submódulo finito generado de $\mathrm{Ker}\,\pi_J$. K es un conjunto ordenado filtrante como sigue: $(J,N) \leq (J',N')$ si $J \subseteq J'$ y $N \subseteq N'$. Dados (J,N), (J',N'), sea $J'' = J \cup J'$ y $N'' = N + N'$, entonces $(J,N),(J',N') \leq (J'',N'')$. Dejamos que el lector compruebe que $M = \varinjlim_{(J,N)\in K} (\oplus_J A)/N$. □

20. Lema : *Si M es un A-módulo plano y N es un A-módulo de presentación finita entonces el morfismo natural*

$$N^* \otimes_A M \to \mathrm{Hom}_A(N,M)$$

que asigna a $w \otimes m$ el morfismo $\overline{w \otimes m}$ definido por $\overline{w \otimes m}(n) := w(n) \cdot m$, es isomorfismo.

Demostración. Sea $L'' \to L' \to N \to 0$ una presentación por libres finito generados de N. Consideremos las sucesiones exactas

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(N,M) & \longrightarrow & \mathrm{Hom}_A(L',M) & \longrightarrow & \mathrm{Hom}_A(L'',M) \\ & & & & \| & & \| \\ 0 & \longrightarrow & N^* \otimes_A M & \longrightarrow & L'^* \otimes_A M & \longrightarrow & L''^* \otimes_A M \end{array}$$

Luego

$$\mathrm{Hom}_A(N,M) = N^* \otimes_A M.$$

□

21. Teorema : *Sea M un A-módulo plano. Dado un módulo N de presentación finita y un morfismo $i : N \to M$ existe un módulo libre finito generado L y un diagrama conmutativo*

$$\begin{array}{ccc} N & \xrightarrow{\varphi} & L \\ & \searrow^{i} & \downarrow \phi \\ & & M \end{array}$$

Demostración. Por el lema anterior, $N^* \otimes_A M = \mathrm{Hom}_A(N,M)$. Por tanto, existen $w_j \in N^*$ y $m_j \in M$, de modo que $i = \sum_{j=1}^{r} w_j \otimes m_j$. Sean $L = A^r$, $\varphi : N \to L$, $\varphi(n) = (w_j(n))_j$ y $\phi : L \to M$, $\phi((a_j)) = \sum_{j=1}^{r} a_j m_j$.

□

Ahora ya, es fácil probar el teorema de Lazard.

22. Teorema de Govorov-Lazard : *Un A-módulo es plano si y solo si es límite inductivo de módulos libres.*

Demostración. Sea M un módulo plano. Por la proposición 0.11.19, $M = \varinjlim_{i \in I} P_i$, con P_i módulos de presentación finita. Denotemos por $f_i : P_i \to M$ y $f_{ij} : P_i \to P_j$ los morfismos

obvios. Por el teorema 0.11.21, para cada P_i existe un módulo libre finito generado L_i y morfismos $g_i : P_i \to L_i$, $h_i : L_i \to M$ de modo que $h_i \circ g_i = f_i$. Como $\mathrm{Hom}_A(L_i, M) = \varinjlim_j \mathrm{Hom}_A(L_i, P_j)$, existe $\phi(i) > i$ y un morfismo $t_i : L_i \to P_{\phi(i)}$ tal que $h_i = f_{\phi(i)} \circ t_i$. Tomando $\phi(i)$ mayor si es necesario, podemos suponer que $t_i \circ g_i = f_{i\phi(i)}$. Sea $(I', \leq')$ el conjunto ordenado definido por $I' = I$ y $i <' j$ si $\phi(i) < j$; y definimos $f'_{ij} = t_j \circ f_{\phi(i)j} \circ t_i$. Dejamos que el lector compruebe que $M = \varinjlim_{i \in I'} L_i$. □

23. Corolario: *Un A-módulo M es plano si y solo si para todo A-módulo de presentación finita N el morfismo natural*

$$N^* \otimes_A M \to \mathrm{Hom}_A(N, M)$$

que asigna a $w \otimes m$ el morfismo $\overline{w \otimes m}$ definido por $\overline{w \otimes m}(n) := w(n) \cdot m$, es epiyectivo (o es isomorfismo).

Demostración. Si M cumple que el morfismo $N^* \otimes_A M \to \mathrm{Hom}_A(N, M)$ es epiyectivo para todo módulo N de presentación finita, entonces el teorema 0.11.21 se cumple (sin la hipótesis de M plano). Entonces como en el teorema de Govorov-Lazard se cumple que M es límite inductivo de módulos libres, luego M es un A-módulo plano. El recíproco es consecuencia del lema 0.11.20. □

0.12. Módulos inyectivos

1. Definición: Diremos que un A-módulo M es inyectivo si el funtor contravariante $\mathrm{Hom}_A(-, M)$ es exacto en la categoría de A-módulos; es decir, si transforma inyecciones en epimorfismos.

Se cumplen trivialmente las siguientes propiedades:

a) El producto directo de módulos inyectivos es inyectivo.

b) Un sumando directo de un módulo inyectivo es también inyectivo.

c) Si M es un módulo inyectivo y M es un submódulo de N, entonces M es un sumando directo de N.

2. Ejemplos: Los k-espacios vectoriales son k-módulos inyectivos.

Si A es un anillo íntegro, $S = A\backslash\{0\}$ y $\Sigma = A_S$. Si M es un Σ-espacio vectorial, entonces M es un A-módulo inyectivo. En efecto,

$$\mathrm{Hom}_A(N,M) = \mathrm{Hom}_\Sigma(N_S,M)$$

y los funtores localizar por S y $\mathrm{Hom}_\Sigma(-,M)$ son exactos. Por tanto, el funtor $\mathrm{Hom}_A(-,M)$ es exacto y M es un A-módulo inyectivo

3. Criterio de inyectividad del ideal: *Un A-módulo M es inyectivo si y solo si para todo ideal $I \subset A$ el morfismo* $\mathrm{Hom}_A(A,M) \to \mathrm{Hom}_A(I,M)$ *es epiyectivo.*

Demostración. Basta ver el recíproco. Dada una inclusión $N' \hookrightarrow N$ y un morfismo $f' : N' \to M$ tenemos que demostrar que f extiende a un morfismo $f : N \to M$. Sea N'' un submodulo de N que contiene a N' y maximal con la condición de que exista una extensión $f'' : N'' \to M$ de f'. La existencia de N'' se debe al lema de Zorn. Tenemos que probar que $N'' = N$. Sea $n \in N$ e $I = \{a \in A : a \cdot n \in N''\}$. Tenemos definido un morfismo $g : I \to M, a \mapsto f''(a \cdot n)$, que por hipótesis extiende a un morfismo $g' : A \to M$. El morfismo $\langle n\rangle \to M, a \cdot n \mapsto g'(a)$ está bien definido, coincide con f'' sobre $\langle n\rangle \cap N'' = I \cdot n$, luego define un morfismo $f''' : N'' + \langle n\rangle \to M, n'' + an \mapsto f''(n'') + g'(a)$. Por maximalidad de N'' ha de cumplirse que $n \in N''$, luego $N'' = N$. □

4. Ejemplo: Sea $n \in \mathbb{N}$ no nulo. Probemos que $\mathbb{Z}/n\mathbb{Z}$ es un $\mathbb{Z}/n\mathbb{Z}$-módulo inyectivo: Sea $I \subset \mathbb{Z}/n\mathbb{Z}$ un ideal, entonces $I = (\bar{m})$. Observemos que $(\bar{m}) = (\bar{m}, \bar{n}) = (\overline{m.c.d.(m,n)})$. Podemos suponer que m divide a n y escribamos $n = r \cdot m$. Sea $\phi : (\bar{m}) \to \mathbb{Z}/n\mathbb{Z}$ un morfismo de $\mathbb{Z}/n\mathbb{Z}$-módulos. Escribamos, $\phi(\bar{m}) = \bar{s}$. Entonces,

$$\overline{r \cdot s} = \bar{r} \cdot \bar{s} = \bar{r} \cdot \phi(\bar{m}) = \phi(\overline{rm}) = 0$$

Luego $r \cdot s$ es múltiplo de $n = r \cdot m$ y $s = t \cdot m$. Por tanto, $\phi : (\bar{m}) \to \mathbb{Z}/n\mathbb{Z}$ extiende al morfismo $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \mapsto t \cdot \bar{a}$.

Sea ahora G un grupo abeliano, o lo que es lo mismo un $\mathbb{Z}$-módulo. Supongamos que $|G| < \infty$. Sea $n \in \mathbb{N}$ mínimo tal que $n \cdot g = 0$, para todo $g \in G$. Escribamos, $n = p_1^{n_1} \cdots p_r^{n_r}$ como producto de potencias de primos distintos. Dado m denotemos $\mathrm{Ker}\, m\cdot = \{g \in G : m \cdot g = 0\}$. Entonces,

$$G = \mathrm{Ker}\, n\cdot = \mathrm{Ker}\, p_1^{n_1} \cdot \oplus \cdots \oplus \mathrm{Ker}\, p_r^{n_r} \cdot .$$

Existe $g_i \in \mathrm{Ker}\, p_i^{n_i}\cdot$ tal que $p_i^{n_i-1} \cdot g_i \neq 0$, porque si no $m = \frac{n}{p_i}$ cumplirá que $m \cdot g = 0$ para todo $g \in G$. Sea $g = (g_1, \ldots, g_r)$, entonces n es el mínimo número natural tal que $n \cdot g = 0$, es decir, $\langle g\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Como G es un $\mathbb{Z}/n\mathbb{Z}$-módulo, $\mathbb{Z}/n\mathbb{Z}$ es un $\mathbb{Z}/n\mathbb{Z}$-módulo inyectivo y $\mathbb{Z}/n\mathbb{Z} \simeq \langle g\rangle \subset G$, tenemos que $G \simeq \mathbb{Z}/n\mathbb{Z} \oplus G'$. Recurrentemente obtendremos que todo grupo abeliano finito G es suma directa de grupos cíclicos.

5. Lema: *Sea P un A-módulo de presentación finita y $\{M_i\}$ un sistema inductivo de A-módulos. Entonces,*

$$\mathrm{Hom}_A(P, \varinjlim M_i) = \varinjlim \mathrm{Hom}_A(P, M_i).$$

Demostración. Existe un morfismo natural $\varinjlim \mathrm{Hom}_A(P, M_i) \to \mathrm{Hom}_A(P, \varinjlim M_i)$. Si P es un A-módulo libre finito generado, es claro que es un isomorfismo. Consideremos una presentación $L \to L' \to P$ de P por módulos libres finito generados. Como $\mathrm{Hom}_A(\ , M_i)$ es un funtor exacto por la izquierda y $\varinjlim$ es exacto, tenemos la sucesiones exactas

$$0 \to \varinjlim \mathrm{Hom}_A(P, M_i) \to \varinjlim \mathrm{Hom}_A(L', M_i) \to \varinjlim \mathrm{Hom}_A(L', M_i)$$

$$0 \to \mathrm{Hom}_A(P, \varinjlim M_i) \to \mathrm{Hom}_A(L', \varinjlim M_i) \to \mathrm{Hom}_A(L, \varinjlim M_i)$$

Como $\varinjlim \mathrm{Hom}_A(L, M_i) = \mathrm{Hom}_A(L, \varinjlim M_i)$ y $\varinjlim \mathrm{Hom}_A(L', M_i) = \mathrm{Hom}_A(L', \varinjlim M_i)$, concluimos que $\varinjlim \mathrm{Hom}_A(P, M_i) = \mathrm{Hom}_A(P, \varinjlim M_i)$. □

6. Proposición: *El límite inductivo de A-módulos inyectivos es inyectivo, cuando el anillo A es noetheriano.*

Demostración. Sea $\{M_i\}$ un sistema inductivo de módulos inyectivos y sea $\mathfrak{a} \subset A$ un ideal. Entonces, el morfismo

$$\mathrm{Hom}_A(A, \varinjlim_i M_i) \overset{0.12.5}{=} \varinjlim_i \mathrm{Hom}_A(A, M_i) \to \varinjlim_i \mathrm{Hom}_A(\mathfrak{a}, M_i) \overset{0.12.5}{=} \mathrm{Hom}_A(\mathfrak{a}, \varinjlim_i M_i)$$

es epiyectivo y por el criterio del ideal $\varinjlim_i M_i$ es inyectivo.

□

7. Definición: Sea A un dominio de integridad. Un A-módulo M se dice de división si para todo $a \in A$ no nulo, el morfismo $M \xrightarrow{a\cdot} M$, $m \mapsto a \cdot m$ es epiyectivo.

8. Teorema: *Sea A íntegro. Todo módulo inyectivo es de división. Si A es un dominio de ideales principales, entonces un módulo es inyectivo precisamente si es de división.*

Demostración. Tómese la sucesión exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & aA & \hookrightarrow & A & \longrightarrow & A/aA & \longrightarrow & 0 \\ & & \downarrow \wr & & \| & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{\cdot a} & A & \longrightarrow & A/aA & \longrightarrow & 0 \end{array}$$

y $\mathrm{Hom}_A(\ , M)$.

□

9. Ejemplos: Como $\mathbb{Q}/\mathbb{Z}$ es un $\mathbb{Z}$-módulo de división, entonces es un $\mathbb{Z}$-módulo inyectivo.

Sea p un número primo y sea $[\mathbb{Q}/\mathbb{Z}](p) := \{[\frac{a}{p^n}] \in \mathbb{Q}/\mathbb{Z} \colon \forall\, a \in \mathbb{Z}, \forall n \in \mathbb{N}\}$. Sea $M = \{[\frac{a}{m}] \in \mathbb{Q}/\mathbb{Z} \colon \forall\, a \in \mathbb{Z}, \forall m \in \mathbb{N}\backslash\{0\}$ primo con $p\}$. Dejamos que el lector compruebe que $[\mathbb{Q}/\mathbb{Z}] = [\mathbb{Q}/\mathbb{Z}](p) \oplus M$, luego $[\mathbb{Q}/\mathbb{Z}](p)$ es inyectivo.

Consideremos los morfismos inyectivos $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $[a] \mapsto [\frac{a}{p^n}]$ y los morfismos inyectivos $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n+m}\mathbb{Z}$, $[a] \mapsto [p^m \cdot a]$. Es fácil comprobar que $\varinjlim_n \mathbb{Z}/p^n\mathbb{Z} = [\mathbb{Q}/\mathbb{Z}](p)$.

Denotemos por $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, para cada $\mathbb{Z}$-módulo (o grupo abeliano) M.

10. Lema: *El morfismo natural $M \to M^{**}$ es inyectivo.*

Demostración. Tenemos que ver que dado $0 \neq m \in M$ existe $w \in M^*$ tal que $w(m) \neq 0$. Sea (n) el ideal anulador de $\langle m \rangle$. Si $n = 0$, sea $w' \colon \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$ el morfismo definido por $w'(r \cdot m) = [\frac{r}{2}]$, y si $n \neq 0$, sea $w' \colon \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$ el morfismo definido por $w'(r \cdot m) = [\frac{r}{n}]$. Como $\mathbb{Q}/\mathbb{Z}$ es inyectivo, existe un morfismo $w \colon M \to \mathbb{Q}/\mathbb{Z}$ que coincide con w' sobre $\langle m \rangle$. Entonces, $w(m) = w'(m) \neq 0$.

□

El funtor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ sobre la categoría de A-módulos es exacto y transforma límites inductivos en límites proyectivos, luego por el teorema de representabilidad es representable de representante

$$A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^{6}$$

que ha de ser un A-módulo inyectivo.

11. Teorema: *Todo módulo es submódulo de un inyectivo. En lenguaje categorial: la categoría de A-módulos tiene suficientes inyectivos.*

Demostración. Consideremos un epimorfismo $\oplus A \to M^*$. Tenemos por tanto una inyección $M^{**} \hookrightarrow \prod A^*$. El producto directo de inyectivos es inyectivo, luego $\prod A^*$ es un A-módulo inyectivo. Por último, por la proposición anterior, $M \hookrightarrow M^{**} \hookrightarrow \prod A^*$ y hemos concluido. □

[6] De otro modo: $\mathrm{Hom}_A(N, A^*) = \mathrm{Hom}_A(N, \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_{\mathbb{Z}}(N \otimes_A A, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$.

0.12.1. Estructura de los módulos inyectivos

12. Definición: Diremos que un morfismo inyectivo de A-módulos $N \hookrightarrow M$ es una extensión esencial si y solo si para todo $0 \neq N' \subset M$ se cumple que $N' \cap N \neq 0$.

13. Ejemplos: Sea A un anillo íntegro, $\Sigma = A_{A\setminus 0}$ e $I \subset A$ un ideal no nulo. Entonces, las inyecciones $A \hookrightarrow \Sigma_A$ e $I \hookrightarrow A$ son esenciales.

14. Proposición: *La composición de extensiones esenciales es esencial. El límite inductivo de extensiones esenciales es esencial.*

Demostración. Sean $N_1 \hookrightarrow N_2$, $N_2 \hookrightarrow N_3$ dos extensiones esenciales y $M \subset N_3$ un submódulo no nulo. Entonces, $M \cap N_2$ es un submódulo no nulo de N_2, luego $M \cap N_1 = M \cap N_2 \cap N_1$ es un submódulo no nulo de M_1. Por tanto, $N \hookrightarrow N_3$ es esencial.

Sea $\{N_i, f_{ij}\}$ un sistema inductivo de extensiones esenciales de N (con $f_{ij|N} = \mathrm{Id}$, para todo $i \leq j$). Para todo morfismo de A-módulos $f: P \to Q$ y submódulo $R \subseteq Q$, denotemos $P \cap R := f^{-1}(R)$. Dado un submódulo $M \hookrightarrow \varinjlim_i N_i$, existe un índice i tal que $N_i \cap M \neq 0$, luego $N \cap M = N \cap (N_i \cap M)$ es no nulo. Por tanto, la inyección $N \hookrightarrow \varinjlim_i N_i$ es esencial.

□

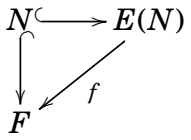
15. Proposición: *Dado un A-módulo N, existe un módulo inyectivo I que lo contiene de modo que la inclusión $N \hookrightarrow I$ es esencial. Además, éste coincide con el módulo inyectivo mínimo que contiene a N y con la extensión esencial máxima de N.*

Demostración. Sea $N \hookrightarrow M$ una inyección de N en un A-módulo inyectivo. Sea $E(N)$ una extensión esencial de N contenida en M máxima (que existe por Zorn). Sea N' un submódulo máximo de M con la condición de que $E(N) \cap N' = 0$. Se cumple que el morfismo $E(N) \xrightarrow{e} M/N'$, $r \mapsto \bar{r}$ es inyectivo y que e es una extensión esencial (por la maximalidad de N'). Por ser M un módulo inyectivo existe un diagrama conmutativo de morfismos de módulos

$$\begin{array}{ccc} E(N) & \xrightarrow{e} & M/N' \\ \downarrow & \swarrow_{f} & \\ M & & \end{array}$$

donde f ha de ser inyectivo, por ser e esencial. Por la maximalidad de $E(N)$ se ha de cumplir que $E(N) = M/N'$. En conclusión, $E(N) \oplus N' = M$. Por tanto, $E(N)$ es inyectivo y

$N \hookrightarrow E(N)$ es esencial. Dado cualquier módulo inyectivo F que contenga a N, tenemos de nuevo un diagrama



con f inyectivo. Concluimos que $E(N)$ es el módulo inyectivo mínimo que contiene a N. Dejamos que el lector pruebe que $E(N)$ es la extensión esencial máxima que contiene a N. □

16. Definición: Dado un A-módulo N, llamaremos envolvente inyectiva de N al mínimo A-módulo inyectivo que lo contiene. Lo denotaremos $E(N)$.

17. Ejemplos: $\mathbb{Q}$ es la envolvente inyectiva del $\mathbb{Z}$-módulo $\mathbb{Z}$, ya que es un $\mathbb{Z}$-módulo inyectivo y la inyección $\mathbb{Z} \hookrightarrow \mathbb{Q}$ es esencial.

$\varinjlim_n \mathbb{Z}/p^n\mathbb{Z}$ es la envolvente inyectiva del $\mathbb{Z}$-módulo $\mathbb{Z}/p\mathbb{Z}$, porque es inyectivo y los morfismos inyectivos $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^n\mathbb{Z}$, $\bar{a} \mapsto p^{n-1} \cdot \bar{a}$ son esenciales (pruébese).

18. Definición: Diremos que un módulo es indescomponible si no contiene dos submódulos no triviales en suma directa, es decir, si el cero es irreducible.

19. Teorema: *Todo módulo inyectivo E es suma directa de módulos inyectivos indescomponibles.*

Demostración. Sea $\mathscr{F}$ el conjunto de familias de submódulos inyectivos indescomponibles de E que están en suma directa en E. La relación de orden en $\mathscr{F}$ es la inclusión de familias. Por el lema de Zorn existe una familia F' maximal. Entonces $\bigoplus_{F_i \in F'} F_i \subset E$ y es inyectivo, luego $E = (\bigoplus_{F_i \in F'} F_i) \oplus E'$. Si $E' \neq 0$, E' contiene submódulos inyectivos indescomponibles y por la maximalidad de F' llegamos a contradicción. Luego, $E = \bigoplus_{F_i \in F'} F_i$. □

Observemos que los módulos indescomponibles inyectivos son la envolvente inyectiva de cualquiera de sus submódulos no nulos. Observemos que toda extensión esencial de un A-módulo indescomponible es indescomponible.

20. Proposición: *Para todo $x \in \operatorname{Spec} A$, $E(A/\mathfrak{p}_x)$ es indescomponible.*

Demostración. Solo tenemos que probar que $A/\mathfrak{p}$ es indescomponible. Dados dos submódulos (ideales) I, J de $A/\mathfrak{p}$ se cumple que $0 \neq I \cdot J \subseteq I \cap J$, luego es indescomponible. □

21. Proposición: *Si $x, y \in \operatorname{Spec} A$ son distintos, entonces $E(A/\mathfrak{p}_x) \neq E(A/\mathfrak{p}_y)$.*

Demostración. Si $E(A/\mathfrak{p}_x) = E(A/\mathfrak{p}_y)$, entonces tendríamos dos submódulos $A/\mathfrak{p}_x, A/\mathfrak{p}_y$ de $E(A/\mathfrak{p}_x)$ que están en suma directa porque los elementos no nulos de $A/\mathfrak{p}_x$ están anulados precisamente por $\mathfrak{p}_x$ y los de $A/\mathfrak{p}_y$ por $\mathfrak{p}_y$. Pero $E(A/\mathfrak{p}_x)$ es indescomponible, contradicción.

□

22. Proposición: *Sea $x \in \operatorname{Spec} A$. Entonces, $E(A/\mathfrak{p}_x)$ es un A_x-módulo.*

Demostración. Sea $s \in A - \mathfrak{p}_x$ y consideremos el diagrama

$$\begin{array}{ccc} A/\mathfrak{p}_x & \xrightarrow{s\cdot} & A/\mathfrak{p}_x \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ E(A/\mathfrak{p}_x) & \xrightarrow{s\cdot} & E(A/\mathfrak{p}_x) \end{array}$$

Observemos que $s\cdot$ ha de ser inyectivo en $E(A/\mathfrak{p}_x)$, porque lo es en $A/\mathfrak{p}_x$ e i es esencial. Además $s\cdot$ es epiyectivo en $E(A/\mathfrak{p}_x)$, porque $E(A/\mathfrak{p}_x)$ es indescomponible. Por tanto $s\cdot$ es un isomorfismo en $E(A/\mathfrak{p}_x)$ y $E(A/\mathfrak{p}_x)$ es un A_x-módulo.

□

23. Proposición: *Sea $E = \overset{N_x}{\oplus} E(A/\mathfrak{p}_x) \oplus \oplus_i E_i$, una descomposición en suma directa de indescomponibles, de modo que los $E_i \neq E(A/\mathfrak{p}_x)$. Entonces,*

$$\dim_{k(x)} \operatorname{Hom}_A(k(x), E) = N_x.$$

Demostración. Si $f\colon k(x) \to E_i$ es un morfismo de A-módulos no nulo, sea $f(k)$ no nulo. Si existe $s_1 \notin \mathfrak{p}_x$ tal que $s_1 \cdot f(k) = 0$, sea $s_2 \notin \mathfrak{p}_x$, tal que el morfismo $k(x) \to k(x)$, $\lambda \mapsto s_1 s_2 \lambda$ sea la identidad. Entonces, $f(k) = f(s_1 s_2 k) = s_1 s_2 f(k) = 0$ y llegamos a contradicción. Por tanto, $\langle f(k) \rangle \simeq A/\mathfrak{p}_x$ y $E_i \simeq E(A/\mathfrak{p}_x)$ y llegamos a contradicción con que f es no nulo.

Sea $T = \{e \in E(A/\mathfrak{p}_x)\colon \mathfrak{p}_x \cdot e = 0\}$. T es un $k(x)$-módulo porque $T_x \subset E(A/\mathfrak{p}_x)_x = E(A/\mathfrak{p}_x)$, T_x es un $k(x)$-módulo y $T = T_x$. Entonces, como $E(A/\mathfrak{p}_x)$ es indescomponible, se tiene que $T \simeq k(x)$. Por tanto,

$$\operatorname{Hom}_A(k(x), E(A/\mathfrak{p}_x)) = \operatorname{Hom}_A(k(x), T) = \operatorname{Hom}_A(k(x), k(x)) = \operatorname{Hom}_A(A/\mathfrak{p}_x, k(x)) \simeq k(x).$$

Además, todo morfismo $f\colon k(x) \to E(A/\mathfrak{p}_x)$, está determinado por $f(\bar{1})$. Por tanto,

$$\operatorname{Hom}_A(k(x), \overset{N_x}{\oplus} E(A/\mathfrak{p}_x)) \simeq \overset{N_x}{\oplus} k(x).$$

Con todo es fácil concluir.

□

A partir de ahora, en esta subsección, supondremos que A **es noetheriano**.

24. Proposición: *Un A-módulo inyectivo E es indescomponible si y solo si $E = E(A/\mathfrak{p})$ para algún primo $\mathfrak{p} \in \operatorname{Spec} A$.*

Demostración. Veamos el directo. En E, como en todo módulo no nulo, existe un elemento $e \in E$ tal que $A/\mathfrak{p} = \langle e \rangle \subset E$. Tenemos entonces una inyección $E(A/\mathfrak{p}) \subset E$. Luego $E = E(A/\mathfrak{p}) \oplus E'$, pero por ser E indescomponible tendremos que $E = E(A/\mathfrak{p})$. □

25. Proposición: *Sea $x \in \operatorname{Spec} A$ y $e \in E(A/\mathfrak{p}_x)$ no nulo. El ideal anulador de e es un ideal $\mathfrak{p}_x$-primario.*

Demostración. Dado $e \in E(A/\mathfrak{p}_x)$ no nulo, sea $\mathfrak{q}$ un ideal primo asociado a la descomposición primaria de $Anul(e)$. Tendremos una inclusión $A/\mathfrak{q} \subset A/Anul(e) = \langle e \rangle \subset E(A/\mathfrak{p}_x)$. Luego $E(A/\mathfrak{q}) = E(A/\mathfrak{p}_x)$ y por tanto $\mathfrak{q} = \mathfrak{p}_x$. Es decir, $\operatorname{Rad}(Anul(e)) = \mathfrak{p}_x$ y concluimos. □

26. Corolario: $E(A/\mathfrak{p}_x)_y = \begin{cases} E(A/\mathfrak{p}_x) \text{ si } y \in \bar{x} \\ 0 \quad \text{si } y \notin \bar{x} \end{cases}$

Demostración. Es consecuencia de 0.12.25. □

27. Ejemplo: Consideremos en $k[[x^{-1}, y^{-1}]]$ la estructura de $k[x,y]$-módulo siguiente: $(x^r \cdot y^s) \cdot (x^{-n} \cdot y^{-m}) = x^{r-n} y^{s-m}$ si $r - n \leq 0$ y $s - m \leq 0$ o cero en caso contrario. El morfismo k-lineal

$$k[[x^{-1}, y^{-1}]] \to \operatorname{Hom}_k(k[x,y], k),\ x^{-\alpha} \mapsto \delta_\alpha, \quad \text{donde } \delta_\alpha(x^\beta) := \begin{cases} 1 \text{ si } \alpha = \beta. \\ 0 \text{ si } \alpha \neq \beta \end{cases}$$

es un isomorfismo de $k[x,y]$-módulos. Por tanto, para todo $k[x,y]$-módulo

$$\begin{aligned} \operatorname{Hom}_k(M,k) &= \operatorname{Hom}_k(M \otimes_{k[x,y]} k[x,y], k) = \operatorname{Hom}_{k[x,y]}(M, \operatorname{Hom}_k(k[x,y], k)) \\ &= \operatorname{Hom}_{k[x,y]}(M, k[[x^{-1}, y^{-1}]]) \end{aligned}$$

y $k[[x^{-1}, y^{-1}]]$ es un $k[x,y]$-módulo inyectivo. Observemos que $k[x^{-1}, y^{-1}] \hookrightarrow k[[x^{-1}, y^{-1}]]$ es el $k[x,y]$-submódulo de $k[[x^{-1}, y^{-1}]]$ formado por los elementos que están anulados por alguna potencia $(x,y)^n$. Por tanto, en la descomposición de $k[[x^{-1}, y^{-1}]]$ como suma directa de idescomponibles, $k[x^{-1}, y^{-1}]$ es la suma directa de los idescomponibles isomorfos a $E(k[x,y]/(x,y)))$

El morfismo $k[x,y]/(x,y)) = k \hookrightarrow k[x^{-1}, y^{-1}]$ es esencial. Por tanto, $k[x^{-1}, y^{-1}] = E(k[x,y]/(x,y)))$.

Integrabilidad de los sistemas de ecuaciones en derivadas parciales con coeficientes constantes:

El objetivo de esta subsección es dar las condiciones necesarias y suficientes para que el sistema de ecuaciones diferenciales en derivadas parciales con coeficientes constantes

$$P_i(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})v(x_1,\dots,x_n) = u_i(x_1,\dots,x_n),\ \ i=1,\dots,m \qquad (*)$$

con $P_i(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$ y $u_i(x_1,\dots,x_n) \in k[[x_1,\dots,x_n]]$, sea integrable, es decir, exista $v(x_1,\dots,x_n) \in k[[x_1,\dots,x_n]]$ verificando el sistema anterior.

Si consideramos una sucesión exacta

$$k[[x_1,\dots,x_n]] \overset{\oplus_i P_i(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})}{\longrightarrow} \bigoplus_{i=1}^{m} k[[x_1,\dots,x_n]] \overset{\phi}{\to} L'$$

la existencia de una solución $v(x_1,\dots,x_n)$ del sistema de ecuaciones anterior, equivale a decir que $\phi(u_1,\dots,u_m) = 0$. Vamos a ver que se puede obtener esta sucesión exacta como dual de otra bien conocida.

Supondremos que el cuerpo es de característica cero.

28. Consideremos $k[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$ como el anillo obvio, isomorfo a $k[x_1,\dots,x_n]$. Consideremos $k[[x_1,\dots,x_n]]$ como $k[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$-módulo del modo obvio:

$$P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})\cdot v(x_1,\dots,x_n) = P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})(v(x_1,\dots,x_n))$$

El morfismo

$$k[[x_1,\dots,x_n]] \overset{\phi}{\to} \mathrm{Hom}_k(k[x_1,\dots,x_n],k)$$

definido por

$$\phi(s(x_1,\dots,x_n))(P(x_1,\dots,x_n)) := (P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})s(x_1,\dots,x_n))(0,\dots,0)$$

es un isomorfismo de $k[x_1,\dots,x_n]$-módulos. Por lo tanto,

$$\begin{aligned}\mathrm{Hom}_{k[x_1,\dots,x_n]}(M,k[[x_1,\dots,x_n]]) &= \mathrm{Hom}_{k[x_1,\dots,x_n]}(M,\mathrm{Hom}_k(k[x_1,\dots,x_n],k))\\ &= \mathrm{Hom}_k(M\otimes_{k[x_1,\dots,x_n]} k[x_1,\dots,x_n],k)) = \mathrm{Hom}_k(M,k))\end{aligned}$$

y $k[[x_1,\dots,x_n]]$ es un $k[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$-módulo inyectivo.

Sea (p_{ij}) una matriz de polinomios tal que la sucesión

$$\overset{r}{\oplus}k[x_1,\ldots,x_n] \overset{(p_{ij})}{\longrightarrow} \overset{m}{\oplus}k[x_1,\ldots,x_n] \overset{\sum P_i\cdot}{\longrightarrow} k[x_1,\ldots,x_n] \to k[x_1,\ldots,x_n]/(P_1,\ldots,P_m) \to 0$$

sea exacta. Aplicando el funtor $\mathrm{Hom}_k(-,k) = \mathrm{Hom}_{k[x_1,\ldots,x_n]}(-,k[[x_1,\ldots,x_n]])$ obtenemos la sucesión exacta

$$0 \hookrightarrow (k[x_1,\ldots,x_n]/(P_1,\ldots,P_m))^* \to$$
$$k[[x_1,\ldots,x_n]] \overset{\oplus P_i(\frac{\partial}{\partial x_1},\ldots,\frac{\partial}{\partial x_n})}{\longrightarrow} \overset{m}{\oplus}k[[x_1,\ldots,x_n]] \overset{(p_{ij}(\frac{\partial}{\partial x_1},\ldots,\frac{\partial}{\partial x_n}))^t}{\longrightarrow} \overset{m}{\oplus}k[[x_1,\ldots,x_n]]$$

29. Teorema : *El sistema de ecuaciones diferenciales en derivadas parciales* $(*)$ *es integrable si y sólo si*

$$(p_{ij}(\frac{\partial}{\partial x_1},\ldots,\frac{\partial}{\partial x_n}))^t(u_1,\ldots,u_n) = 0.$$

Además, la dimensión del espacio de soluciones es $\dim_k(k[x_1,\ldots,x_n]/(P_1,\ldots,P_m))$.

0.13. Teorema de representabilidad

Hemos probado que un módulo queda caracterizado si se conocen sus "relaciones con los demás", es decir, si se conocen sus morfismos en los demás módulos, o los morfismos de los demás módulos en él. Con la terminología del funtor de puntos: los objetos quedan determinados por sus puntos.

Hemos definido los módulos proyectivos, límites inductivos, límites proyectivos, etc., caracterizando sus relaciones con los demás objetos, es decir, vía sus propiedades universales. Hemos probado que el producto tensorial de dos módulos cumple la propiedad universal de representar a las aplicaciones bilineales. Sorprendentemente, veremos que esta propiedad implica la existencia del producto tensorial. Este es un principio general en Matemáticas, expresado en "el teorema de representabilidad", que nos permitirá construir objetos (en nuestro caso, módulos) no dando sus elementos, sino sus morfismos con los demás objetos.

Diremos que dos monomorfismos $f : N \to M$ y $f' : N' \to M$ son equivalentes si existe un isomorfismo $h : N \to N'$ tal que $f = f' \circ h$. La clase de equivalencia de un momorfismo $f : N \to M$ se le denomina subobjeto.

1. Definición : Se dice que un objeto A de una categoría $\mathscr{C}$ es un generador si para cada objeto M y par de subobjetos distintos $N, N' \hookrightarrow M$, existe un morfismo $A \to M$ que factoriza a través de N pero no factoriza a través de N'.

Si en una categoría hay un generador A, la familia de los subobjetos de un objeto es un conjunto. En efecto, la asignación

$$\{\text{Subobjetos de } M\} \to \{\text{Subconjuntos de } \mathrm{Hom}_{\mathscr{C}}(A,M)\},\ N \mapsto \mathrm{Hom}_{\mathscr{C}}(A,N)$$

es inyectiva. Por tanto, en una categoría abeliana con un generador la familia de cocientes de un objeto forman un conjunto.

Sea $\mathscr{C}$ una categoría abeliana con sumas directas infinitas y con un generador A. Dado un objeto M, el morfismo natural $\pi\colon \underset{\mathrm{Hom}_{\mathscr{C}}(A,M)}{\oplus} A \to M$ es un epimorfismo. De nuevo, existe un epimorfismo $\underset{I}{\oplus} A \to \mathrm{Ker}\,\pi$ y hemos obtenido una sucesión exacta

$$\underset{I}{\oplus} A \to \underset{J}{\oplus} A \to M \to 0$$

El concepto dual de generador es el de cogenerador.

2. Ejemplo: Un generador de la categoría de A-módulos es A. Un cogenerador de esta categoría es el A-módulo inyectivo $A^* := \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ (véase 0.12.11).

3. Notaciones: A partir de ahora, en esta sección, todas las categorías consideradas serán abelianas y todos los funtores serán contravariantes y aditivos y valorarán en la categoría de grupos abelianos, $\mathscr{C}_{gr}$. Dado un funtor F y un objeto M, sabemos que $\mathrm{Hom}(M^{\cdot}, F) = F(M)$. Vía esta igualdad, $\phi \in F(M)$ se corresponderá (por notación) con $\phi^{\cdot} \in \mathrm{Hom}(M^{\cdot}, F)$ (que cumple $\phi^{\cdot}_{M}(\mathrm{Id}_M) = \phi$). En particular, $\phi \in M^{\cdot}(N) = \mathrm{Hom}(N, M)$ se corresponde con $\phi^{\cdot}\colon N^{\cdot} \to M^{\cdot}$.

4. Lema: *Sean $F, F'\colon \mathscr{C} \to \mathscr{C}_{gr}$ dos funtores contravariantes aditivos y*

$$f\colon F \to F'$$

un morfismo de funtores de grupos. Entonces,

$$(\mathrm{Ker}\, f)(N) = \{\phi \in F(N)\colon f_N(\phi) = 0\} = \{\phi^{\cdot} \in \mathrm{Hom}_{\mathscr{C}}(N^{\cdot}, F)\colon f \circ \phi^{\cdot} = 0\}.$$

.

5. Lema: *Un funtor $F\colon \mathscr{C} \to \mathscr{C}_{gr}$ contravariante aditivo es exacto por la izquierda si y solo si para toda sucesión exacta $M_1 \xrightarrow{i} M_2 \xrightarrow{\pi} M_3 \to 0$ si consideramos la sucesión*

$$M_1^{\cdot} \xrightarrow{i^{\cdot}} M_2^{\cdot} \xrightarrow{\pi^{\cdot}} M_3^{\cdot} \to 0$$

se cumple que un morfismo $f\colon M_2^{\cdot} \to F$ factoriza vía $M_3^{\cdot}$ si y solo si $f \circ i^{\cdot} = 0$, y que si $g\colon M_3^{\cdot} \to F$ es tal que $g \circ \pi^{\cdot} = 0$ entonces $g = 0$.

Demostración. Considérese el diagrama el diagrama conmutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & F(M_3) & \longrightarrow & F(M_2) & \longrightarrow & F(M_1) \\ & & \| & & \| & & \| \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathscr{C}}(M_3^{\cdot},F) & \longrightarrow & \mathrm{Hom}_{\mathscr{C}}(M_2^{\cdot},F) & \longrightarrow & \mathrm{Hom}_{\mathscr{C}}(M_1^{\cdot},F) \end{array}$$

□

6. Teorema: *Sea $\mathscr{C}$ una categoría abeliana que tiene un generador, sea $\mathscr{C}_{gr}$ la categoría de grupos abelianos y $F: \mathscr{C} \to \mathscr{C}_{gr}$ un funtor contravariante aditivo exacto por la izquierda.*

1. *Si existe un epimorfismo $\underset{i\in I}{\oplus} P_i^{\cdot} \to F$, entonces F es un límite inductivo de funtores representables.*
2. *Supongamos que $\mathscr{C}$ tiene sumas directas infinitas y que $F(\underset{j\in J}{\oplus} M_j) \subseteq \underset{j\in J}{\prod} F(M_j)$ para toda suma directa. Entonces, F es el límite inductivo de sus subfuntores representables.*
3. *Supongamos que $\mathscr{C}$ tiene sumas directas infinitas y que $F(\underset{j\in J}{\oplus} M_j) = \underset{j\in J}{\prod} F(M_j)$ para toda suma directa. Entonces, F es representable.*

Demostración. Sea $f^{\cdot}: M^{\cdot} \to F$ un morfismo de funtores. Si una composición de morfismos $P^{\cdot} \xrightarrow{g^{\cdot}} M^{\cdot} \to F$ es nula, entonces la composición $(\mathrm{Im}\, g)^{\cdot} \hookrightarrow M^{\cdot} \to (M/\mathrm{Im}\, g)^{\cdot} \to F$ es nula.

Sea $\{M_k\}$ el conjunto de los subobjetos de M, tales que la composición de morfismos $M_k^{\cdot} \hookrightarrow M^{\cdot} \to F$ sea nula. La composción $(M_k \oplus M_j)^{\cdot} = M_k^{\cdot} \oplus M_j^{\cdot} \to M^{\cdot} \to F$ es nula, luego la composición $(M_k + M_j)^{\cdot} \to M^{\cdot} \to (M/M_k + M_j)^{\cdot} \to F$ es nula, luego $M_j + M_k$ pertenece al conjunto considerado y éste es un sistema inductivo de subobjetos de M.

Sea $N_k := M/M_k$, $M^{\cdot} \to F$ factoriza de modo único vía un morfismo $N_k^{\cdot} \to F$, luego vía un morfismo $g: \varinjlim N_k^{\cdot} \to F$. El morfismo $g: \varinjlim N_k^{\cdot} \to F$ es un monomorfismo: Sea $h: P^{\cdot} \to \varinjlim N_k^{\cdot}$ tal que $g \circ h = 0$. El morfismo h factoriza vía un morfismo $h_k: P^{\cdot} \to N_k^{\cdot}$ (porque $(\varinjlim N_k^{\cdot})(P) = \varinjlim N_k^{\cdot}(P)$). Como la composición $P^{\cdot} \to N_k^{\cdot} \to F$ es nula, entonces $N_k^{\cdot} \to F$, factoriza vía $(N_k/\mathrm{Im}\, h_k)^{\cdot}$, luego $N_k/\mathrm{Im}\, h_k = N_{k'}$ (para cierto k'), el morfismo $P^{\cdot} \to N_{k'}^{\cdot}$ es nulo y $h: P^{\cdot} \to \varinjlim N_k^{\cdot}$ es nulo.

1. Denotemos para cada morfismo $M^{\cdot} \to F$, $F_M = \varinjlim_k N_k^{\cdot}$ que es un subfuntor de F. Morfismos $N^{\cdot} \to M^{\cdot} \to F$ inducen monomorfismos $F_N \hookrightarrow F_M \hookrightarrow F$. Dados dos subfuntores $F_N, F_M \subset F$, entonces F_N, F_M son subfuntores de $F_{N \oplus M}$.

Sea X el conjunto de los subconjuntos finitos de I, y para cada $J \in X$ denotemos $P_J = \underset{j \in J}{\oplus} P_j$. Entonces, $F = \sum_{i \in I} F_{P_i} = \varinjlim_{J \in X} F_{P_J} = \varinjlim_{J,k} (P_J / P_{J.k})^{\cdot}$, donde los $\{P_{J.k}\}$ son los subobjetos de P_J tales que la composición $P_{J,k}^{\cdot} \to P_J^{\cdot} \to F$ es nula.

2. La composición de morfismos $\oplus_k M_k^{\cdot} \to (\oplus_k M_k)^{\cdot} \to M^{\cdot} \xrightarrow{f^{\cdot}} F$ es nula, luego la composición $(\oplus_k M_k)^{\cdot} \to M^{\cdot} \xrightarrow{f^{\cdot}} F$ es nula, porque

$$\mathrm{Hom}_{\mathscr{C}}((\oplus_k M_k)^{\cdot}, F) = F(\oplus_k M_k) \subset \prod_k F(M_k) = \mathrm{Hom}_{\mathscr{C}}(\oplus_k M_k^{\cdot}, F)$$

Por tanto, la composición $(\sum_k M_k)^{\cdot} \hookrightarrow M^{\cdot} \to (M/\sum_k M_k)^{\cdot} \to F$ es nula, y $M' = \sum_k M_k$ es el mayor subobjeto de M, tal que la composición $M'^{\cdot} \to M^{\cdot} \to F$ es nula. Por tanto, el morfismo $M^{\cdot} \to F$ factoriza vía un único morfismo $F_M = (M/M')^{\cdot} \hookrightarrow F$, que hemos probado que es un monomorfismo,

Veamos que la familia de subfuntores representables de F es un conjunto. Sea A un generador de $\mathscr{C}$. Dados dos subfuntores representables distintos $M_1^{\cdot}, M_2^{\cdot} \hookrightarrow F$ sea $M_3^{\cdot} \subset F$ tal que los contenga (tómese $M_3^{\cdot} = F_{M_1 \oplus M_2}$). Sea A un generador de $\mathscr{C}$. Tenemos $M_1, M_2 \subset M_3$ Existe un morfismo $A \to M_1$ (o $A \to M_2$) de modo que el morfismo inducido $A \to M_3$ no factoriza vía un morfismo $A \to M_2$ (o $A \to M_1$, respectivamente). Por tanto, el morfismo $A^{\cdot} \to F$ inducido por $A^{\cdot} \to M_1^{\cdot}$, no factoriza vía un morfismo $A^{\cdot} \to M_2^{\cdot}$. Luego, los morfismos $\mathrm{Hom}_{\mathscr{C}}(A^{\cdot}, F)$ distinguen los subfuntores representables de F. Luego, la familia de subfuntores representables de F es un conjunto y es un sistema inductivo.

Dado $\phi \in F(M)$, tenemos el morfismo $\phi^{\cdot} : M^{\cdot} \to F$, y $\phi_M^{\cdot}(\mathrm{Id}) = \phi$. El morfismo $\phi^{\cdot}$ factoriza vía un subfuntor representable. Por tanto, el límite inductivo de todos los subfuntores representables de F se epiyecta (e inyecta) en F.

3. Sea A un generador de $\mathscr{C}$. Como

$$\mathrm{Hom}_{\mathscr{C}}(\underset{I}{\oplus} A^{\cdot}, F) = \prod_I \mathrm{Hom}_{\mathscr{C}}(A^{\cdot}, F) = \prod_I F(A) = F(\underset{I}{\oplus} A) = \mathrm{Hom}_{\mathscr{C}}((\underset{I}{\oplus} A)^{\cdot}, F)$$

el morfismo natural $\underset{F(A)}{\oplus} A^{\cdot} \to F$ factoriza vía un (único) morfismo $\pi^{\cdot} : (\underset{F(A)}{\oplus} A)^{\cdot} \to F$. Sea $M^{\cdot} \hookrightarrow F$ un subfuntor representable de F que contenga a $\mathrm{Im}\,\pi^{\cdot}$. Si $M^{\cdot} \neq F$ entonces existe uno mayor $M^{\cdot} \underset{\neq}{\subset} N^{\cdot} \subseteq F$. Luego existe un morfismo $A^{\cdot} \to N^{\cdot}$, que no factoriza vía $M^{\cdot}$, pero la composición $A^{\cdot} \to N^{\cdot} \hookrightarrow F$, factoriza vía un morfismo $A^{\cdot} \to (\underset{F(A)}{\oplus} A)^{\cdot}$, luego vía $A^{\cdot} \to M^{\cdot}$ y llegamos a contradicción.

□

7. Definición: Sea $\mathscr{C}$ una categoría con límites inductivos y $\mathscr{C}'$ una categoría con límites proyectivos, sea $\{M_i, f_{ij}\}_{i\in I}$ un sistema inductivo de objetos de una categoría $\mathscr{C}$ y $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$ un funtor contravariante. . Los morfismos naturales $M_j \to \varinjlim M_i$ inducen morfismos $F(\varinjlim M_i) \to F(M_j)$ y por tanto un morfismo $F(\varinjlim M_i) \to \varprojlim F(M_i)$. Diremos que el funtor F transforma límites inductivos en límites proyectivos si el morfismo anterior $F(\varinjlim M_i) \to \varprojlim F(M_i)$ es isomorfismo, para todo sistema inductivo de objetos.

8. Ejemplo: La propiedad universal del límite inductivo nos dice que el funtor a la categoría de conjuntos

$$N^{\cdot} = \mathrm{Hom}_{\mathscr{C}}(-, N)$$

transforma límites inductivos en proyectivos.

Un funtor aditivo contravariante exacto por la izquierda transforma límites inductivos en límites proyectivos si y solo si transforma sumas directas en productos directos.

Si F es un funtor covariante y $\mathscr{C}$ una categoría con límites proyectivos, existe un morfismo natural $F(\varprojlim M_i) \to \varprojlim F(M_i)$, y se dice que F transforma límites proyectivos en límites proyectivos si dicho morfismo es isomorfismo, para todo sistema de objetos. La propiedad universal del límite proyectivo nos dice que el funtor $\mathrm{Hom}_A(N, -)$ transforma límites proyectivos en proyectivos.

0.14. Problemas

1. Sea G un grupo. Si $a, g \in G$, se dice que aga^{-1} es el *conjugado* de g por a. La conjugación $\tau_a : G \to G$, $\tau_a(g) = aga^{-1}$ es un automorfismo de grupos (tales automorfismos de G reciben el nombre de *automorfismos internos*), y la aplicación $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, es un morfismo de grupos.

2. El centro del grupo simétrico S_n es trivial cuando $n \geq 3$.

3. Sean H y K dos subgrupos de un grupo G. Si $K \subseteq N(H)$, entonces $HK = KH$ es un subgrupo de G. Si además G es finito, entonces $|HK| = |H| \cdot |K| / |H \cap K|$.

4. Si G es un grupo de orden un número primo, entonces G es cíclico.

5. Si los únicos subgrupos de un grupo G son los triviales 1 y G, entonces $G \simeq \mathbb{Z}/p\mathbb{Z}$ para algún número primo p.

6. Todo grupo finito de orden par contiene algún elemento $g \neq 1$ tal que $g^2 = 1$.

7. Si H es un subgrupo propio de un grupo finito G, entonces existe algún elemento de G que no está contenido en ninguno de los subgrupos conjugados de H.

8. Sea X un G-conjunto. Dado $x \in X$ denotemos I_x el subgrupo de isotropía de x. Si $x' = g \cdot x$, prueba que $I_{x'} = g \cdot I_x \cdot g^{-1}$.

9. Los morfismos de G-conjuntos transforman órbitas en órbitas, y todo endomorfismo de una órbita es un automorfismo.

10. Sean H y K dos subgrupos de un grupo G. Los G-conjuntos G/H y G/K son isomorfos precisamente cuando H y K son subgrupos conjugados.

11. Sea X un G-conjunto, $H \subseteq G$ un subgrupo y consideremos G/H como G-conjunto de modo natural: $g \cdot \bar{g'} := \overline{gg'}$. Prueba que la aplicación,

$$\mathrm{Hom}_G(G/H, X) \to X^H, f \mapsto f(\bar{1})$$

es biyectiva.

12. Si H es un subgrupo de un grupo G, el grupo de automorfismos del G-conjunto G/H es isomorfo al grupo $N(H)/H$.

13. Si H es un subgrupo de un grupo finito G, el número de subgrupos conjugados de H divide al índice, $|G/H|$, de H en G.

14. Todo subgrupo de índice 2 es normal. (*Indicación:* Si $g \notin H$, entonces gH es el complementario de H.)

15. Si el índice de un subgrupo H de un grupo finito G es el menor número primo que divide al orden de G, entonces H es un subgrupo normal de G. (*Indicación:* Considérese la acción de H, o la de G, en G/H.)

16. El grupo A_4 no tiene ningún subgrupo de orden 6 (aunque su orden es múltiplo de 6).

17. Sea G un grupo finito. Si el conjunto de subgrupos de G está totalmente ordenado (i.e., no tiene pares incomparables), entonces G es un grupo cíclico de orden potencia de un primo.

18. Sea p un número primo. Un grupo finito G es un p-grupo precisamente cuando para todo G conjunto finito X se cumple que $|X| \equiv |X^G|$ (módulo p).

19. Todo subgrupo normal de orden p de un p-grupo G está contenido en el centro de G.

20. Todo subgrupo normal H de un p-grupo G tiene intersección no trivial con el centro de G; es decir, $Z(G) \cap H \neq 1$.

21. Si G es un p-grupo no abeliano de orden p^3, entonces todo subgrupo normal de G contiene al centro.

22. Si H es un subgrupo propio de un p-grupo, entonces $H \neq N(H)$.

23. Determina los subgrupos de Sylow de los grupos simétricos S_3, S_4 y S_5.

24. Determina todos los subgrupos normales de S_3, S_4 y A_4.

25. Si una potencia p^r de un número primo divide al orden de un grupo finito G, entonces G tiene algún subgrupo de orden p^r.

26. Todo grupo de orden 100 tiene algún subgrupo normal de orden 25.

27. Sea H un subgrupo de orden p^k de un grupo G de orden $p^n m$. Si $k < n$, entonces G tiene un subgrupo H' de orden p^{k+1} tal que $H \lhd H'$.

28. Si H es un p-subgrupo normal de un grupo finito G, entonces H está contenido en todos los p-subgrupos de Sylow de G.

29. El grupo diédrico D_n (el grupo de los movimientos que dejan invariante un polígono regular de n lados) tiene orden $2n$ y está generado por dos elementos g y s tales que $g^n = s^2 = 1$, $sgs = g^{-1}$. Calcula el centro y el grupo de automorfismos del grupo D_n.

30. Si p es un número primo, todo grupo no abeliano de orden $2p$ es isomorfo al grupo D_p.

31. Si para cada número primo que divide al orden de un grupo finito G éste tiene un único subgrupo de Sylow, entonces G es isomorfo al producto directo de sus subgrupos de Sylow.

32. Clasificar, salvo isomorfismos, los grupos de orden ≤ 10.

33. Si $n \geq 5$, el único subgrupo propio de S_n de índice menor que n es A_n. (*Indicación:* Si H es un subgrupo de índice d en un grupo G, la acción de G en G/H define un morfismo $G \to S_d$.)

34. Las proyectividades de una recta proyectiva sobre un cuerpo con 5 elementos definen un subgrupo P de índice 6 del grupo S_6; luego existe un automorfismo $\tau\colon S_6 \to S_6$ tal que $\tau(P) = \{\sigma \in S_6 \colon \sigma(6) = 6\}$, y éste es un automorfismo externo del grupo S_6.

35. Demuestra que $\mathbb{C}[x,y]/(x) \simeq \mathbb{C}[y]$. Prueba que $\mathbb{C}[x,y,z]/(y-x^2, y^3+z^3)$ es una $\mathbb{C}$-álgebra isomorfa a $\mathbb{C}[x,z]/(x^6+z^3)$.

36. Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. Los elementos de S son invertibles en A si y solo si el morfismo de localización $A \to A_S$ es un isomorfismo.

37. Prueba que $k[x,y]/(xy-1) \simeq k[x]_{\{1,x,x^2,\dots\}}$.

38. Prueba que $\mathbb{C}[x]_{\mathbb{R}[x]-0} \simeq \mathbb{C}(x)$.

39. Prueba que el morfismo de localización $i\colon A \to A_S$ es un isomorfismo si y solo si $i^*\colon \operatorname{Spec} A_S \to \operatorname{Spec} A$ es un homeomorfismo. Pruébese que $\operatorname{Spec} A_S = \operatorname{Spec} A_{S'}$ (en $\operatorname{Spec} A$) si y solo si $A_S = A_{S'}$.

40. Calcula $\operatorname{Spec} \mathbb{Z}/6\mathbb{Z}$, $\operatorname{Spec}(\mathbb{C}[x,y]/(y^2-x^3))_x$.

41. Calcula $\operatorname{Spec} \mathbb{Z}[x]$, $\operatorname{Spec} \mathbb{Z}[\sqrt{5}]$.

42. Calcula $\operatorname{Spec} \mathbb{R}[x,y]$.

43. Sean $I, I' \subseteq A$ dos ideales. Prueba que $(I)_0 = (I')_0$ si y solo si $r(I) = r(I')$, donde denotamos $r(I) = \{a \in A \colon a^n \in I \text{ para cierto } n \in \mathbb{N}\}$.

44. Prueba que los elementos de los ideales primos minimales de un anillo son divisores de cero (Pista: localícese en los ideales primos minimales).

45. Prueba que si $f\colon A \hookrightarrow B$ es un morfismo de anillos inyectivo, entonces el morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación continua de imagen densa.

46. Prueba que la intersección de dos rectas paralelas $(ax+by+c)_0$, $(ax+by+c')_0$ $(c \neq c')$ es vacía.

47. Dado el morfismo $i\colon \mathbb{C}[x] \to \mathbb{C}[x,y]/(y^2-x^2+x^3)$, $i(p(x)) = \overline{p(x)}$, calcula las fibras del morfismo inducido $i^*\colon \operatorname{Spec} \mathbb{C}[x,y]/(y^2-x^2+x^3) \to \operatorname{Spec} \mathbb{C}[x]$.

48. Calcula el morfismo $f\colon \mathbb{C}[x,y]/(x-1) \to \mathbb{C}[x,y]/(y-x^3)$ que en espectros aplica cada punto (cerrado) (α,β) de la cúbica $y=x^3$ en el punto de la recta $x=1$ que se obtiene como corte de la recta que pasa por el origen y (α,β), con la recta $x=1$.

49. Sea $I \subseteq A$ un ideal y M un A-módulo. Prueba que $IM := \{\sum_i a_i m_i \in M$, con $a_i \in I$ y $m_i \in M\}$ es un A-submódulo.

    Si M' es otro A-módulo prueba que $I(M \oplus M') = IM \oplus IM'$. Si M y M' son submódulos de un módulo prueba que $I(M+M') = IM + IM'$.

50. Sean $N \subseteq M$ y $N' \subseteq M'$ submódulos. Prueba que $N \oplus N'$ es un submódulo de modo natural de $M \oplus M'$, de modo que $(M \oplus M')/(N \oplus N') = M/N \oplus M'/N'$.

51. Sean N, N' submódulos de un módulo M. Prueba que $(N+N')/N' = N/(N \cap N')$. Si denotamos por $\bar{N} = \{\bar{n} \in M/N' : n \in N\}$, prueba que $(M/N')/\bar{N} = M/(N+N')$.

52. Sea $f\colon M \to M'$ un morfismo de A-módulos. Sean N_1, N_2 dos submódulos de M prueba que $f(N_1+N_2) = f(N_1) + f(N_2)$ (denotamos por $f(N) = \{f(n) \in M'$, con $n \in N\}$). Sea I un ideal, probar que $f(I \cdot N_1) = I \cdot f(N_1)$.

53. Sea $f\colon M \to M'$ un morfismo de A-módulos y $m' = f(m)$. Prueba que $f^{-1}(m') = m + \operatorname{Ker} f := \{m+n$ con $n \in \operatorname{Ker} f\}$. Sea N un submódulo de M, prueba que $f^{-1}(f(N)) = N + \operatorname{Ker} f$.

54. Prueba la igualdad $\operatorname{Hom}_A(A/I, M) = \{m \in M : Im = 0\}$. Prueba que $\operatorname{Hom}_A(A^n, M) = M \oplus \overset{n}{\ldots} \oplus M$.

55. Calcula los siguientes $\mathbb{Z}$-módulos: $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z})$, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Q})$ y por último $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z})$.

56. Prueba que si un endomorfismo $f\colon M \to M$, cumple que $f^2 = f$ entonces $M = \operatorname{Ker} f \oplus \operatorname{Ker}(f - \mathrm{Id})$.

57. Prueba que el anulador del A-módulo A/I es I.

58. Prueba que si M es un A-módulo libre entonces $\operatorname{Anul}(M) = 0$.

59. Sea el $\mathbb{Z}$-módulo $M = \bigoplus_{0 \neq n \in \mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. Prueba que $\operatorname{Anul} M = (0)$. ¿Existe algún $m \in M$ de modo que $\operatorname{Anul}(\langle m \rangle) = 0$?

60. Prueba que si $M \simeq M_1 \oplus \cdots \oplus M_n$ entonces $\operatorname{Anul}(M) = \bigcap_i \operatorname{Anul}(M_i)$. Calcula el ideal anulador del $\mathbb{Z}$-módulo $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$.

61. Sea $0 \to M_1 \to M_2 \to M_3 \to 0$ una sucesión exacta de A-módulos. Demuestra que $\mathrm{Anul}(M_2) \supseteq \mathrm{Anul}(M_1) \cdot \mathrm{Anul}(M_3)$.

62. ¿Es $\mathbb{Z}/4\mathbb{Z}$ un $\mathbb{Z}$-módulo libre? ¿Es un $\mathbb{Z}/4\mathbb{Z}$-módulo libre? Define un sistema generador de $\mathbb{Z}/4\mathbb{Z}$ como $\mathbb{Z}$-módulo.

63. Sea $M = \{\frac{a}{2^n}, a \in \mathbb{Z}, n \in \mathbb{N}\} \subset \mathbb{Q}$. Prueba que M es un $\mathbb{Z}$-submódulo de $\mathbb{Q}$ y que no es finito generado.

64. Prueba que todo cociente de un módulo finito generado es finito generado. Prueba que la suma de dos submódulos finito generados es finito generado.

65. Sea $C(\mathbb{R})$ el anillo de todas las funciones reales continuas de variable real. Demuestra que el conjunto de las funciones reales continuas de variable real que se anulan en algún entorno del cero forman un ideal de $C(\mathbb{R})$, que no es finito generado.

66. Prueba que todo $\mathbb{Z}$-submódulo finito generado de $\mathbb{Q}$ no nulo, es libre generado por un elemento. Prueba que $\mathbb{Q} \neq \mathbb{Z}$.

67. Halla una base (si existe) de $\mathbb{Z}[x]$ como $\mathbb{Z}$-módulo.

68. Prueba que todo epimorfismo de un módulo en un libre tiene sección.

69. Sea $i\colon N \hookrightarrow M$ un morfismo inyectivo de A-módulos. Si $r\colon M \to N$ es un retracto de i, es decir, $r \circ i = \mathrm{Id}$. Prueba que $M \simeq N \oplus \mathrm{Ker}\, r$.

    Sea $\pi\colon M \to M'$ un epimorfismo de módulos, de modo que exista una sección s de π, es decir, $\pi \circ s = \mathrm{Id}$. Prueba que $M \simeq \mathrm{Ker}\, \pi \oplus M$.

70. Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta de A módulos. Se dice que la sucesión exacta rompe o está escindida si existe un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \| \mathrm{Id} & & \| \phi & & \| \mathrm{Id} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M' \oplus M'' & \xrightarrow{\pi} & M'' & \longrightarrow & 0 \end{array}$$

    donde ϕ es un isomorfismo, $i(m') = (m', 0)$ y $\pi(m', m'') = m''$.

    Prueba que si $r\colon M \to M'$ es un retracto de f, i.e., $r \circ f = \mathrm{Id}$ entonces la sucesión exacta rompe. Prueba que si $s\colon M'' \to M$ es una sección de g, i.e., $g \circ s = \mathrm{Id}$, entonces la sucesión exacta rompe.

71. Prueba que $(\mathrm{Anul}_A(M))_S = \mathrm{Anul}_{A_S}(M_S)$, si M es un A-módulo finito generado.

72. Sea $f: A \to B$ un morfismo de anillos. Sea $S \subset A$ un sistema multiplicativo. Sabemos que B es de modo natural un A-módulo, por tanto, podemos definir B_S. Por otra parte, $f(S) \subset B$ es un sistema multiplicativo. Demuestra que $B_S = B_{f(S)}$.

73. Sea $I \subseteq A$ un ideal y $\mathfrak{p}_x \subset A$ un ideal primo. Prueba que $I_x = A_x$ si y solo si $x \notin (I)_0$.

74. Prueba que $(I \cdot M)_S = I_S \cdot M_S = I \cdot M_S$.

75. Sea A un anillo íntegro, e $I \neq 0$ un ideal. Prueba que I es libre si y solo si $I = aA$ $(a \neq 0)$.

76. Sea M un A-módulo finito generado y $S \subset A$ un sistema multiplicativo de A. Prueba que si $M_S = 0$ entonces existe un $s \in S$ tal que $s \cdot m = 0$ para todo $m \in M$.

77. Sea $I \subseteq A$ un ideal y M un A-módulo finito generado. Prueba que $IM = M \iff M_{1+I} = 0$.

78. Prueba que si un endomorfismo $T: M \to M$ de un A-módulo finito generado es epiyectivo entonces es un isomorfismo.

79. Demuestra que $\mathbb{Z}^n$ es un $\mathbb{Z}$-módulo isomorfo a $\mathbb{Z}^m$ si y solo si $n = m$.

80. Demuestra que A^n es un A-módulo isomorfo a A^m si y solo si $n = m$.

81. Sea M un A-módulo finito generado. Prueba que si $M \simeq M \oplus N$ entonces $N = 0$. ¿Es siempre cierto este resultado si M no es finito generado?

82. Sea $m_1, \ldots, m_s$ un sistema generador de un A-módulo libre A^n. Prueba que $s \geq n$.

83. Prueba que todo sistema de n generadores de un módulo libre A^n es base.

84. Sean M y M' dos A-módulos finito generados. Sea $f: M \to M'$ un morfismo de A-módulos. Prueba que si los morfismos $\bar{f}_x: M/\mathfrak{m}_x M \to M'/\mathfrak{m}_x M'$, $\bar{m} \mapsto \overline{f(m)}$ son epiyectivos, para todo punto cerrado $x \in \mathrm{Spec}\, A$, entonces el morfismo f es epiyectivo.

85. Demuestra que si existe un morfismo de A-módulos $A^m \hookrightarrow A^n$ inyectivo, entonces $m \leq n$.

86. Demuestra que la longitud del $k[x]$-módulo $k[x]/(x^n)$ es n.

87. Sea $A \to B$ un morfismo de anillos. Sea Δ el núcleo del morfismo $B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$. Prueba que Δ es un ideal de $B \otimes_A B$ y que $\Delta = \langle b \otimes 1 - 1 \otimes b \rangle_{b \in B}$.

    Si M y M' son B-módulos, prueba que

$$M \otimes_B M' \simeq (M \otimes_A M')/\Delta \cdot (M \otimes_A M').$$

88. Demuestra que el morfismo natural $M^* \otimes_A N \to \mathrm{Hom}_A(M,N)$, $w \otimes n \mapsto \phi_{w \otimes n}$, donde $\phi_{w \otimes n}(m) := w(m) \cdot n$ es un isomorfismo lineal si N es un A-módulo libre finito generado. Demuestra que el morfismo natural $M^* \otimes_A N^* = Bil_A(M,N;A)$, $w \otimes w' \mapsto \phi_{w \otimes w'}$, donde $\phi_{w \otimes w'}(m,n) = w(m) \cdot w'(n)$, es un isomorfismo lineal si N es un A-módulo libre finito generado.

89. Prueba que $\mathbb{R}[x]/(p(x)) \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x]/(p(x))$.

90. Prueba que $(A[x_1,\ldots,x_n]/I) \otimes_A B = B[x_1,\ldots,x_n]/I \cdot B[x_1,\ldots,x_n]$.

91. Prueba que $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \times \mathbb{C}$ como $\mathbb{C}$-álgebra. Calcula $\mathrm{Hom}_{\mathbb{R}-\text{álg.}}(\mathbb{C},\mathbb{C})$.

92. Prueba que $\mathrm{Hom}_{k-\text{álg.}}(A,k)$ es igual al conjunto de ideales primos maximales de A, de conúcleo k.

93. Sea A un anillo íntegro y M un A-módulo plano. Prueba que $T(M) = 0$.

94. Prueba que si M y N son A-módulos planos, también lo es $M \otimes_A N$. Prueba que si B es una A-álgebra plana y M es un B-módulo plano, entonces M es un A-módulo plano.

95. Sea $A \to B$ un morfismo de anillos fielmente plano. Sea M un A-módulo. Prueba que si $M \otimes_A B$ es un B-módulo finito generado, entonces M es un A-módulo finito generado.

96. Sea $A \hookrightarrow B$ un morfismo de anillos fielmente plano. Prueba que la sucesión

$$A \hookrightarrow B \overset{\overset{i_1}{\longrightarrow}}{\underset{i_2}{\longrightarrow}} B \otimes_A B$$

    (donde $i_1(b) := b \otimes 1$ e $i_2(b) = 1 \otimes b$) es exacta (es decir, $\mathrm{Ker}(i_1 - i_2) = A$).

    Resolución: Tensando la sucesión por $\otimes_A B$, basta ver que la sucesión

$$B \hookrightarrow B' \overset{\overset{i'_1}{\longrightarrow}}{\underset{i'_2}{\longrightarrow}} B' \otimes_B B'$$

(donde $B' = B \otimes_A B$) es exacta. El morfismo $r\colon B' = B \otimes_A B \to B$, $r(b_1 \otimes b_2) := b_1 b_2$ es retracto de la inclusión $B \hookrightarrow B' = B \otimes B$. Consideremos el morfismo $r \otimes 1\colon B' \otimes_B B' \to B'$, $(r \otimes 1)(b_1' \otimes b_2') = r(b_1') \cdot b_2'$. Si $(i_1' - i_2')(b') = 0$, entonces aplicando $r \otimes 1$ obtenemos que $r(b') - b' = 0$, luego $b' \in B$.

97. Prueba que $k[x,y]/(x)$ no es un $k[x,y]$-módulo plano. Sea $k[x] \to k[x,y]/(y^2 - x)$ el morfismo natural, prueba que $k[x,y]/(y^2 - x)$ es una $k[x]$-álgebra plana.

98. Sea A un dominio de ideales principales y M un A-módulo sin torsión. Prueba que M es unión de módulos libres finito generados.

99. Sea $N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n \supseteq \cdots$ una sucesión decreciente de A-submódulos de N_0. Prueba que $\varprojlim_n N_n = \bigcap_n N_n$.

100. Sea I un conjunto filtrante decreciente y $J \subseteq I$ un subconjunto con la propiedad de que dado $i \in I$ existe $j \in J$ tal que $j \geq i$. Sea $\{M_i\}_{i \in I}$ un sistema proyectivo de objetos. Prueba que $\varprojlim_{i \in I} M_i = \varprojlim_{j \in J} M_j$.

101. Prueba que $\varprojlim_{i \in I} (M_i \times N_i) = (\varprojlim_{i \in I} M_i) \times (\varprojlim_{i \in I} N_i)$, en la categoría de A-módulos, por ejemplo.

102. Demuestra que todo módulo es el límite inductivo de sus submódulos finito generados.

103. Dado un conjunto X denotemos $X^* := \{f : X \to \mathbb{Z}, \text{ inyectiva}\}$. Prueba que si $X \to\!\!\!\rightarrow X'$ es una aplicación inyectiva entre conjuntos finitos, entonces la aplicación inducida $X'^* \to X^*$ es epiyectiva. Dado un sistema inductivo $\{X_i, f_{ij}\}$ de aplicaciones, prueba que $(\varinjlim_i X_i)^* = \varprojlim_i X_i^*$. Sea $\{X_i\}$ el conjunto de subconjuntos finitos de $\mathbb{R}$. Prueba que $\{X_i^*\}$ es un sistema proyectivo de aplicaciones epiyectivas tal que $\varinjlim_i X_i^* = \emptyset$.

104. Demuestra que el límite inductivo de módulos planos es plano.

105. Sea x un punto de un espacio topológico X. Sea I el conjunto de entornos abiertos de x, ordenados del siguiente modo: $U \leq V$ si $U \subseteq V$. Sea $C(U)$ las funciones reales continuas sobre U, tenemos un sistema inductivo de anillos $\{C(U)\}$, donde los morfismos $C(U) \to C(V)$ son los de restricción. Probar que $\varinjlim_{x \in U} C(U)$ es el anillo de gérmenes de funciones continuas en x.

106. Sea $x \in \operatorname{Spec} A$ y M un A-módulo. Demuestra que $M_x = \varinjlim_{\{x \in U_a\}} M_a$.

107. Sea $M = C_0^\infty(\mathbb{R})$ el anillo de gérmenes de funciones diferenciables reales de la recta real en el origen. Prueba que M es un $C^\infty(\mathbb{R})$-módulo plano finito generado, no proyectivo, ni de presentación finita.

108. Sea $\{A_i\}$ un sistema inductivo de anillos. Probar $\operatorname{Spec} \varinjlim A_i = \varprojlim \operatorname{Spec} A_i$.

109. Sean N,N' submódulos de M, tales que $M = N+N'$. Prueba que M es noetheriano si y solo si N,N' son noetherianos.

110. Sean N,N' submódulos de M, tales que $N \cap N' = 0$. Prueba que M es noetheriano si y solo si M/N,M/N' son noetherianos.

111. Sea M un A-módulo noetheriano. Prueba que $A/\operatorname{Anul}(M)$ es un anillo noetheriano.

112. Prueba que si M es un A-módulo noetheriano entonces $M[x]$ es un $A[x]$-módulo noetheriano.

113. Prueba que si $A[x]$ es noetheriano entonces A es noetheriano.

114. Escribamos $\operatorname{Spec} A = \cup_i U_{a_i}$. Prueba que un A-módulo M es noetheriano si y solo si M_{a_i} son A_{a_i}-módulos noetherianos para todo i.

115. Demuestra que $\prod^\infty \mathbb{Z}$ no es un anillo noetheriano.

116. Sea A un anillo noetheriano íntegro. Prueba que todo elemento propio de A es producto de irreducibles.

117. Sea A un anillo noetheriano. Prueba que existe un $n \in \mathbb{N}$ de modo que $(\operatorname{rad} A)^n = 0$.

118. Sea A un anillo noetheriano, e $I \subset A$ un ideal. Prueba que existe un $n \in \mathbb{N}$ de modo que $r(I)^n \subseteq I$.

119. Sea A un anillo noetheriano y sea $f = \sum_{i=0}^{\infty} a_i x^i \in A[[x]]$. Demuestra que f es nilpotente si y solo si cada a_i es nilpotente.

120. Sea A un dominio de ideales principales. Si $aA \cap bA = cA$, pruébese que c es el mínimo común múltiplo de a y b.

121. Sea A un dominio de ideales principales. Sean $a = p_1^{n_1} \cdots p_r^{n_r}$, $b = p_1^{m_1} \cdots p_r^{m_r}$ con $n_i, m_j \geq 0$, p_i irreducibles y p_i primo con p_j, para $i \neq j$. Calcúlese el mínimo común múltiplo y máximo común divisor de a y b.

122. Sean p y q números primos distintos. Se pide calcular el número de grupos abelianos finitos desisomorfos de orden p^2q.

123. Pruébese que un grupo abeliano finito que no sea cíclico contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, para un cierto entero primo p.

124. Sea G un grupo abeliano finito. Demuestra que G es cíclico si y solo si para cada n divisor del orden de G, existe un único subgrupo de G de orden n.

125. Sea G un subgrupo discreto del grupo aditivo de $\mathbb{R}^n$. Pruébese que existe un número natural $r \leq n$, tal que G está generado como $\mathbb{Z}$-módulo por r vectores linealmente independientes sobre $\mathbb{R}$.

126. Clasifíquese el endomorfismo "multiplicar por x" sobre el k-espacio vectorial

$$E = k[x]/(x) \oplus k[x]/(x^3) \oplus k[x]/(x^5).$$

127. Clasifíquense los endomorfismos nilpotentes de un espacio vectorial de dimensión 3. Problema análogo para espacios de dimensión 4 y 5.

128. Clasifíquense los endomorfismos T de un espacio vectorial real E, que cumplan

   a) Anulador de $T = (x-1)^2$, $\dim E = 5$.

   b) Anulador de $T = (x^2+4)^2(x+8)^2$, $\dim E = 8$.

129. Clasifica sobre el cuerpo racional el endomorfismo $T = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.

130. Sea E el espacio vectorial real de todos los polinomios con coeficientes reales de grado menor que 6, y sea D el operador derivada sobre E. Clasifíquese el endomorfismo $T = D^2$.

131. La ley del enfriamiento de Newton establece que la tasa de pérdida de calor de un cuerpo es proporcional a la diferencia de temperatura entre el cuerpo y sus alrededores. Un sólido a 20º centígrados es introducido en un lago de agua a temperatura de 5º. Si tarda dos minutos en enfriarse diez grados ¿Cuántos minutos tardará en enfriarse 14 grados?

132. Sea F el espacio vectorial formado por las funciones de $\mathbb{R}$ a $\mathbb{C}$ infinitamente derivables y $D: F \to F$ el operador derivada. Prueba que

    a) $D(e^f \cdot g) = e^f \cdot (D + f' \cdot \mathrm{Id})(g)$.

    b) Calcula las soluciones de la ecuación diferencial lineal $y' + fy = g$.

133. Sea F el espacio vectorial formado por las funciones de $\mathbb{R}^+$ a $\mathbb{C}$ infinitamente derivables y $\Theta: F \to F$ el operador $\mathbb{C}$-lineal definido por $\Theta(f) := xf'$.

    a) Prueba que $\mathrm{Ker}(\Theta - \alpha)^r = x^\alpha \cdot \{\sum_{i=0}^{r-1} \lambda_i (\ln x)^i : \ \forall\, \lambda_i \in \mathbb{C}\}$.

    b) Resuelve la ecuación de Euler-Cauchy $x^2 y'' + bxy' + cy = 0$, para $b, c \in \mathbb{C}$ y $x > 0$.

134. Resuelve la ecuación diferencial del movimiento armónico amortiguado

$$f'' + af' + bf = 0, \ \text{(con } a^2 - 4b < 0 \text{ y } a > 0\text{)}.$$

135. Resuelve la ecuación diferencial del movimiento armónico forzado

$$f'' + af' + bf = c\cos(wx), \ \text{(con } a^2 - 4b < 0 \text{ y } a > 0\text{)}.$$

136. Calcula $\int x^2 e^x \, dx$.

137. Pruébese que $\Delta\binom{n}{i} = \binom{n}{i-1}$. Pruébese que $\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}\}$ es una base de $\mathrm{Ker}\,\Delta^{r+1}$. Sea $p(n) = \sum_{i=0}^{r} \lambda_i \binom{n}{i}$, pruébese que λ_i es el término 0 de la sucesión $\Delta^i(p(n))$, es decir,

$$\lambda_i = \sum_{j=0}^{i} \binom{i}{j} \cdot (-1)^j p(i-j).$$

    Calcula $\sum_{i=0}^{n} i^2$.

138. Calcúlense cuántos números de longitud n se pueden escribir con ceros y unos, de modo que nunca aparezcan dos ceros seguidos (ejemplo: los números de longitud tres cumpliendo lo dicho son $010, 011, 101, 110, 111$, que son cinco distintos).

139. Resuélvase la ecuación $a_{n+2} + 2a_{n+1} - 8a_n = 2^n$.

140. Calcúlese $\sum_{i=0}^{n} g^i$.

141. Sea $p(x) \in \mathbb{R}[x]$ un polinomio mónico de grado n. Sean $s_1(x), \ldots, s_n(x)$ soluciones, linealmente independientes, de la ecuación diferencial $p(D)y = 0$. Pruébese que si las funciones $c_1(x), \ldots, c_n(x)$ cumplen las ecuaciones

$$\begin{array}{rcl} c_1(x)'s_1(x) + \ldots + c_n(x)'s_n(x) & = & 0 \\ \ldots & = & 0 \\ c_1(x)'s_1(x)^{n-2)} + \ldots + c_n(x)'s_n(x)^{n-2)} & = & 0 \\ c_1(x)'s_1(x)^{n-1)} + \ldots + c_n(x)'s_n(x)^{n-1)} & = & f(x) \end{array}$$

entonces $c_1(x)s_1(x) + \ldots + c_n(x)s_n(x)$ es una solución particular de $p(D)y = f(x)$.

142. Sea $p(x) \in \mathbb{R}[x]$ un polinomio mónico de grado r. Sean $s_1(n), \ldots, s_r(n)$ soluciones, linealmente independientes, de la ecuación en diferencias $p(\nabla)y = 0$. Pruébese que si las sucesiones $c_1(n), \ldots, c_r(n)$ cumplen las ecuaciones

$$\begin{array}{rcl} \Delta(c_1)\nabla(s_1) + \ldots + \Delta(c_r)\nabla(s_r) & = & 0 \\ \ldots & = & 0 \\ \Delta(c_1)\nabla^{r-1}(s_1) + \ldots + \Delta(c_r)\nabla^{r-1}(s_r) & = & 0 \\ \Delta(c_1)\nabla^{r}(s_1) + \ldots + \Delta(c_r)\nabla^{r}(s_r) & = & f \end{array}$$

entonces $c_1 s_1 + \ldots + c_r s_r$ es una solución particular de $p(\nabla)y = f$.

143. Prueba que un grupo abeliano finito generado no trivial es cíclico si y solo si tiene un único factor invariante no invertible.

144. ¿Es posible dar un procedimiento algorítmico para saber si dos endomorfismos de un $\mathbb{R}$-espacio vectorial de dimensión finita (es decir, dos matrices cuadradas con coeficientes reales) son equivalentes o no? En el caso de que sean equivalentes, ¿puede calcularse un endomorfismo (o matriz) que de la equivalencia?

145. Prueba que si el polinomio característico de un endomorfismo lineal tiene todas sus raíces distintas entonces coincide con el primer factor invariante.

146. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Prueba que la condición necesaria y suficiente para que el endomorfismo $p(T)$ sea invertible es que $p(x)$ y $c_T(x)$ sean primos entre si.

147. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Sea $E' \subseteq E$ un subespacio estable por T. Denotemos $\bar{T}\colon E/E' \to E/E'$, $\bar{T}(\bar{e}) = \overline{T(e)}$, el endomorfismo inducido por T en E/E'. Prueba que

$$c_T(x) = c_{T_{|E'}}(x) \cdot c_{\bar{T}}(x).$$

148. Sea E un $\mathbb{C}$-espacio vectorial de dimensión n y T un endomorfismo de E. Sea $c_T(x) = \prod_{i=1}^{n}(x-\alpha_i)$ la descomposición en factores lineales del polinomio característico de T. Pruébese que si $p(x)$ es un polinomio con coeficientes en $\mathbb{C}$, entonces

$$c_{p(T)}(x) = \prod_{i=1}^{n}(x - p(\alpha_i)).$$

En particular, se tiene que $\operatorname{tr}(p(T)) = \sum_{i=1}^{n} p(\alpha_i)$, $\det(p(T)) = \prod_{i=1}^{n} p(\alpha_i)$.

149. Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita. Sea $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal de E. Demuestra que si $c_T(x)$ es el polinomio característico de T considerado como endomorfismo $\mathbb{C}$-lineal, entonces el polinomio característico de T considerado como endomorfismo $\mathbb{R}$-lineal es $c_T(x)\cdot\overline{c_T(x)}$ (donde $\overline{c_T(x)}$ es el conjugado de $c_T(x)$).

150. *a*) Sea $X' = AX$ un sistema homogéneo de ecuaciones diferenciales, siendo A una matriz cuadrada de coeficientes constantes. Probar que $e^{At}\cdot C$ son las soluciones del sistema, siendo C una matriz columna de constantes.

b) Sea $X' = AX + B(t)$ un sistema lineal de ecuaciones diferenciales. Calcula la matriz columna $C(t)$ tal que $e^{At}\cdot C(t)$ sea una solución del sistema.

151. Resuélvanse los siguientes sistemas de ecuaciones diferenciales

$$\begin{aligned} \tfrac{dx}{dt} &= x - 3y + 3z \\ \tfrac{dy}{dt} &= -2x - 6y + 13z \\ \tfrac{dz}{dt} &= -x - 4y + 8z \end{aligned} \qquad \begin{aligned} \tfrac{dx}{dt} &= 3x - y \\ \tfrac{dy}{dt} &= x + y \\ \tfrac{dy}{dt} &= 3x + 5z - 3u \\ \tfrac{du}{dt} &= 4x - y + 3z - u \end{aligned} \qquad \begin{aligned} \tfrac{dx}{dt} &= -11x - 4y \\ \tfrac{dy}{dt} &= 15x + 6y \end{aligned}$$

152. Sea $P(x) \in \mathbb{R}[x]$ un polinomio de grado n. Prueba que la ecuación diferencial $P(D)y = f(x)$ es equivalente a un sistema de ecuaciones diferenciales lineales de n variables. Usando el problema 150 b), pruébese el problema 141.

153. Sea A un anillo euclídeo y (a_{ij}) una matriz con coeficientes $a_{ij} \in A$. Sustituyendo de modo conveniente y sucesivo la fila F_i por la fila $F_i + b_j F_j$, $i \neq j$, $b_j \in A$ (i, j, b_j arbitrarios), demuestra que la matriz (a_{ij}) es triangulable. Si admitimos, además, las mismas transformaciones "elementales" con las columnas, demuestra que (a_{ij}) es diagonalizable. Resuelve el sistema de ecuaciones diofánticas

$$\begin{aligned} 7x + 5y &= 1 \\ 5x + 3y &= 3 \end{aligned}$$

154. Clasifica el $\mathbb{Z}$-módulo $(\mathbb{Z}\times\mathbb{Z})/\langle(7,5),(5,3)\rangle$.

155. Sea A una matriz con coeficientes en $k[D]$. Prueba que mediante las transformaciones elementales, el problema de resolver los sistemas $AX(t)=Y(t)$, se reduce al problema de resolver ecuaciones $P(D)f(t)=h(t)$.

Capítulo 1

Raíces reales y complejas de polinomios

El teorema de Kronecker afirma que dado un polinomio con coeficientes en un cuerpo $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$, existe una extensión finita de cuerpos $k \hookrightarrow K$ y $\alpha_1, \ldots, \alpha_n \in K$ tal que $p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n)$.

Los coeficientes de un polinomio son polinomios simétricos en las raíces del polinomio (fórmulas de Cardano) y todo polinomio simétrico en las raíces es igual a un polinomio en los coeficientes de las raíces. Usando este hecho y el teorema de Kronecker probaremos el teorema fundamental del Álgebra que afirma que para todo polinomio $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$, existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ de modo que $p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n)$. Vía la teoría del exceso y el teoremas de Sturm sabremos calcular el número de raíces complejas de un polinomio con coeficientes complejos contenidas en el interior de un circuito (por ejemplo un rectángulo). Luego podremos separarlas y calcularlas por aproximación. Para la resolución de los sistemas de ecuaciones algebraicas se introduce la resultante de polinomios. Gracias a ésta, dado un sistema de ecuaciones k-algebraicas podremos eliminar una variable, digamos x_1, de modo que si $(\alpha_1, \ldots, \alpha_n)$ es una solución del primero $(\alpha_2, \ldots, \alpha_n)$ es una solución del segundo sistema. Se reduce así el problema de resolver un sistema de ecuaciones algebraicas al problema del cálculo las raíces de un polinomio (con coeficientes en una extensión de cuerpos de k).

1.1. Funciones simétricas

1.1.1. Funciones simétricas elementales

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = c(x-\alpha_1)\cdots(x-\alpha_n)$. Desarrollando el último término e igualando coeficientes de los x^i se obtiene las fórmulas de Cardano:

$$\begin{aligned}
a_0 &= c \\
a_1 &= -c\cdot(\alpha_1+\cdots+\alpha_n) \\
&\cdots \\
a_i &= (-1)^i c\cdot \sum_{1\le j_1<\cdots<j_i\le n} \alpha_{j_1}\cdots\alpha_{j_i} \\
&\cdots \\
a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n
\end{aligned}$$

1. Definición: Llamaremos *funciones simétricas elementales* (o polinomios simétricos elementales) en las letras $x_1,\ldots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\ldots,x_n]$ $(i=1,\ldots,n)$ definidos por:

$$\begin{aligned}
s_1 &= x_1+\cdots+x_n \\
&\cdots \\
s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\
&\cdots \\
s_n &= x_1\cdots x_n
\end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x-x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n.$$

Sea S_n el grupo de las permutaciones de $\{1,\ldots,n\}$. Consideremos la operación de S_n en $A[x_1,\ldots x_n]$ siguiente:

$$\sigma(P(x_1,\ldots,x_n)) := P(x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

para cada $\sigma\in S_n$ y $P(x_1,\ldots,x_n)\in A[x_1,\ldots x_n]$. Observemos que cada $\sigma\in S_n$ opera en $A[x_1,\ldots x_n]$ como morfismo de A-álgebras.

2. Definición: Diremos que un polinomio $P(x_1,\ldots,x_n)\in A[x_1,\ldots x_n]$ es simétrico cuando $\sigma(P)=P$ para toda $\sigma\in S_n$.

$A[x_1,\ldots,x_n]^{S_n}$ es el conjunto de las funciones simétricas y es una A-subálgebra de $A[x_1,\ldots x_n]$.

3. Teorema de las funciones simétricas: *Se cumple la igualdad:*

$$A[x_1,\ldots,x_n]^{S_n} = A[s_1,\ldots,s_n].$$

Es decir, un polinomio en $x_1,\ldots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y solo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Procedemos por inducción sobre el número n de variables. Para $n = 1$ es trivial. Sea $n \geq 1$. Sea $P(x_1,\ldots,x_n) \in A[x_1,\ldots,x_n]^{S_n}$. Descomponiendo P en sus componentes homogéneas, podemos suponer que P es homogéneo de grado m. Haciendo cociente por x_n se obtiene que $P(x_1,\ldots,x_{n-1},0)$ es un polinomio homogéneo de grado m en $n-1$ variables e invariante por las permutaciones de éstas, luego por hipótesis de inducción $P(x_1,\ldots,x_{n-1},0) = Q(s'_1,\ldots,s'_{n-1})$, siendo s'_i la i-ésima función simétrica en las $n-1$ primeras variables. Observemos que en $Q(s'_1,\ldots,s'_{n-1})$ cada sumando $\lambda_{(m_1,\ldots,m_{n-1})} s'^{m_1}_1 \cdots s'^{m-1}_{n-1}$ es un polinomio homogéneo en $x_1,\ldots,x_{n-1}$ de grado $m_1+2m_2+\cdots+(n-1)m_{n-1}$. Podemos suponer que $\lambda_{(m_1,\ldots,m_{n-1})} = 0$, cuando $m_1+2m_2+\cdots+(n-1)m_{n-1} \neq m$. Por tanto, $Q(s_1,\ldots,s_{n-1})$ es un polinomio en $x_1,\ldots,x_n$ homogéneo de grado m. Sea $H(x_1,\ldots,x_n) = P(x_1,\ldots,x_n) - Q(s_1,\ldots,s_{n-1})$. Se verifica que H es simétrico y homogéneo de grado m y se anula para $x_n = 0$ (ya que $s_i = s'_i \, mod \, x_n$), luego es múltiplo de x_n y por ser simétrico es múltiplo de $x_1\cdots x_n = s_n$, es decir, $H(x_1,\ldots,x_n) = s_n \cdot \tilde{H}(x_1,\ldots,x_n)$ y, por tanto, $\tilde{H}(x_1,\ldots,x_n)$ es simétrico también y homogéneo de grado $gr(\tilde{H}) = gr(H) - n = gr(P) - n < gr(P)$, luego por recurrencia sobre el grado m de P se concluye que $\tilde{H}(x_1,\ldots,x_n) = \widetilde{Q}(s_1,\ldots,s_n)$. Sustituyendo en la definición de H y despejando se obtiene:

$$P(x_1,\ldots x_n) = Q(s_1,\ldots,s_{n-1}) + s_n \cdot \widetilde{Q}(s_1,\ldots,s_n),$$

con lo que se concluye. □

4. Corolario : *Sea k un cuerpo y $k(x_1,\ldots,x_n)$ es el cuerpo de fracciones del anillo $k[x_1,\ldots,x_n]$. Entonces, se verifica la igualdad:*

$$k(x_1,\ldots,x_n)^{S_n} = k(s_1,\ldots,s_n).$$

Demostración. Sea $\frac{P}{Q} \in k(x_1,\dots,x_n)^{S_n}$. Por ser,

$$\frac{P}{Q} = \frac{\prod_{\sigma\in S_n}\sigma(P)}{Q\cdot\prod_{\mathrm{Id}\neq\sigma\in S_n}\sigma(P)}$$

invariante, al igual que el numerador $\prod_{\sigma\in S_n}\sigma(P)$, se concluye que el denominador $Q\cdot\prod_{\mathrm{Id}\neq\sigma\in S_n}\sigma(P)$ es invariante y, por tanto,

$$\frac{P}{Q} = \frac{\prod_{\sigma\in S_n}\sigma(P)}{Q\cdot\prod_{\mathrm{Id}\neq\sigma\in S_n}\sigma(P)} \in k(s_1,\dots,s_n).$$

□

1.1.2. Teorema fundamental del Álgebra

5. Teorema fundamental del Álgebra: *El cuerpo de los números complejos es un cuerpo algebraicamente cerrado.*

Demostración. Dado un polinomio cualquiera, $0\neq p(x)\in\mathbb{C}[x]$, tenemos que probar que tiene una raíz en $\mathbb{C}$. Basta probar que todo polinomio con coeficientes reales tiene una raíz compleja, porque el producto de $p(x)$ por su conjugado, $q(x) = p(x)\cdot\overline{p(x)}$ es un polinomio con coeficientes reales y si α es una raíz de $q(x)$, entonces α o su conjugada es una raíz de $p(x)$. Si $p(x)\in\mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} p(x) = -\lim_{x\to-\infty} p(x), \quad (\text{y } |\lim_{x\to+\infty} p(x)| = +\infty).$$

Luego por el teorema de Bolzano existe un $\alpha\in\mathbb{R}$ tal que $p(\alpha)=0$. Supongamos que $\mathrm{gr}\,p(x) = r = 2^n\cdot m$, con m impar. Para probar que $p(x)$ tiene una raíz compleja procedamos por inducción sobre n. Para $n=0$ lo hemos probado. Supongamos $n>0$. Sean $\alpha_1,\dots,\alpha_r$ las raíces de $p(x)$ y fijado $\lambda\in\mathbb{R}$ sean $\beta_{ij} := \alpha_i+\alpha_j+\lambda\alpha_i\cdot\alpha_j$. El polinomio $h(x) := \prod_{i<j}(x-\beta_{ij})\in\mathbb{R}[x]$, porque los coeficientes de $h(x)$ son funciones simétricas en $\alpha_1,\dots,\alpha_n$, luego por el teorema de las funciones simétricas, los coeficientes de $h(x)$ son polinomios en los coeficientes de $p(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2} = 2^{n-1}\cdot m'$ con m' impar. Por inducción sobre n, cierto $\beta_{rs} = \alpha_r+\alpha_s+\lambda\alpha_r\cdot\alpha_s\in\mathbb{C}$. Variando el λ fijado (tómese $\binom{r}{2}+1$ distintos), existirán $\lambda\neq\lambda'$, para los que existen r,s, de modo que

$$\alpha_r+\alpha_s+\lambda\alpha_r\cdot\alpha_s,\ \alpha_r+\alpha_s+\lambda'\alpha_r\cdot\alpha_s\in\mathbb{C}.$$

Luego $a := \alpha_r+\alpha_s$ y $b := \alpha_r\cdot\alpha_s\in\mathbb{C}$. Como α_r y α_s son las raíces de $(x-\alpha_r)(x-\alpha_s) = x^2-ax+b$, tenemos que $\alpha_r,\alpha_s = (a\pm\sqrt{a^2-4b})/2\in\mathbb{C}$.

□

1.1.3. Fórmulas de Newton y Girard

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0(x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$.

6. Teorema: *Sea $P'(x)$ la derivada (formal) de $P(x)$ y $\sigma_i = \alpha_1^i + \cdots + \alpha_n^i$ las potencias simétricas en las raíces de $P(x)$ (definimos $\sigma_0 = n$). Se verifica:*

1. $\frac{P'(x)}{P(x)} = \frac{1}{x-\alpha_1} + \cdots + \frac{1}{x-\alpha_n}$.
2. *Fórmula de Girard:* $\frac{P'(x)}{P(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \cdots + \frac{\sigma_i}{x^{i+1}} + \cdots \in k[[\frac{1}{x}]]$.
3. *Fórmulas de Newton:*

$$\begin{aligned}
0 &= a_1 + \sigma_1 a_0 \\
0 &= 2a_2 + \sigma_1 a_1 + a_0\sigma_2 \\
0 &= 3a_3 + \sigma_1 a_2 + \sigma_2 a_1 + \sigma_3 a_3 \\
0 &= na_n + a_{n-1}\sigma_1 + \cdots + a_0\sigma_n \\
&\text{---------} \\
0 &= a_n\sigma_1 + \cdots + a_0\sigma_{n+1} \\
&\cdots \\
0 &= a_n\sigma_i + \cdots + a_0\sigma_{n+i} \\
&\cdots
\end{aligned}$$

Demostración. 1. $P'(x) = \sum_i a_0(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)$, luego

$$P'(x)/P(x) = (\sum_i a_0(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n))/(a_0(x-\alpha_1)\cdots(x-\alpha_n)) = \sum_i 1/(x-\alpha_i)$$

2. Sustituyendo $\frac{1}{x-\alpha_i} = \frac{1}{x}\frac{1}{1-\frac{\alpha_i}{x}} = \frac{1}{x}\sum_j(\frac{\alpha_i}{x})^j$ en la identidad anterior y agrupando en las potencias de $\frac{1}{x}$ se concluye.

3. Resulta de igualar coeficientes en las potencias de x en la identidad $P'(x) = P(x)\cdot\sum_i \frac{\sigma_i}{x^{i+1}}$.

□

7. Nota: *Una fórmula útil en el cálculo de funciones simétricas es la siguiente: Sea $f(x)$ una función racional cuyo denominador es primo con el polinomio mónico $P(x)$ de raíces $\{\alpha_i\}_{i=1}^n$. Se trata de calcular la función simétrica*

$$\sum_i f(\alpha_i).$$

$H(x) := \sum_i f(\alpha_i)\frac{P(x)}{x-\alpha_i}$ coincide con $f(x)P'(x)$ en $k[x]/(P(x))$: Podemos suponer que $P(x)$ es el polinomio genérico de raíces $\alpha_1 = x_1, \ldots, \alpha_n = x_n$ y que k las contiene, en tal caso $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, $\overline{q(x)} \mapsto (q(\alpha_1), \ldots, q(\alpha_n))$ y $H(x) = f(x)P'(x)$ en $k[x]/(P(x))$. De donde igualando el coeficiente en grado $n-1$ obtenemos

$$\boxed{\sum_i f(\alpha_i) = \textit{coeficiente en grado } n-1 \textit{ de } f(x)P'(x) \, mod \, P(x)}$$

1.1.4. El discriminante de un polinomio

Sea $P(x) = \prod_{i=1}^n (x - x_i) = x^n + a_1 x^{n-1} + \cdots + a_n$.

8. Definición: Llamaremos discriminante de P a la función simétrica:

$$\Delta(P) = \prod_{i<j} (x_i - x_j)^2.$$

Por el teorema de las funciones simétricas $\Delta(P)$ es un polinomio en las $a_i = (-1)^i s_i$ con coeficientes en $\mathbb{Z}$. Por tanto, tiene sentido hablar de discriminante de cualquier polinomio mónico con coeficientes en un anillo.

La siguiente proposición es inmediata:

9. Proposición: *El discriminante de un polinomio sobre un cuerpo es cero si y solo si el polinomio tiene alguna raíz doble.*

Sean las funciones simétricas $\sigma_i = x_1^i + \cdots + x_n^i$ (conviniendo que $\sigma_0 = n$). Como sabemos estas funciones se pueden computar recurrentemente a partir de las funciones simétricas elementales usando las fórmulas de Newton o también por la fórmula de Girard:

$$\frac{P'(x)}{P(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \frac{\sigma_2}{x^3} + \cdots$$

10. Teorema: *Se cumple que*

$$\Delta(P) = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

Demostración. Consideremos el determinante de Vandermonde

$$V = \begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

Si hacemos $x_i = x_j$, este determinante se anula, luego V es múltiplo de $\prod_{i<j}(x_i - x_j)$. V es un polinomio homogéneo de grado $n\cdot(n-1)/2$. Además el coeficiente que acompaña a $x_1^0\cdot x_2^1\cdots x_n^{n-1}$ es igual a 1. $\prod_{i<j}(x_i - x_j)$ es homogéneo de grado $n\cdot(n-1)/2$ y el coeficiente que acompaña a $x_1^0\cdot x_2^1\cdots x_n^{n-1}$ es igual a ± 1. Luego, $V = \pm\prod_{i<j}(x_i - x_j)$. Por tanto, $V^2 = \Delta(P(x))$. Ahora bien

$$V^2 = \left|\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} \circ \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_1 & \cdots & x_1^{n-1} \end{pmatrix}\right| = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

□

11. Corolario: *1. El discriminante de $x^2 + ax + b$ es $\Delta = a^2 - 4b$.*

2. El discriminante de $x^3 + px + q$ es $\Delta = -(4p^3 + 27q^2)$.

3. El discriminante de $x^3 + ax^2 + bx + c$ es $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

Demostración. 1. $\sigma_0 = 2, \sigma_1 = -a, \sigma_2 = \sigma_1^2 - 2b = a^2 - 2b$, luego:

$$\Delta = \begin{vmatrix} 2 & -a \\ -a & a^2 - 2b \end{vmatrix} = a^2 - 4b$$

2. $\sigma_0 = 3, \sigma_1 = 0, \sigma_2 = -2p, \sigma_3 = -3q, \sigma_4 = 2p^2$, luego:

$$\Delta = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -(4p^3 + 27q^2)$$

3. Si se hace el cambio $x = y - \frac{1}{3}a$ se obtiene otro polinomio (en y) de grado 3 cuyo segundo coeficiente es cero y cuyas raíces son $\alpha_i + \frac{1}{3}a$, luego como el discriminante es salvo el signo el producto de las diferencias de raíces, y éstas diferencias son las mismas para ambos polinomios, el discriminante es el mismo:

$$P(y - \frac{1}{3}a) = y^3 + (b - \frac{1}{3}a^2)y + (\frac{2}{27}a^3 - \frac{1}{3}ab + c)$$

luego $\Delta = -4(b - \frac{1}{3}a^2)^3 - 27(\frac{2}{27}a^3 - \frac{1}{3}ab + c)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

□

12. Teorema: *1. El discriminante genérico $\Delta = \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[a_1, \ldots, a_n]$ es un polinomio irreducible.*

2. *Consideremos la raíz cuadrada del discriminante,* $\sqrt{\Delta} = \prod_{i<j}(x_i - x_j)$. *Entonces,*

$$\mathbb{Z}_2[x_1,\ldots,x_n]^{A_n} = \mathbb{Z}_2[a_1,\ldots,a_n,\sqrt{\Delta}]$$
$$\mathbb{Q}(x_1,\ldots,x_n)^{A_n} = \mathbb{Q}(a_1,\ldots,a_n,\sqrt{\Delta})$$

donde $\mathbb{Z}_2$ *es la localización de* $\mathbb{Z}$ *por las potencias de 2.*

Demostración. 1. Sea $P(x) = x^n + a_1x^{n-1} + \cdots + a_n$ el polinomio genérico, $p \in \mathbb{Z}$ primo y $\bar{P} \in \mathbb{Z}/p\mathbb{Z}[a_1,\ldots,a_n]$ la clase de P módulo p. Obviamente $\overline{\Delta(P)} = \Delta(\bar{P}) \neq 0$, luego $\Delta = \Delta(P)$ es un polinomio primitivo. Si $\Delta = H_1 \cdot H_2$ con $H_1, H_2 \in \mathbb{Z}[a_1,\ldots,a_n]$ entonces H_1 debe ser divisible por $x_i - x_j$ para alguna pareja i, j. Por ser simétrico (en las variables x_i) resulta que es divisible por $\prod_{i<j}(x_i - x_j) = \sqrt{\Delta}$. Análogamente H_2 es divisible por $\sqrt{\Delta}$ y quedaría $\Delta = (\sqrt{\Delta}\cdot H_1')\cdot(\sqrt{\Delta}\cdot H_2') = \Delta \cdot H_1' \cdot H_2'$, luego H_1', H_2' son constantes (invertibles). Pero $H_1 = \lambda\sqrt{\Delta}$ no es invariante y se llega a contradicción.

2. Por el morfismo del signo se tiene que $S_n/A_n \approx \pm 1$. Si $P \in \mathbb{Z}_2[x_1,\ldots,x_n]^{A_n}$ es invariante por A_n y σ es tal que $S_n/A_n = <\bar{\sigma}>$ (es decir, $\text{sign}(\sigma) = -1$), entonces:

$$P = \frac{1}{2}((P + \sigma(P)) + (P - \sigma(P)))$$

y basta ver que $Q^+ := P + \sigma(P) \in \mathbb{Z}_2[a_1,\ldots,a_n]$ y $Q^- := P - \sigma(P) \in \sqrt{\Delta}\cdot\mathbb{Z}_2[a_1,\ldots,a_n]$. Lo primero resulta de que $Q^+ = P + \sigma(P)$ es invariante. Para lo segundo se observa que Q^- es invariante por A_n y $\sigma(Q^-) = -Q^-$. Por tanto, la fracción $\frac{Q^-}{\sqrt{\Delta}}$ es invariante, luego es $\frac{Q^-}{\sqrt{\Delta}} = \frac{S}{T}$ con $S, T \in \mathbb{Z}_2[a_1,\ldots,a_n]$ primos entre sí. Ahora teniendo en cuenta que $(Q^-)^2$ es invariante, que Δ es irreducible y que $\frac{(Q^-)^2}{\Delta} = \frac{S^2}{T^2}$ se concluye que T^2 es invertible, luego T es invertible y $T = \pm 2^n$ con $n \in \mathbb{Z}$. Por tanto,

$$Q^- = \pm\frac{1}{2^n}S\cdot\sqrt{\Delta} \in \sqrt{\Delta}\cdot\mathbb{Z}_2[a_1,\ldots,a_n].$$

La segunda igualdad se prueba análogamente, pues si una función racional Q^- invariante por A_n verifica que $\sigma(Q^-) = -Q^-$, entonces $\frac{Q^-}{\sqrt{\Delta}}$ es simétrica y, por tanto, $\frac{Q^-}{\sqrt{\Delta}} \in \mathbb{Q}(a_1,\ldots,a_n)$ y $Q^- = \sqrt{\Delta}\cdot\frac{Q^-}{\sqrt{\Delta}} \in \sqrt{\Delta}\cdot\mathbb{Q}(a_1,\ldots,a_n)$. Ahora se procede como en el caso anterior.

□

Caso real: $k = \mathbb{R}$

13. Teorema: *Si* $P(x) \in \mathbb{R}[x]$, *entonces*

1. $\Delta(P) = 0$ *si y solo si* $P(x)$ *tiene una raíz doble.*

2. $\Delta(P) < 0$ *si y solo si las raíces de* $P(x)$ *son distintas y tiene un número impar de parejas de raíces complejas no reales.*

3. $\Delta(P) > 0$ *si y solo si las raíces de* $P(x)$ *son distintas y tiene un número par de parejas de raíces complejas no reales.*

Demostración. 1. Es la Proposición 1.1.9.

2. y 3.: $\Delta(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Para cada pareja de raíces distintas $\{\alpha_i, \alpha_j\}$, pueden darse dos casos: (1) que el par no sea invariante por conjugación, es decir, $\{\alpha_i, \alpha_j\} \neq \{\overline{\alpha}_i, \overline{\alpha}_j\}$, en cuyo caso agrupándolos es $(\alpha_i - \alpha_j)^2 \cdot (\overline{\alpha}_i - \overline{\alpha}_j)^2 = |\alpha_i - \alpha_j|^2 > 0$ y no altera el signo del discriminante. (2) $\{\alpha_i, \alpha_j\} = \{\overline{\alpha}_i, \overline{\alpha}_j\}$, es decir: (A) $\alpha_i = \overline{\alpha}_i, \alpha_j = \overline{\alpha}_j$ ó (B) $\alpha_j = \overline{\alpha}_i$. En el caso (A), las dos raíces son reales y, por tanto, $(\alpha_i - \alpha_j)^2 > 0$ y no altera el signo del discriminante. En el caso (B), es un par de raíces complejas conjugadas (no reales), y resulta $(\alpha_i - \overline{\alpha}_i)^2 = (2i\,Im(\alpha_i))^2 = -4\,Im(\alpha_i)^2 < 0$.

□

1.2. Separación de raíces

1.2.1. Acotación de las raíces

1. Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$. Queremos encontrar un número real $L > 0$, que llamaremos cota (de las raíces) de $P(x)$, de modo que si $\alpha \in \mathbb{C}$ es una raíz de $P(x)$ entonces $|\alpha| < L$.

Cota de MacLaurin: Una cota de $P(x)$ es $L = 1 + \text{máx}\{|a_1|, \ldots, |a_n|\}$, porque si $|z| \geq L$,

$$|P(z)| \geq |z|^n - |a_1||z|^{n-1} - \cdots - |a_n| \geq |z|^n - (|z|-1)|z|^{n-1} - \cdots - (|z|-1) = 1.$$

2. Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{R}[x]$. Queremos encontrar un número real L, que llamaremos cota superior (de las raíces reales) de $P(x)$, de modo que si $r \in \mathbb{R}$ es una raíz de $P(x)$ entonces $r < L$.

Cota superior de Newton: Si $P(a), P'(a), \ldots, P^{n)}(a) \geq 0$, entonces $L = a$ es una cota superior: $P(x) = \sum_{i=0}^{n} P^{i)}(a)\frac{(x-a)^i}{i!}$, luego $P(r) > 0$, para todo $r \geq a$.

Cota superior de Lagrange: Sea $N = \text{máx}\{|a_i| : a_i \leq 0\}$. Si a_s es el primer coeficiente negativo, una cota superior de $P(x)$ es $L = 1 + \sqrt[s]{N}$, porque si $r \geq L$,

$$P(r) = r^n + a_1 r^{n-1} + \cdots + a_n \geq r^n - (r-1)^s r^{n-s} - \cdots - (r-1)^s = r^n - \frac{(r-1)^s r^{n-s+1} - (r-1)^s}{r-1}$$
$$= r^n - (r-1)^{s-1} \cdot (r^{n-s+1} - 1) > r^n - r^{s-1} \cdot r^{n-s+1} = 0.$$

Observación Se dice que $I \in \mathbb{R}$ es una cota inferior (de las raíces reales) de $P(x) \in \mathbb{R}[x]$, si I es menor o igual que toda raíz real de $P(x)$. I es una cota inferior de $P(x)$ si y solo si $-I$ es una cota superior de $P(-x)$.

1.2.2. Exceso de una función racional real

En esta sección los polinomios considerados son con coeficientes reales.

Sea una función racional $f(x) = \frac{P(x)}{Q(x)}$ (con P y Q primos entre sí). Diremos que $f(x)$ tiene un polo en $a \in \mathbb{R}$ cuando a sea raíz de Q. Diremos que la multiplicidad de f en el polo a es n si ésta es la multiplicidad de a como raíz de Q.

Escribamos $f(x) = \tilde{f}(x) \cdot \frac{1}{(x-a)^n}$ siendo n la multiplicidad de f en el polo a y $0 \neq \tilde{f}(a) \in \mathbb{R}$.

3. Definición: Llamaremos exceso de $f(x) = \frac{P(x)}{Q(x)}$ en $a \in \mathbb{R}$, al número:

$$E_a(f) = \begin{cases} 0 \text{ si } f(x) \text{ no tiene polo en } a \text{ o es de multiplicidad par} \\ 1 \text{ si } f(x) \text{ tiene polo de multiplicidad impar y } \tilde{f}(a) > 0 \\ -1 \text{ si } f(x) \text{ tiene polo de multiplicidad impar y } \tilde{f}(a) < 0 \end{cases}$$

De otro modo: si $f(x)$ pasa de $-\infty$ a ∞ al pasar x por a de izquierda a derecha el exceso es 1; si $f(x)$ pasa de ∞ a $-\infty$ al pasar x por a de izquierda a derecha el exceso es -1 y es cero en cualquier otro caso.

4. Definición: Dados $a, b \in \mathbb{R}$ y $f(x)$ una función racional llamaremos exceso de $f(x)$ entre a y b a la suma de los excesos de $f(x)$ en sus polos contenidos en (a, b):

$$E_a^b(f) = \sum_{t \in (a,b)} E_t(f).$$

5. Evidentemente, si $a < c < b$ y $f(x)$ no tiene polos en c, entonces

$$E_a^b(f) = E_a^c(f) + E_c^b(f).$$

Si f y g son dos funciones racionales sin polos comunes en (a, b) entonces

$$E_a^b(f + g) = E_a^b(f) + E_a^b(g).$$

Si P es un polinomio entonces $E_a^b(P) = 0$.

Veamos qué relación hay entre las raíces de un polinomio y el exceso.

6. Proposición: *Sean $a<b$ números reales y $P\in\mathbb{R}[x]$. Entonces,*

$$E_a^b(\frac{P'}{P}) = N^o \text{ de raíces reales distintas de } P \text{ en } (a,b).$$

Demostración. Sean $\alpha_1,\dots,\alpha_r$ las raíces complejas (distintas) de P. Entonces $P(x) = a_0\cdot\prod_{i=1}^{r}(x-\alpha_i)^{n_i}$ y $P'(x) = a_0\cdot\sum_{i=1}^{r} n_i\cdot(x-\alpha_i)^{n_i-1}\prod_{j\neq i}(x-\alpha_j)^{n_j}$ y

$$\frac{P'}{P} = \sum_i \frac{n_i}{x-\alpha_i}.$$[1]

Por tanto, si α_i es real, entonces $E_{\alpha_i}\frac{P'}{P} = 1$. Luego, el número de raíces distintas en (a,b) coincide con $E_a^b\frac{P'}{P}$.

□

Por tanto, el cálculo del número de raíces de P se reduce al cálculo de $E_a^b(\frac{P'}{P})$. El teorema 1.2.9 (y su corolario: el teorema de Sturm) resolverá este problema.

Dado un número real no nulo $r\in\mathbb{R}$, diremos que $\operatorname{sign}(r)=1$ si $r>0$ y $\operatorname{sign}(r)=-1$ si $r<0$.

7. Definiciones: Dados dos números reales no nulos a,b se define

$$V(a,b) := \begin{cases} 1 \text{ si } \operatorname{sign} a \neq \operatorname{sign} b \\ 0 \text{ si } \operatorname{sign} a = \operatorname{sign} b \end{cases}$$

Dados números reales no nulos $a_1,\dots,a_n$ llamaremos variaciones de signo de dicha sucesión al número:

$$V(a_1,\dots,a_n) := \sum_{i=1}^{r} V(a_i,a_{i+1}),$$

Si algunos términos a_i (con $1<i<n$) son nulos se define las variaciones de signo $V(a_1,\dots,a_n)$ suprimiendo los términos nulos. Por ejemplo,

$$V(1,0,0,-1,0,3,1) = V(1,-1,3,1) = 2.$$

Dados dos números reales a,b y n polinomios reales $P_1,\dots,P_n$ (supongamos que P_1 y P_n no se anulan en a ni en b), definimos

$$V_a^b(P_1,\dots,P_n) := V(P_1(a),\dots,P_n(a)) - V(P_1(b),\dots,P_n(b)).$$

[1] De otro modo: $\frac{P'}{P} = (\ln P)' = (\sum_i n_i \ln(x-\alpha_i))' = \sum_i \frac{n_i}{x-\alpha_i}$.

8. Evidentemente, dados tres números reales a,b,c (suponemos que P_1 y P_n no se anulan en a, ni en b ni en c) se cumple que

$$V_a^b(P_1,\ldots,P_n) = V_a^c(P_1,\ldots,P_n) + V_c^b(P_1,\ldots,P_n).$$

9. Teorema : *Sean $a<b$ dos números reales y P,Q dos polinomios reales que no se anulan en a ni en b, entonces*

$$E_a^b(\frac{P}{Q}) + E_a^b(\frac{Q}{P}) = V_a^b(P,Q).$$

Demostración. Se puede suponer que P y Q son primos entre sí, pues los factores comunes se pueden suprimir sin que altere la fórmula. Sean $a = a_1 < a_2 < \cdots < a_n = b$ tales que $P\cdot Q$ tiene a lo más una raíz (múltiple o no) en (a_i,a_{i+1}) y $(P\cdot Q)(a_i)\neq 0$, para todo i. Basta probar que

$$E_{a_i}^{a_{i+1}}(\frac{P}{Q}) + E_{a_i}^{a_{i+1}}(\frac{Q}{P}) = V_{a_i}^{a_{i+1}}(P,Q),$$

para todo i, por 1.2.5 y 1.2.8. Intercambiando P por Q si es necesario, podemos suponer que P no tiene raíces en (a_i,a_{i+1}), luego $E_{a_i}^{a_{i+1}}(\frac{Q}{P})=0$. Cambiando P y Q por $-P$ y $-Q$ podemos suponer que $P>0$ en (a_i,a_{i+1}). Tenemos

$$E_{a_i}^{a_{i+1}}(\frac{P}{Q}) + E_{a_i}^{a_{i+1}}(\frac{Q}{P}) = E_{a_i}^{a_{i+1}}(\frac{P}{Q}) \overset{*}{=} V_{a_i}^{a_{i+1}}(P,Q),$$

donde $\overset{*}{=}$ es fácil de probar. □

10. Sea $P(x)\in\mathbb{R}[x]$ y supongamos que $P'(x)$ no tiene raíces en (a,b) y que $P(a)\cdot P(b)\neq 0$. Entonces,

$$\text{N}^\text{o} \text{ de raíces de } P(x) \text{ en } (a,b) = E_a^b(\frac{P'}{P}) = |E_a^b(\frac{1}{P})| = |V_a^b(P,1)| = V(P(a),P(b))$$

De otro modo: $P(x)$ es estrictamente creciente (o decreciente) en el intervalo (a,b), luego tendrá una (resp. ninguna) raíz si $V(P(a),P(b))=1$ (resp. $V(P(a),P(b))=0$).

Si $P(x)$ no tiene raíces múltiples, entonces las raíces reales de $P'(x)$ separan las raíces reales de $P(x)$. La dificultad está en el cálculo de las raíces α_i de $P'(x)$ (y en el cálculo de $P(\alpha_i)$).

1.2.3. Teorema de Sturm

Veamos que el teorema anterior nos da un modo de calcular, vía el algoritmo de Euclides, el exceso de una función racional y por ende un modo de calcular el número de raíces de un polinomio en un intervalo.

Sean P,Q dos polinomios con coeficientes reales y consideremos los restos R_i obtenidos en el algoritmo de Euclides (cambiados de signo):

$$\begin{aligned} P &= C_1Q - R_1\\ Q &= C_2R_1 - R_2\\ &\cdots\\ R_{n-2} &= C_nR_{n-1} - R_n\\ R_{n-1} &= C_{n+1}R_n \end{aligned}$$

Se dice que los $\{R_i\}$ son los restos de Sturm de P y Q.

11. Teorema : *Sean $a<b$ dos números reales, P,Q dos polinomios con coeficientes reales y supongamos que P no se anula en a ni en b, entonces:*

$$E_a^b\frac{Q}{P} = V_a^b(P,Q,R_1,\ldots,R_n).$$

Demostración. (1) Supongamos que Q y los restos de Sturm no se anulan en a ni en b.

Procedamos por inducción sobre n. Para $n=0$, es decir, P es múltiplo de Q, $E_a^b\frac{Q}{P} \overset{1.2.9}{=} V_a^b(P,Q) - E_a^b\frac{P}{Q} = V_a^b(P,Q)$. Sea $n>0$. De la igualdad $P = C_1Q - R_1$ se obtiene $\frac{P}{Q} = C_1 - \frac{R_1}{Q}$, luego $E_a^b\frac{P}{Q} = -E_a^b\frac{R_1}{Q}$. Aplicando esta igualdad e inducción se obtiene:

$$\begin{aligned} E_a^b\frac{Q}{P} &\overset{1.2.9}{=} V_a^b(P,Q) - E_a^b\frac{P}{Q} = V_a^b(P,Q) + E_a^b\frac{R_1}{Q}\\ &= V_a^b(P,Q) + V_a^b(Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n). \end{aligned}$$

(2) Supongamos que $Q =: R_0$ o algún resto de Sturm se anula en a o en b.

Se observa que no puede haber dos términos consecutivos $R_i(a) = R_{i+1}(a) = 0$, pues entonces $x-a$ sería divisor del máximo común divisor de R_i y R_{i+1}, y por tanto de P, contradiciendo la hipótesis del teorema. Igualmente, no puede ser que $R_i(b) = R_{i+1}(b) = 0$. Por la misma razón $R_n(a)\neq 0$ y $R_n(b)\neq 0$. Por otro lado, si $R_i(a)=0$, como $R_{i-1} = C_{i+1}R_i - R_{i+1}$, se tiene que $R_{i-1}(a)$ y $R_{i+1}(a)$ son de signo contrario. Igualmente, si $R_i(b)=0$, entonces $R_{i-1}(b)$ y $R_{i+1}(b)$ son de signo contrario.

Modifiquemos $a \rightsquigarrow a' = a+\epsilon$ y $b \rightsquigarrow b' = b-\epsilon$ ligeramente de manera que: $E_a^b\frac{Q}{P} = E_{a'}^{b'}\frac{Q}{P}$, $R_i(a')\neq 0$ (y $R_i(b')\neq 0$) para todo i, y $\operatorname{sign}(R_j(a)) = \operatorname{sign}(R_j(a'))$ cuando $R_j(a)\neq 0$ (y $\operatorname{sign}(R_j(b)) = \operatorname{sign}(R_j(b'))$ cuando $R_j(b)\neq 0$). Si $R_i(a)=0$ entonces

$$V(R_{i-1}(a'),R_i(a'),R_{i+1}(a')) = 1 = V(R_{i-1}(a),R_{i+1}(a)) = V(R_{i-1}(a),R_i(a),R_{i+1}(a)),$$

ya que $\operatorname{sign}(R_{i-1}(a')) = \operatorname{sign}(R_{i-1}(a)) = -\operatorname{sign}(R_{i+1}(a)) = -\operatorname{sign}(R_{i+1}(a'))$. Igualmente, si $R_i(b) = 0$ entonces $V(R_{i-1}(b'),R_i(b'),R_{i+1}(b')) = V(R_{i-1}(b),R_i(b),R_{i+1}(b))$. Por tanto,

$$E_a^b\frac{Q}{P} = E_{a'}^{b'}\frac{Q}{P} \overset{(1)}{=} V_{a'}^{b'}(P,Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n).$$

□

12. Teorema de Sturm: *Sean $a < b$ dos números reales, P un polinomio con coeficientes reales que no se anula en a ni en b y $\{R_1,\ldots,R_n\}$ los restos de Sturm para P y su derivada P'. Entonces,*

$$N^o \text{ de raíces reales distintas de } P \text{ en } (a,b) = V_a^b(P,P',R_1,\ldots,R_n).$$

Demostración. Es consecuencia del teorema anterior y la proposición 1.2.6.

□

13. Una vez que sabemos que todas las raíces reales de $P(x)$ están incluidas en un intervalo (a,b), el teorema de Sturm nos da el procedimiento para separarlas[2]: Consideremos los intervalos $(a,\frac{a+b}{2})$ y $(\frac{a+b}{2},b)$ (supongamos por sencillez que $P((a+b)/2) \neq 0$). Por el teorema de Sturm sabemos calcular el número de raíces reales de $P(x)$ en cada uno de los dos intervalos. Dividiendo sucesivamente en dos los intervalos que contengan raíces consiguiremos determinar los intervalos en los que hay una única raíz (múltiple o no).

14. Si $P(x)$ tiene una única raíz en (a,b) (contando multiplicidades) y $P(a),P(b) \neq 0$, entonces $1 = |E_a^b(\frac{1}{P})| = |V_a^b(P,1)| = V(P(a),P(b))$.

15. Si $V(P(a),P(b)) = 1$ y $P(a),P(b) \neq 0$, entonces por el teorema de Bolzano, existe una raíz de $P(x)$ en el intervalo (a,b). Consideremos los intervalos $(a,\frac{a+b}{2})$ y $(\frac{a+b}{2},b)$ (supongamos por sencillez que $P((a+b)/2) \neq 0$). Entonces, o $V(P(a),P(\frac{a+b}{2})) = 1$, o bien $V(P(\frac{a+b}{2}),P(b)) = 1$. De nuevo, $P(x)$ tiene una raíz en $(a,\frac{a+b}{2})$, o bien en $(\frac{a+b}{2},b)$. Reiterando este proceso calcularemos aproximadamente una raíz de $P(x)$ en (a,b). Existen otros métodos de aproximación, como el método de aproximación de Newton o *regula falsi* que el lector conocerá del Análisis Numérico.

16. Si sabemos calcular las raíces reales de un polinomio real entonces sabemos calcular las raíces reales de un polinomio complejo: Sea $P(x) \in \mathbb{C}[x]$ y consideremos el producto de este polinomio por su conjugado, $Q(x) = P(x)\cdot\overline{P(x)} \in \mathbb{R}[x]$ (o consideremos

[2]No hacemos un análisis de la dificultad intrínseca del cálculo de los polinomios de Sturm.

$Q(x) = m.c.d.(P(x), \overline{P(x)}) \in \mathbb{R}[x]$). Las raíces reales de $P(x) \in \mathbb{C}[x]$ coinciden con las raíces reales de $Q(x) \in \mathbb{R}[x]$.

17. Observación: Sean P y Q primos entre sí, supongamos que P no se anula en a ni en b y sea $r_a^b(P)$ el número de raíces reales de P (contadas con su multiplicidad) en (a,b). Entonces,

$$\pm E_a^b \frac{Q}{P} \leq r_a^b(P).$$

Además, como $1 = -1 \, mod \, 2$, se cumple la igualdad $E_a^b \frac{Q}{P} = r_a^b(P) \, mod \, 2$.

18. Teorema de Budan-Fourier: *Sea P un polinomio con coeficientes reales de grado n que no se anula en a ni en b, y r_a^b el número de raíces reales de P en $[a,b]$ (contadas con su multiplicidad).. Se cumple la acotación:*

$$r_a^b(P) \leq V_a^b(P, P', P'', \ldots, P^{n)}),$$

Además esta desigualdad es una igualdad módulo 2.

Demostración. Procedemos por recurrencia sobre el grado n del polinomio P. Si $n = 1$ entonces $r_a^b(P) \overset{1.2.12}{=} V_a^b(P, P')$.

(1) Supongamos que todas las raíces reales de P son simples y que P y sus derivadas iteradas no se anulan en a ni en b. Entonces,

$$\begin{aligned} r_a^b(P) &\overset{1.2.6}{=} E_a^b \frac{P'}{P} \overset{1.2.9}{=} V_a^b(P, P') - E_a^b \frac{P}{P'} \leq V_a^b(P, P') + r_a^b(P') \\ &\leq V_a^b(P, P') + V_a^b(P', P'', \ldots, P^{n)}) = V_a^b(P, P', P'', \ldots, P^{n)}). \end{aligned}$$

Las desigualdades son igualdades módulo 2 por serlo la primera (por la observación 1.2.17) y serlo la segunda por recurrencia.

(2) Supongamos ahora que P y sus derivadas iteradas no se anulan en a ni en b. Sustituyendo cada factor $(x-\alpha_i)^{s+1}$ de P (con $\alpha_i \in \mathbb{R}$) por $(x-\alpha_i)(x-\alpha_i-\epsilon)\cdots(x-\alpha_i-s\epsilon)$ con ϵ pequeño, se obtiene otro polinomio Q con raíces simples tal que $r_a^b Q = r_a^b P$ y $V_a^b(Q, Q', Q'', \ldots, Q^{n)}) = V_a^b(P, P', P'', \ldots, P^{n)})$. Por tanto,

$$r_a^b(P) = r_a^b Q \overset{(1)}{\leq} V_a^b(Q, Q', Q'', \ldots, Q^{n)}) = V_a^b(P, P', P'', \ldots, P^{n)})$$

y se cumple la igualdad módulo 2.

(3) Por último, supongamos que alguna derivada iterada de P se anula en a (igualmente en b). Vamos a ver que cambiando infinitesimalmente a (y b), estamos en las

condiciones de (2) y no cambia el número de raíces de P (evidentemente) ni el número de las variaciones de signo de P y sus derivadas iteradas. Haciendo el cambio de variable $x' = x - a$ se puede suponer $a = 0$. Haciendo el cambio $a = 0 \rightsquigarrow a = \epsilon > 0$ se puede suponer que $\operatorname{sign}(P^{i)}(0) = \operatorname{sign}(P^{i)}(\epsilon))$, para todo ϵ pequeño, cuando $P^{i)}(0) \neq 0$. Supongamos que

$$P^{i-1)}(0) \neq 0, \quad P^{i)}(0) = \cdots = P^{i+h-1)}(0) = 0, \quad P^{i+h)}(0) \neq 0.$$

Entonces es $P^{i)}(x) = x^h(\mu + \gamma x + \cdots)$ y por tanto $P^{i+r)}(x) = c_r x^{h-r}(\mu + \gamma' x + \cdots)$ (siendo $c_r = h(h-1)\cdots(h-r+1) > 0$) para $r \leq h$. Por tanto, para ϵ suficientemente pequeño y $r \leq h$ es $\operatorname{sign} P^{i+r)}(\epsilon) = \operatorname{sign}\mu$, de donde

$$\begin{aligned} &V(P^{i-1)}(\epsilon), P^{i)}(\epsilon), \ldots, P^{i+h-1)}(\epsilon), P^{i+h)}(\epsilon)) = V(P^{i-1)}(\epsilon), \mu, \ldots, \mu, \mu) \\ &= V(P^{i-1)}(0), 0, \ldots, 0, P^{i+h)}(0)) = V(P^{i-1)}(0), P^{i)}(0), \ldots, P^{i+h-1}(0), P^{i+h)}(0)). \end{aligned}$$

Luego, $V(P(\epsilon), P'(\epsilon), \ldots, P^{n)}(\epsilon)) = V(P(0), P'(0), \ldots, P^{n)}(0))$ y se concluye. □

19. Teorema de Descartes: *Sea $P(x) = a_0 x^n + \cdots a_{n-1}x + a_n$ un polinomio con coeficientes reales de grado n sin la raíz 0 (i.e. $a_n \neq 0$). Entonces,*

$$r_0^{+\infty}(P) \leq V(a_0, a_1, \ldots, a_n)$$

y es una igualdad módulo 2 (es decir, ambos números tienen la misma paridad).

Demostración. Basta aplicar el teorema de Budan-Fourier teniendo en cuenta que $a_i = P^{n-i)}(0)/(n-i)!$ y que $\operatorname{sign} P^{i)}(+\infty) = \operatorname{sign} a_0$ (es decir, no depende de i y, por tanto, sus variaciones son nulas).

□

Haciendo el cambio $x \mapsto -x$ y aplicando el teorema de Descartes se concluye que

$$r_{-\infty}^{0}(P(x)) = r_0^{+\infty}(P(-x)) \leq V(a_0, -a_1, \ldots, (-1)^n a_n)$$

y es una igualdad módulo 2.

20. Corolario: *Si todas las raíces de P son reales (y no nulas), entonces:*

$$r_0^{+\infty}(P) = V(a_0, a_1, \ldots, a_n) \quad y \quad r_{-\infty}^{0}(P) = V(a_0, -a_1, \ldots, (-1)^n a_n)$$

y además $P(x)$ no puede tener dos coeficientes consecutivos nulos.

Demostración. Por el teorema de Descartes,

$$n = r_0^{+\infty}(P) + r_{-\infty}^0(P) \leq V(a_0, a_1, \ldots, a_n) + V(a_0, -a_1, \ldots, (-1)^n a_n)$$

Es fácil ver que el último sumando es siempre menor o igual que n, y que si es n no puede haber dos coeficientes consecutivos nulos. Ahora es fácil concluir. □

Este corolario se usa en Álgebra Lineal para determinar cuándo una métrica simétrica es euclídea: Todos los autovalores de las matrices simétricas con coeficientes reales son reales, y la matriz simétrica es euclídea si y solo si todos los autovalores son estrictamente positivos. Por el corolario, la métrica simétrica es euclídea si y solo si $V(a_0, a_1, \ldots, a_n) = n$, donde $P(x) = a_0 x^n + \cdots + a_{n-1} x + a_n$ es el polinomio característico asociado a la matriz.

1.2.4. Número de raíces complejas en un rectángulo

Orientemos S^1 en sentido anti-horario. Dados $a, b \in S^1$ denotemos $[a, b]$ el arco bien orientado de S^1 que empieza en a y acaba en b.

Sea $f : [a, b] \to S^1 = \mathbb{R} \coprod \infty$ una función continua tal que $f^{-1}(\infty)$ sea unión de un número finito (o nulo) de intervalos cerrados.

Sea $p \in (a, b)$. Si p es un polo aislado de f, es decir, p es un abierto de $f^{-1}(\infty)$, definimos $E_p(f)$ del modo usual: $E_p(f) = 1$ si $\lim_{x \to p^-} f(x) = -\infty$ y $\lim_{x \to p^+} f(x) = +\infty$, etc. Si $[p, b] \cap f^{-1}(\infty)$ es un abierto de $f^{-1}(\infty)$, diremos que $E_p(f) = \frac{1}{2}$ si $\lim_{x \to p^-} f(x) = -\infty$ y diremos que $E_p(f) = \frac{-1}{2}$ si $\lim_{x \to p^-} f(x) = +\infty$. Si $[a, p] \cap f^{-1}(\infty)$ es un abierto de $f^{-1}(\infty)$, diremos que $E_p(f) = \frac{1}{2}$ si $\lim_{x \to p^+} f(x) = +\infty$ y diremos que $E_p(f) = \frac{-1}{2}$ si $\lim_{x \to p^+} f(x) = -\infty$. Si p no es un polo o $f^{-1}(\infty)$ es un entorno de p, entonces diremos que $E_p(f) = 0$.

Dado un intervalo $[a, b]$, tal que a y b no son polos, se define $E_a^b(f) = \sum_{p \in [a,b]} E_p(f)$. Si $c \in [a, b]$ no es un polo, entonces $E_a^b(f) = E_a^c(f) + E_a^c(f)$. Si f y g no tienen polos comunes, entonces $E_a^b(f + g) = E_a^b(f) + E_a^b(g)$ Por último, argumentando como la demostración de teorema 1.2.9, tenemos que

$$E_a^b(f) + E_a^b(\frac{1}{f}) = V_a^b(f, 1)$$

(f sin polos ni ceros en a y b, $f^{-1}(0)$ como $f^{-1}(\infty)$ es igual a un número finito de intervalos cerrados). Por tanto, si $[a, b] = S^1$ entonces

$$E_{S^1}(f) + E_{S^1}(\frac{1}{f}) = 0.$$

21. Definición: Llamaremos **curva racional** en $\mathbb{C}$ a cualquier aplicación continua

$$\sigma\colon [a,b]\to\mathbb{C}$$

definida a trozos por funciones racionales, es decir, una aplicación continua $\sigma(t)=u(t)+iv(t)$ tal que existen un número finito de números reales $a=a_0<a_1<\cdots<a_n=b$ de manera que las funciones u,v en cada intervalo $[a_i,a_{i+1}]$ son de la forma $u(t)=\frac{P_i(t)}{Q_i(t)}$ y $v(t)=\frac{S_i(t)}{H_i(t)}$ con $P_i(t),Q_i(t),S_i(t),H_i(t)$ polinomios. Diremos que es **circuito** cuando $\sigma(a)=\sigma(b)$.

Es claro que la unión de dos curvas racionales (a trozos) tal que la segunda empieza en el punto donde termina la primera, es otra curva racional.

22. Ejemplos: Las circunferencias son circuitos. En efecto: basta ver que las semicircunferencias son curvas racionales, pues la circunferencia es unión de dos semicircunferencias. Sea (c_1,c_2) el centro y $r\in\mathbb{R}^+$ el radio de una circunferencia. Consideremos el haz de rectas que pasan por el punto de la circunferencia $p_1=(c_1+r,c_2)$, es decir, $y=t(x-c_1-r)+c_2$. Para cada pendiente t, la correspondiente recta, corta a la circunferencia en un único punto (aparte de p_1). Computando dicho punto es:

$$(r\frac{t^2-1}{t^2+1}+c_1, r\frac{-2t}{t^2+1}+c_2).$$

Luego para $t\in[-1,1]$ parametriza la semicircunferencia correspondiente a su cara izquierda (es decir, tales que $x\le c_1$).[3]

Otro ejemplo trivial es un segmento en $\mathbb{C}$ (usando las ecuaciones paramétricas de las rectas). Por tanto, cualquier polígono es un circuito.

23. Definición: Diremos que una curva σ pasa por un punto $z\in\mathbb{C}$ cuando $z\in\operatorname{Im}\sigma$.

24. Definición: Dado un circuito $\sigma\colon[a,b]\to\mathbb{C}$, $\sigma(t)=u(t)+iv(t)$ que no pasa por el origen, llamaremos número de vueltas alrededor del origen (en el sentido de las agujas del reloj) al número

$$\mathrm{v}(\sigma)=\frac{1}{2}E_a^b\frac{v(t)}{u(t)}.$$

25. Observaciones: (1) El exceso de la fracción $\frac{v(t)}{u(t)}$ es 1 en $t=t_0$ cuando se anula u (es decir la curva corta el eje OY) y la fracción pasa de negativa a positiva, es decir: (i) si $v(t_0)$ es negativo, entonces u pasa de positivo a negativo (o equivalentemente,

[3] Podemos considerar $t\in(-\infty,\infty)$, que parametriza la circunferencia (salvo el punto (c_1+r,c_2)) y para $t\to\pm\infty$ obtenemos el punto (c_1+r,c_2).

$\sigma(t)$ pasa del cuarto cuadrante al tercero); (ii) si $v(t_0)$ es positivo u pasa de negativo a positivo (es decir $\sigma(t)$ pasa del segundo cuadrante al primero). Por tanto es claro que cada vez que la curva da una vuelta alrededor del origen el exceso es 2 y de ahí la definición.

(2) Análogamente se puede definir $\mathrm{v}(\sigma) = -\frac{1}{2}E_a^b \frac{u(t)}{v(t)}$ contabilizando el número de cortes con el eje OX. En efecto, ambos números coinciden, pues como sabemos

$$E_a^b \frac{v(t)}{u(t)} + E_a^b \frac{u(t)}{v(t)} = V_a^b(u,v) = V(u(a),v(a)) - V(u(b),v(b)) = 0,$$

porque $u(a) = u(b), v(a) = v(b)$.

(3) Realmente, en el número de vueltas lo que se cuenta es el número de vueltas en el sentido de las agujas del reloj menos el número de vueltas en sentido contrario.

26. Lema : *Si $\sigma_1(t), \sigma_2(t)\colon [a,b] \to \mathbb{C}$ son dos circuitos (que no pasan por el origen), entonces el número de vueltas de $\sigma_1(t)\cdot\sigma_2(t)$ es igual a la suma de las vueltas que da cada uno de ellos:*

$$v(\sigma_1(t)\cdot\sigma_2(t)) = v(\sigma_1(t)) + v(\sigma_2(t)).$$

Demostración. Supongamos que $\sigma_1(t), \sigma_2(t)$ no cortan simultáneamente al eje OX para ningún valor de t. Escribamos el número de vueltas por $\mathrm{v}(\sigma(t)) = -\frac{1}{2}E_a^b \frac{u(t)}{v(t)} = \frac{1}{2}E_a^b f(t)$ (siendo $\sigma(t) = u(t) + v(t)i$ y $f(t) = -\frac{u(t)}{v(t)}$). Se verifica que la parte real e imaginaria de $\sigma_1(t)\cdot\sigma_2(t)$ es $u_1u_2 - v_1v_2$ y $u_1v_2 + v_1u_2$ y por tanto el número de vueltas es

$$\mathrm{v}(\sigma_1(t)\cdot\sigma_2(t)) = -\frac{1}{2}E_a^b \frac{u_1u_2 - v_1v_2}{u_1v_2 + v_1u_2} = -\frac{1}{2}E_a^b \frac{\frac{u_1}{v_1}\frac{u_2}{v_2} - 1}{\frac{u_1}{v_1} + \frac{u_2}{v_2}} = \frac{1}{2}E_a^b \frac{f_1f_2 - 1}{f_1 + f_2}.$$

Ahora bien, si f_1 ó f_2 tiene polo en un punto t_0, la fracción $\frac{f_1f_2-1}{f_1+f_2}$ no tiene polo en t_0 (toma el valor finito $f_2(t_0)$ ó $f_1(t_0)$ respectivamente), luego los polos se dan exactamente cuando se anula el denominador, es decir, cuando $f_1(t_0) = -f_2(t_0)$ y en tales puntos el numerador es estrictamente negativo ($f_1(t_0)f_2(t_0) - 1 = -f_1(t_0)^2 - 1 < 0$), es decir,

$$\frac{1}{2}E_a^b \frac{f_1f_2 - 1}{f_1 + f_2} = -\frac{1}{2}E_a^b \frac{1}{f_1 + f_2} = \frac{1}{2}E_a^b(f_1 + f_2) = \frac{1}{2}E_a^b f_1 + \frac{1}{2}E_a^b f_2 = \mathrm{v}(\sigma_1(t)) + \mathrm{v}(\sigma_2(t)).$$

En particular, si $\sigma_2(t) = cte =: z$ entonces $v(\sigma_1(t)) = v(\sigma_1(t)\cdot z)$. En el caso de que $\sigma_1(t), \sigma_2(t)$ corten simultáneamente el eje OX, para casi todo $z \in \mathbb{C}$, tenemos que

$$v(\sigma_1\cdot\sigma_2) = v(\sigma_1\cdot\sigma_2\cdot z) = v(\sigma_1) + v(\sigma_2\cdot z) = v(\sigma_1) + v(\sigma_2).$$

□

27. Teorema : *Sea $P(z)$ un polinomio con coeficientes complejos y $\sigma\colon [a,b] \to \mathbb{C}$ un rectángulo (por sencillez) recorrido en el sentido de las agujas del reloj y no pasando por ninguna raíz de $P(z)$. Entonces el número $r_\sigma(P(z))$ de raíces de $P(z)$ (contadas con su multiplicidad) contenidas en el interior del rectángulo coincide con el número de vueltas $v(P(\sigma(t)))$ de $P(\sigma(t))$ alrededor del origen:*

$$r_\sigma(P(z)) = v(P(\sigma(t))) := \frac{1}{2} E_a^b \frac{[P(\sigma(t))]_{Im}}{[P(\sigma(t))]_{Re}},$$

donde $[P(\sigma(t))]_{Im}$ es la parte imaginaria de $P(\sigma(t))$ y $[P(\sigma(t))]_{Re}$ la parte real.

Demostración. Escribamos $P(z) = H(z) \cdot \prod_i (z-\alpha_i)^{r_i}$ siendo α_i las raíces de $P(z)$ contenidas en el rectángulo y $H(z)$ sin raíces en el mismo. Por el lema anterior, $\mathrm{v}(P(\sigma(t))) = \mathrm{v}(H) + \sum_i r_i \cdot \mathrm{v}(z-\alpha_i) = \mathrm{v}(H) + \sum_i r_i$.

Solo tenemos que probar que si un polinomio $H(z)$ no tiene raíces en el rectángulo entonces $\mathrm{v}(H) = 0$. Supongamos que $\mathrm{v}(H) \neq 0$ y lleguemos a contradicción.

Se observa que si dos polígonos tienen un tramo en común pero recorridos en sentido contrario, entonces la suma de los excesos sobre estos estos dos coincide con el exceso en el contorno de la unión, pues en el tramo común el exceso de uno se cancela con el del otro. Por tanto si el interior de un polígono es unión de los interiores de varios polígonos de modo que cada dos de ellos tengan como mucho un tramo de su borde en común y éste está recorrido en sentido contrario en cada uno, entonces el exceso en el borde del polígono es la suma de los excesos en los bordes de los polígonos en los que descompone.

En particular cuadriculando el rectángulo (de manera que los ejes verticales y horizontales no pasen por las raíces) se puede suponer que dichos rectángulos son todo lo pequeños que se quiera.

Como el número de vueltas es no nulo, se puede elegir una cadena de rectángulos $\sigma_n(t)$ de manera que cada uno está contenido en el siguiente y el tamaño (de sus lados) es menor que $\frac{1}{2^n}$ y tal que el número de vueltas en él es no nulo. Estos rectángulos se intersecan en un punto α. $H(\alpha) = \lambda \neq 0$, entonces existe n tal que $H(\sigma_n(t))$ corta como mucho con uno de los ejes. Por lo tanto, por las observaciones (1) y (2), el número de vueltas de $H(\sigma_n(t))$ es nulo y hemos llegado a contradicción.

□

Este teorema permite separar las raíces de un polinomio complejo cualquiera. En efecto, $M = 1 + \mathrm{máx}\{|a_1|, \ldots, |a_n|\}$ es una cota de $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$. Comencemos con un cuadrado centrado en el origen y lado de longitud $2M$. Éste contendrá todas las raíces de $P(z)$. Subdividiendo este cuadrado en cuadrados con lado de longitud la mitad y calculando el número de vueltas en cada uno de ellos se va aproximando y separando las raíces.

Por otro lado permite demostrar de nuevo el teorema fundamental del Álgebra.

28. Teorema de D'Alembert: *Todo polinomio con coeficientes complejos tiene todas sus raíces complejas.*

Demostración. Sea $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$. Se trata de ver que eligiendo un cuadrado σ centrado en el origen y de lado suficientemente grande es $\mathrm{v}_\sigma(P(z)) = n$. Basta elegir un cuadrado σ centrado en el origen y con lado de longitud mayor que $2nM$ (siendo M como arriba). En efecto, sea $f(z) = \frac{P(z)}{z^n}$. Se tiene $P(z) = z^n f(z)$, luego $\mathrm{v}_\sigma(P(z)) = \mathrm{v}_\sigma(z^n) + \mathrm{v}_\sigma(f(z)) = n + \mathrm{v}_\sigma(f(z))$, luego basta ver que sobre σ es $\mathrm{v}_\sigma(f(z)) = 0$. Ahora bien, $|\sigma(t)| > nM$, y para todo z tal que $|z| > nM$ se cumple que $|f(z) - 1| = |\frac{P(z)}{z^n} - 1| = |a_1 z^{-1} + \cdots + a_n z^{-n}| < \frac{1}{n} + \cdots + \frac{1}{n} = 1$. En particular $f(\sigma(t))$ no corta al eje OY, por tanto, el número de vueltas de $f(z)$ al recorrer σ es nulo.

□

29. Lema : *Sean $\sigma_1(t), \sigma_2(t) \colon [a,b] \to \mathbb{C}$ dos curvas racionales (que no pasan por el origen) y $\sigma_3(t) := \sigma_1(t) \cdot \sigma_2(t)$. Denotemos $\sigma_j(t) = u_j(t) + v_j(t) \cdot i$. Entonces,*

$$E_a^b \frac{u_3(t)}{v_3(t)} = E_a^b \frac{u_1(t)}{v_1(t)} + E_a^b \frac{u_2(t)}{v_2(t)} - V_a^b(v_1 v_2, v_3),$$

donde suponemos que v_1, v_2, v_3 no se anulan ni en a ni en b.

Demostración. Supongamos que $\sigma_1(t), \sigma_2(t)$ no cortan simultáneamente al eje OX para ningún valor de t. Tenemos que $\sigma_3(t) = (u_1 u_2 - v_1 v_2) + (u_1 v_2 + v_1 u_2) \cdot i$. Denotemos $f_i = \frac{u_i}{v_i}$. y por tanto el número de vueltas es

$$E_a^b \frac{u_3}{v_3} = E_a^b \frac{u_1 u_2 - v_1 v_2}{u_1 v_2 + v_1 u_2} = E_a^b \frac{f_1 f_2 - 1}{f_1 + f_2}$$

Ahora bien, si f_1 ó f_2 tiene polo en un punto t_0, la fracción $\frac{f_1 f_2 - 1}{f_1 + f_2}$ no tiene polo en t_0 (toma el valor finito $f_2(t_0)$ ó $f_1(t_0)$ respectivamente), luego los polos se dan exactamente cuando se anula el denominador, es decir, cuando $f_1(t_0) = -f_2(t_0)$ y en tales puntos el numerador es estrictamente negativo ($f_1(t_0) f_2(t_0) - 1 = -f_1(t_0)^2 - 1 < 0$), es decir,

$$\begin{aligned} E_a^b \frac{f_1 f_2 - 1}{f_1 + f_2} &= -E_a^b \frac{1}{f_1 + f_2} = E_a^b(f_1 + f_2) - V_a^b(f_1 + f_2, 1) = E_a^b f_1 + E_a^b f_2 - V_a^b(f_1 + f_2, 1) \\ &= E_a^b \frac{u_1}{v_1} + E_a^b \frac{u_2}{v_2} - V_a^b(u_1 v_2 + u_2 v_1, v_1 v_2) = E_a^b \frac{u_1}{v_1} + E_a^b \frac{u_2}{v_2} - V_a^b(v_3, v_1 v_2) \end{aligned}$$

y obtendremos la fórmula requerida.

En particular, para casi todo número complejo 1_ϵ muy próximo a 1 (de parte imaginaria no nula), si $\sigma_2(t) = 1_\epsilon$, entonces se cumplirá que $E_a^b(\frac{u_3}{v_3}) = E_a^b(\frac{u_1}{v_1})$.

En general, existe un número complejo 1_ϵ muy próximo a 1, de modo que si definimos $\sigma_1' = \sigma_1$, $\sigma_2' = 1_\epsilon \cdot \sigma_2$ y $\sigma_3' = 1_\epsilon \cdot \sigma_3 = \sigma_1' \cdot \sigma_2'$, entonces los σ_i' están en las hipótesis del teorema y en las del párrafo primero de la demostración, $E_a^b \frac{u_i}{v_i} = E_a^b \frac{u_i'}{v_i'}$ y $V_a^b(v_1v_2, v_3) = V_a^b(v_1'v_2', v_3')$. Con lo que concluimos fácilmente.

□

30. Observación: Si tomamos las curvas $\sigma_1' = i \cdot \sigma_1$, $\sigma_2' = \sigma_2$ y $\sigma_3' = \sigma_1' \cdot \sigma_3'$, entonces obtendremos que

$$E_a^b \frac{v_3(t)}{u_3(t)} = E_a^b \frac{v_1(t)}{u_1(t)} - E_a^b \frac{u_2(t)}{v_2(t)} + V_a^b(u_1v_2, u_3),$$

donde suponemos que u_1, v_2, u_3 no se anulan ni en a ni en b

31. Teorema: *Sea $p(z) = z^n + a_1z^{n-1} + \cdots + a_n \in \mathbb{C}[x]$ un polinomio mónico y escribamos $p(x+iy) = u(x,y) + v(x,y) \cdot i$. Sea $a \in \mathbb{R}$ y supongamos que la recta del plano complejo $y = a$ no pasa por ninguna raíz de $p(z)$. Entonces,*

$$[N^o \text{ de raíces de } p(z) \text{ contenidas en el semiplano } y < a\ ] = \frac{n}{2} + \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{v(t,a)}{u(t,a)}$$

Demostración. Probemos que para todo $A >> 0$, $E_{-\infty}^{+\infty} \frac{v(t,A)}{u(t,A)} = n$. Si definimos $q(z) = 1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$, entonces $p(z) = q(z) \cdot z^n$. Observemos $q(z)$ es un número complejo muy próximo a 1, cuando $|z| >> 0$. Denotemos $\sigma_1(t) = q(t + Ai) = u_1(t) + v_1(t) \cdot i$ y $\sigma_2(t) = (t + Ai)^n = u_2(t) + v_2(t) \cdot i$. Entonces,

$$\begin{aligned} E_{-\infty}^{\infty} \frac{v(t,A)}{u(t,A)} &= E_{-\infty}^{\infty} \frac{v_1(t,A)}{u_1(t,A)} - E_{-\infty}^{\infty} \frac{u_2(t,A)}{v_2(t,A)} + V_{-\infty}^{\infty}(u_1v_2, u) \\ &= -E_{-\infty}^{\infty} \frac{u_2(t,A)}{v_2(t,A)} + V_{-\infty}^{\infty}(t^{n-1}, t^n) = -E_{-\infty}^{\infty} \frac{u_2(t,A)}{v_2(t,A)} + 1. \end{aligned}$$

Tenemos que probar que $E_{-\infty}^{\infty} \frac{u_2(t,A)}{v_2(t,A)} = -(n-1)$. Sea $\sigma_1'(t) = t + Ai = u_1' + v_1' \cdot i$ y $\sigma_2'(t) = (t + Ai)^{n-1} = u_2' + v_2' \cdot i$, entonces

$$\begin{aligned} E_{-\infty}^{\infty} \frac{u_2(t,A)}{v_2(t,A)} &= E_{-\infty}^{\infty} \frac{u_1'(t,A)}{v_1'(t,A)} + E_{-\infty}^{\infty} \frac{u_2'(t,A)}{v_2'(t,A)} - V_{-\infty}^{\infty}(v_1'v_2', v_2) \\ &= E_{-\infty}^{\infty} \frac{u_2'(t,A)}{v_2'(t,A)} - V_{-\infty}^{\infty}(t^{n-2}, t^{n-1}) = E_{-\infty}^{\infty} \frac{u_2'(t,A)}{v_2'(t,A)} - 1, \end{aligned}$$

y recurrentemente concluimos.

Procedamos ahora con toda generalidad. Sea $A >> 0$ y $B >> A$. Si definimos $q(z) = 1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$, entonces $p(z) = z^n \cdot q(z)$. Observemos $q(z)$ es un número complejo muy próximo a 1, cuando $|z| >> 0$. $\pm B + ti$, con $|t| \leq A$, es un número complejo de argumento muy próximo a cero o π, y módulo grande, luego $(\pm B + ti)^n$ también y $p(\pm B + ti)$ también; luego, la parte real de $p(\pm B + ti)$ es no nula. Sea m el número de raíces de $p(z)$ que yacen en el semiplano $y < a$. Entonces,

$$\frac{1}{2} \cdot (E_{-B}^{B} \frac{v(t,A)}{u(t,A)} - E_{a}^{A} \frac{v(B,t)}{u(B,t)} - E_{-B}^{B} \frac{v(t,a)}{u(t,a)} + E_{a}^{A} \frac{v(-B,t)}{u(-B,t)}) = n - m$$

Luego, $\frac{1}{2} \cdot (n - 0 - E_{-B}^{B} \frac{v(t,a)}{u(t,a)} + 0) = n - m$ y por tanto $m = \frac{n}{2} + \frac{1}{2} E_{-\infty}^{+\infty} \frac{v(t,a)}{u(t,a)}$.

□

32. Observaciones: 1. En el teorema hemos supuesto que $a_0 = 1$, podíamos haber supuesto con mayor generalidad que $a_0 \in \mathbb{R}^*$.

2. Evidentemente, dados $a > b$ y si $p(z)$ no tiene raíces en las rectas $y = a$ e $y = b$, entonces

$$[\text{Nº de raíces de } p(z) \text{ en la banda } b < y < a\ ] = \frac{1}{2} \cdot (E_{-\infty}^{+\infty} \frac{v(t,a)}{u(t,a)} - E_{-\infty}^{+\infty} \frac{v(t,b)}{u(t,b)}).$$

3. Supongamos que $p(z)$ no tiene raíces en la recta $x = a$. Las raíces de $p(z)$ contenidas en el semiplano $x > a$ se corresponden biunívocamente con las raíces de $p(i \cdot z)$ contenidas en el semiplano $y < -a$. Observemos que $p(iz) = p(i(x + yi)) = p(-y + xi) = u(-y,x) + v(-y,x)i$.

   Si n es par, el primer coeficiente de $p(i \cdot z)$ es igual a ± 1, luego

$$[\text{Nº de raíces de } p(z) \text{ contenidas en el semiplano } x > a\ ] = \frac{n}{2} + \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{v(a,t)}{u(a,t)}$$

   Si n es impar, observemos que el primer coeficiente de $i \cdot p(i \cdot z)$ es igual a ± 1 y $ip(iz) = -v(-y,x) + u(-y,x)i$, luego

$$[\text{Nº de raíces de } p(z) \text{ contenidas en el semiplano } x > a\ ] = \frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{u(a,t)}{v(a,t)}$$

33. Sea ahora $p(z) \in \mathbb{R}[z]$. Entonces $p(0+ti) = \sum_{r=0}^{n} i^{n-r} a_r t^{n-r}$. Si $n = 2m$ es par entonces

$$u(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s} t^{n-2s} \quad \text{y} \quad v(0,t) = (-1)^m \sum_{s=1}^{m} (-1)^s a_{2s-1} t^{n-2s+1}.$$

Si $n = 2m+1$ es impar entonces

$$u(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s+1} t^{n-2s-1} \quad \text{y} \quad v(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s} t^{n-2s}.$$

Supongamos que $p(x)$ no tiene raíces imaginarias puras. Entonces,

$$(*) \qquad \left[\begin{array}{c} \text{Nº de raíces de } p(x) \in \mathbb{R}[x] \text{ contenidas} \\ \text{en el semiplano } x > 0 \end{array} \right] = \frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{\phi_1(t)}{\phi_0(t)}$$

con

$$\phi_1(t) = a_1 t^{n-1} - a_3 t^{n-3} + a_5 t^{n-5} - \cdots$$
$$\phi_0(t) = a_0 t^n - a_2 t^{n-2} + a_4 t^{n-4} - \cdots$$

Este cálculo es importante en el problema de la estabilidad en los sistemas de ecuaciones diferenciales (lineales). Si $a_1 \neq 0$, el primer resto de Sturm de la pareja ϕ_0, ϕ_1 es

$$R_1(t) = -(\phi_0(t) - \frac{a_1}{a_0} \cdot t \cdot \phi_1(t)) = (a_2 - \frac{a_0}{a_1} \cdot a_3) t^{n-2} - (a_4 - \frac{a_0}{a_1} \cdot a_5) t^{n-4} + (a_6 - \frac{a_0}{a_1} \cdot a_7) t^{n-6} - \cdots.$$

34. Lema: *Si $a_1 \neq 0$, entonces*

$$\left[\frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} (\frac{\phi_1(t)}{\phi_0(t)}) \right] = \left[\frac{n-1}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} (\frac{R_1(t)}{\phi_1(t)}) \right] + V(a_0, a_1).$$

Demostración. Para todo $b >> 0$,

$$E_{-b}^{b} \frac{\phi_1(t)}{\phi_0(t)} + E_{-b}^{b} \frac{\phi_0(t)}{\phi_1(t)} = V_{-b}^{b}(\phi_1, \phi_0) = V(a_1 \cdot (-1)^{n-1}, (-1)^n a_0) - V(a_1, a_0) = \text{sign}(a_0 \cdot a_1) \cdot 1.$$

Luego, $E_{-\infty}^{+\infty} \frac{\phi_1(t)}{\phi_0(t)} = -E_{-\infty}^{+\infty} \frac{\phi_0(t)}{\phi_1(t)} + \text{sign}(a_0 \cdot a_1) \cdot 1 = E_{-\infty}^{+\infty} \frac{R_1(t)}{\phi_1(t)} + \text{sign}(a_0 a_1)$. Por tanto,

$$\frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{\phi_1(t)}{\phi_0(t)} = \frac{n-1}{2} + \frac{1}{2} - \frac{1}{2} (E_{-\infty}^{+\infty} \frac{R_1(t)}{\phi_1(t)} + \text{sign}(a_0 a_1)) = \frac{n-1}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{R_1(t)}{\phi_1(t)} + V(a_0, a_1).$$

□

35. Proposición: *Sea $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{R}[x]$ (con $a_0 \neq 0$), $R_1, \ldots, R_m$ los restos de Sturm de la pareja ϕ_0, ϕ_1 y c_i el coeficiente de grado máximo de R_i. Si $m = n-1$, el número de raíces de $p(x)$ de parte real positiva es igual a $V(a_0, a_1, c_1, c_2, \ldots, c_{n-1})$.*

Demostración. Observemos que ha de ser $\operatorname{gr}\phi_1 = n-1$ y $\operatorname{gr}(R_i) = n-i-1$, para todo i. En particular, $a_1 \neq 0$. Además, ϕ_0 y ϕ_1 han de ser primos entre sí, luego $p(x)$ no tiene ninguna raíz imaginaria pura. Por la fórmula $(*)$, solo tenemos que probar que $\frac{n}{2} - \frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = V(a_0,a_1,c_1,c_2,\ldots,c_{n-1})$. Procedamos por inducción sobre n. El caso $n=1$ es de comprobación inmediata. Por el lema de 1.2.34 e inducción

$$\begin{aligned}\frac{n}{2} - \frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} &= \frac{n-1}{2} - \frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{R_1(t)}{\phi_1(t)} + V(a_0,a_1) = V(a_1,c_1,c_2,\ldots,c_{n-1}) + V(a_0,a_1)\\ &= V(a_0,a_1,c_1,c_2,\ldots,c_{n-1}).\end{aligned}$$

□

36. Teorema: *Sea* $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{R}[x]$ *(con* $a_0 \neq 0$*) y consideremos la matriz*

$$H(\phi_0,\phi_1) := \begin{pmatrix} a_1 & a_0 & 0 & 0 & \ldots & 0\\ a_3 & a_2 & a_1 & a_0 & \ldots & 0\\ a_5 & a_4 & a_3 & a_2 & \ldots & \\ \vdots & \vdots & \vdots & \vdots & & \vdots\\ a_{2n-1} & a_{2n-2} & a_{2n-3} & a_{2n-4} & \ldots & a_n \end{pmatrix}$$

(con $a_m = 0$ *para todo* $m > n$*) y sea* D_i *el menor principal de orden* i *de* $H(\phi_0,\phi_1)$*. Si* $D_i \neq 0$ *para todo* i*, entonces el número de raíces de* $p(x)$ *de parte real positiva es igual a* $V(a_0, D_1, \frac{D_2}{D_1}, \frac{D_3}{D_2}, \ldots, \frac{D_n}{D_{n-1}})$*, que es igual a*

$$V(a_0,D_1,D_3,D_5,\ldots) + V(1,D_2,D_4,D_6,\ldots).$$

Demostración. Probemos la primera afirmación. Sean $R_1,\ldots,R_m$ los restos de Sturm de la pareja ϕ_0,ϕ_1. Sigamos las notaciones del teorema anterior. Basta que probemos que $m = n-1$ y que $c_i = \frac{D_{i+1}}{D_i}$. Procedamos por inducción sobre n. El caso $n=1$ es de comprobación inmediata. Observemos que $\operatorname{gr}\phi_1 = n-1$, porque $a_1 = D_1 \neq 0$, y que los restos de Sturm de la pareja ϕ_1, R_1 son $R_2,\ldots,R_m$. Denotemos $D_i(\phi_0,\phi_1)$ el menor principal de orden i de $H(\phi_0,\phi_1)$. Si a las columnas pares les restamos $\frac{a_0}{a_1}$ veces la columna anterior, los menores principales no cambian y si a continuación eliminamos la primera fila y la primera columna obtenemos la matriz $H(\phi_1,R_1)$. Luego $D_i(\phi_0,\phi_1) = a_1 \cdot D_{i-1}(\phi_1,R_1)$. Por inducción, $m-1 = n-1$ y $\frac{D_{i+1}(\phi_0,\phi_1)}{D_i(\phi_0,\phi_1)} = \frac{D_i(\phi_1,R_1)}{D_{i-1}(\phi_1,R_1)} = c_i$.

Por último, observemos que $V(D_1, \frac{D_2}{D_1}) = V(D_1^2, D_2) = V(1, D_2)$ y que $V(\frac{D_i}{D_{i-1}}, \frac{D_{i+1}}{D_i}) = V(\frac{D_i^2}{D_{i-1}}, D_{i+1}) = V(D_{i-1}, D_{i+1})$.

□

37. Definición: Se dice que un polinomio $p(x) \in \mathbb{R}[x]$ es de Hurwitz si la parte real de todas sus raíces es negativa.

En los sistemas de ecuaciones diferenciales lineales de primer orden, un punto crítico es estable si y solo si el polinomio característico de la matriz del sistema es de Hurwitz.

38. Proposición: *Sea* $p(x) = \sum_{i=0}^{n} a_i x^{n-i}$, *con* $a_0 > 0$. *Las siguientes afirmaciones son equivalentes*

1. $p(x)$ *es de Hurwitz.*
2. $E_{-\infty}^{+\infty}(\frac{\phi_1(t)}{\phi_0(t)}) = n$.

Si $p(x)$ *es de Hurwitz entonces* $a_1, \ldots, a_n > 0$.

Demostración. Si $p(x)$ tiene alguna raíz imaginaria pura entonces no sería de Hurwitz y ϕ_1 y ϕ_0 tendrían raices comunes, luego el número de polos de ϕ_1/ϕ_0 sería menor que n, luego $E_{-\infty}^{+\infty}(\frac{\phi_1(t)}{\phi_0(t)}) < n$. Por la fórmula previa $(*)$, $p(x)$ es de Hurwitz si y solo si $E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = n$.

Supongamos que $p(x)$ es de Hurwitz. Entonces, $E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = n$, y por el lema 1.2.34 $E_{-\infty}^{+\infty}(\frac{R_1(t)}{\phi_1(t)}) = n-1$ (y $a_0, a_1 > 0$). Por tanto, $\phi_0(t)$ tiene n raíces reales y $\phi_1(t)$ tiene $n-1$ raíces reales. Por la regla de Descartes $a_{2i} > 0$ para todo i y $a_{2i+1} > 0$ para todo i.

□

39. Criterio de Hurwitz: *El polinomio* $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{R}[x]$ *(con* $a_0 > 0$*) es de Hurwitz si y solo si todos los menores principales de la matriz*

$$\begin{pmatrix} a_1 & a_0 & 0 & 0 & \ldots & 0 \\ a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\ a_5 & a_4 & a_3 & a_2 & \ldots & \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{2n-1} & a_{2n-2} & a_{2n-3} & a_{2n-4} & \ldots & a_n \end{pmatrix}$$

(con $a_m = 0$ *para todo* $m > n$*) son positivos.*

Demostración. Es consecuencia inmediata del teorema 1.2.36. □

1.3. Teoría de la eliminación: Resultante de dos polinomios

Sean $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m$ variables $\mathbb{Q}$-algebraicamente independientes y sean $P(x) := a_0x^n + a_1x^{n-1} + \cdots + a_n$ y $Q(x) := b_0x^m + b_1x^{m-1} + \cdots + b_m$ polinomios genéricos de grados n y m.

Sean $x_1, \ldots, x_n$ las raíces de $P(x)$ y $y_1, \ldots, y_m$ las raíces de $Q(x)$. Observemos que $a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m$ son $\mathbb{Q}$-algebraicamente independientes porque la extensión $\mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m) \hookrightarrow \mathbb{Q}(a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m)$ es algebraica, luego

$$\operatorname{gr\,tr}_{\mathbb{Q}} \mathbb{Q}(a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m) = \operatorname{gr\,tr}_{\mathbb{Q}} \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m) = n + m + 2.$$

1. Definición: Llamaremos resultante genérica (de dos polinomios de grados n y m), que denotaremos $R(P,Q)$, a la resultante de P y Q, es decir:

$$R(P,Q) := a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

2. Propiedades:

1. $R(P,Q) = (-1)^{nm} R(Q,P)$.
2. $R(P,Q) = a_0^m \prod_{i=1}^{n} Q(x_i)$
3. $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$ *y es homogéneo de grado* m *en las variables* a_i *y homogéneo de grado* n *en las* b_j.

Demostración. (1)

$$\begin{aligned} R(P,Q) &= a_0^m b_0^n \textstyle\prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (-1)(y_i - x_j) \\ &= (-1)^{nm} b_0^n a_0^m \textstyle\prod_{j=1}^{m} \prod_{i=1}^{n} (y_i - x_j) = (-1)^{nm} R(Q,P). \end{aligned}$$

(2)

$$R(P,Q) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) = a_0^m \prod_{i=1}^{n} b_0 \prod_{j=1}^{m} (x_i - y_j) = a_0^m \prod_{i=1}^{n} Q(x_i).$$

(3) Por el apartado anterior se obtiene que $R(P,Q)$ es un polinomio en las $\{b_i\}$ y en a_0 y simétrico en las $\{x_i\}$, luego $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]_{a_0}$. De (1) se obtiene por la misma razón que $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]_{b_0}$. Por tanto, $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$.

Si sustituimos $\{b_i\}_{i=1}^m$ por $\{\lambda b_i\}_{i=1}^m$, entonces $Q(x)$ se transforma en $\lambda Q(x)$ y por el apartado (2) es $R(P, \lambda Q) = \lambda^n R(P,Q)$, luego la resultante queda afectado del factor

λ^n y $R(P,Q)$ es homogéneo de grado n en las $\{b_i\}_{i=1}^m$. Aplicando (1) se concluye que también es homogéneo de grado m en las $\{a_i\}_{i=1}^n$.

□

Sea $\bar{A}$ un anillo cualquiera y

$$\left.\begin{aligned}\overline{P}(x) &= \overline{a}_0 x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_n \\ \overline{Q}(x) &= \overline{b}_0 x^m + \overline{b}_1 x^{m-1} + \cdots + \overline{b}_m\end{aligned}\right\} \in \bar{A}[x], \quad \overline{a}_0, \overline{b}_0 \neq 0$$

3. Definición: $R(\overline{P},\overline{Q}) \in \bar{A}$ es el valor obtenido en la resultante genérica $R(P,Q)$ dando a las variables $\{a_0,\ldots,a_n,b_0,\ldots,b_m\}$ los valores $\{\overline{a}_0,\ldots,\overline{a}_n,\overline{b}_0,\ldots,\overline{b}_m\}$.

Evidentemente, $R(\bar{P},\bar{Q}) = (-1)^{nm} R(\bar{Q},\bar{P})$.

Esta definición da sentido a la resultante de polinomios cualesquiera (de grados positivos) aunque no se conozcan sus raíces, incluso sin hacer presunción de que éstas existan. Ahora bien, si $\bar{P} = \bar{a}_0(x-\bar{x}_1)\cdots(x-\bar{x}_n)$ y $\bar{Q} = \bar{b}_0(x-\bar{y}_1)\cdots(x-\bar{y}_n)$, entonces

$$R(\overline{P},\overline{Q}) = \bar{a}_0^m \bar{b}_0^n \prod_{i=1}^n \prod_{j=1}^m (\bar{x}_i - \bar{y}_j) = \bar{a}_0^m \prod_{i=1}^n \bar{Q}(\bar{x}_i),$$

ya que ya si damos a las variables x_i el valor $\bar{x}_i$ y a a_0 el valor $\bar{a}_0$ (luego a a_i el valor $\bar{a}_i$) y si damos a las variables y_i el valor $\bar{y}_i$ y a b_0 el valor $\bar{b}_0$ (luego a b_i el valor $\bar{b}_i$), entonces el valor de $R(P,Q) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = a_0^m \prod_{i=1}^n Q(x_i)$ es lo requerido.

El interés de la resultante lo da el siguiente teorema.

4. Teorema: *Sea k un cuerpo. Dos polinomios $\overline{P}(x),\overline{Q}(x) \in k[x]$, tienen alguna raíz en común si y solo si $R(\overline{P},\overline{Q}) = 0$.*

5. Ejercicio: Prueba que $R(P_1(x)\cdot P_2(x),Q(x)) = R(P_1(x),Q(x))\cdot R(P_2(x),Q(x))$, (suponemos $\mathrm{gr}(P_1P_2) = \mathrm{gr}(P_1) + \mathrm{gr}(P_2)$).

6. Teorema: *La resultante genérica $R(P,Q) \in \mathbb{Z}[a_0,\ldots,a_n,b_0,\ldots,b_m]$ (con $grP, grQ > 0$) es un polinomio irreducible.*

Demostración. En primer lugar $R(P,Q) \in \mathbb{Z}[a_0,\ldots,a_n,b_0,\ldots,b_m]$ no es divisible por b_0, pues $R(P,Q) = a_0^m \prod_i Q(x_i)$ y al hacer módulo b_0, $\bar{Q} = b_1 x^{m-1} + b_2 x^{m-2} + \cdots + b_m$, que es otro polinomio genérico, luego $\bar{Q}(x_i) \neq 0$ y $R(P,Q) \neq 0 \mod b_0$. Análogamente $R(P,Q)$ no es divisible por a_0. Ahora, por ser $R(P,Q) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j)$, se concluye que si $R(P,Q)$ admite un divisor $H \in \mathbb{Z}[a_0,\ldots,a_n,b_0,\ldots,b_m]$, entonces H es divisible por $x_i - y_j$ para algún i,j, luego como además es simétrico debe ser divisible por todos los factores $x_i - y_j$, es decir, $R(P,Q) = a_0^s b_0^t H$ y, por lo dicho al principio es $s = 0 = t$.

□

7. Lema de Euler: *Sea k un cuerpo. Dos polinomios $P(x),Q(x) \in k[x]$ de grados $n,m > 0$ respectivamente, tienen una raíz común si y solo si existen polinomios no nulos $\lambda(x),\mu(x) \in k[x]$ de grados menores que m y n respectivamente, tales que:*

$$\lambda(x)P(x) + \mu(x)Q(x) = 0$$

Demostración. Supongamos que $P(x),Q(x)$ no tienen ninguna raíz en común, es decir, que son primos entre sí. Si se verifica $\lambda(x)P(x) + \mu(x)Q(x) = 0$, entonces $Q(x)$ divide a $\lambda(x)P(x)$, luego por ser primo con $P(x)$ divide a $\lambda(x)$ de donde $gr\,\lambda(x) \geq gr\,Q(x)$ en contra de lo supuesto. Si no son primos entre sí, sea $D(x) = m.c.d.(P,Q)$. Dados $\lambda(x) := \frac{Q(x)}{D(x)}$ y $\mu(x) := -\frac{P(x)}{D(x)}$ y se tiene que $\lambda(x)P(x) + \mu(x)Q(x) = 0$. □

8. Lema : *Sea k un cuerpo y sean $P(x),Q(x) \in k[x]$ dos polinomios primos entre sí de grados $n,m > 0$ respectivamente. Existen dos polinomios $\lambda(x),\mu(x) \in k[x]$ de grados menor o igual que $m-1$ y $n-1$ respectivamente, únicos, tales que*

$$\lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = 1$$

Demostración. Existencia: Como $P(x)$ y $Q(x)$ son primos entre sí $(P(x),Q(x)) = k[x]$, y existen dos polinomios $\lambda'(x),\mu'(x) \in k[x]$ tales que $\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = 1$. Sean $c(x),\lambda(x) \in k[x]$ tales que $\lambda'(x) = c(x) \cdot Q(x) + \lambda(x)$ y $\mathrm{gr}\,\lambda(x) < \mathrm{gr}\,Q(x) = m$. Si definimos $\mu(x) := c(x) \cdot P(x) + \mu'(x)$, entonces $\lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = 1$ y por grados ha de ser $\mathrm{gr}\,\mu(x) < \mathrm{gr}\,P(x)$.

Unicidad: Si existen otros dos polinomios $\lambda_2(x),\mu_2(x) \in k[x]$ de grados menor o igual que $m-1$

y $n-1$ respectivamente, tales que $\lambda_2(x) \cdot P(x) + \mu_2(x) \cdot Q(x) = 1$, entonces $(\lambda(x) - \lambda_2(x)) \cdot P(x) + (\mu(x) - \mu_2(x)) \cdot Q(x) = 0$. Por el lema anterior, $\lambda(x) - \lambda_2(x) = 0 = \mu(x) - \mu_2(x)$.

□

9. Teorema: *Sean $P(x),Q(x) \in A[x]$ ($A = \mathbb{Z}[a_0,\ldots,a_n,b_0,\ldots,b_m]$), polinomios genéricos de grados $n,m > 0$ respectivamente. Sea $K = A_{A\setminus\{0\}}$ y sean $\lambda(x)$, $\mu(x) \in K[x]$ los únicos polinomios de grados menores que m y n respectivamente, tales que*

$$\lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = 1$$

Entonces, $R(P,Q) \in A$ es el elemento "menor" (todo otro es múltiplo de éste), único salvo signo, tal que $\lambda'(x) := R(P,Q) \cdot \lambda(x)$ y $\mu'(x) := R(P,Q) \cdot \mu(x)$ pertenecen a $A[x]$. En particular,

$$\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = R(P,Q)$$

Demostración. Sea $S \in A$ el elemento menor tal que $\lambda'(x) := S \cdot \lambda(x)$ y $\mu'(x) := S \cdot \mu(x)$ pertenecen a $A[x]$. Tenemos

$$\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = S$$

Escribamos $S = R^r \cdot a_0^s \cdot b_0^t \cdot S'$, donde $R = R(P,Q)$ y S' no es divisible por R, a_0, ni b_0. Tenemos que probar que $S' = \pm 1$, $s = t = 0$ y $r = 1$. Sea $T \in A$ irreducible que divida a S'. Entonces, en el cuerpo de fracciones de $A/(T)$, tenemos que $R \neq 0$ y que P y Q tienen raíces comunes (por el lema de Euler) y llegamos a contradicción. Por tanto, $S' = \pm 1$. Si $s > 0$ y hacemos $a_0 = 0$, en $\mathbb{Q}(a_1, \ldots, a_n, b_0, \ldots, b_m)[x]$, tendremos $\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = 0$, $Q(x)$ es irreducible, primo con $P(x)$ y de grado mayor que $\lambda'(x)$, lo cual es imposible. En conclusión, tenemos

$$\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = R(P,Q)^r$$

Derivando respecto de a_n, tenemos

$$\lambda'(x)' \cdot P(x) + \lambda'(x) + \mu'(x)' \cdot Q(x) = r \cdot R(P,Q)^{r-1} \cdot R(P,Q)'$$

Supongamos $r > 1$. Si las a_i, b_j toman valores en un cuerpo, todas las raíces comunes de $P(x)$ y $Q(x)$ son raíces también de $\lambda'(x)$. Tomemos $a_n = b_m = 0$, en el cuerpo $K = \mathbb{Q}(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1})$, 0 es la única raíz común de $P(x)$ y $Q(x)$. Ahora bien, $\lambda'(x) = c \cdot (Q(x)/x)$ y $\mu(x) = -c(P(x)/x)$ para cierto $c \in K$, y el 0 no es una raíz de $\lambda'(x)$. Hemos llegado a contradicción y $r = 1$.

□

10. Proposición: *Dados dos polinomios $P(x), Q(x) \in A[x]$ de grados n y m respectivamente, existen dos polinomios $\lambda(x), \mu(x) \in A[x]$ de grados menor o igual que $m-1$ y $n-1$ respectivamente, tales que*

$$(*) \qquad \lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = R(P,Q)$$

Si A es íntegro y $R(P,Q) \neq 0$, entonces $\lambda(x)$ y $\mu(x)$ son únicos cumpliendo la igualdad.

Demostración. La existencia es consecuencia inmediata del teorema anterior. La unicidad en el caso íntegro y con $R(P,Q) \neq 0$, es consecuencia inmediata del lema anterior.

□

11. Corolario: *Sean $P(x), Q(x) \in A[x]$ ($A = \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$), polinomios genéricos de grados $n, m > 0$ respectivamente y consideremos el ideal $(P,Q) \subseteq A[x]$. Entonces,*

$$(P,Q) \cap A = (R(P,Q))$$

Demostración. 1. Dados $f_1, f_2 \in A[x]$, si $f_1 \cdot P(x) + f_2 \cdot Q(x) = S \in A$ entonces $R(P,Q)$ divide a S: Haciendo $R(P,Q) = 0$, $P(x)$ y $Q(x)$ no son primos entre sí (en $k[x]$, siendo k el cuerpo de fracciones de $A/(R(P,Q))$. Por tanto, S ha de ser nulo en k, luego $R(P,Q)$ divide a S.

2. Por el teorema anterior, $R(P,Q) \in (P,Q) \cap A$.

□

1.3.1. Métodos de cómputo de la resultante

Vamos a dar algoritmos explícitos de cómputo de la resultante.

A. Resultante de Euler:

Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$ y $Q(x) = \sum_{i=0}^{m} b_i x^{m-i} \in k[x]$.

Por el lema de Euler, estos polinomios tienen una raíz común si y solo si existen polinomios $\lambda(x), \mu(x)$ de grados menores que los de $Q(x), P(x)$ respectivamente tales que:

$$\lambda(x)P(x) + \mu(x)Q(x) = 0$$

es decir, si denotamos $k[x]_{<s} \subset k[x]$ el subespacio vectorial de los polinomios de grado menor que s, esto equivale a que la aplicación lineal:

$$\begin{aligned} k[x]_{<m} \times k[x]_{<n} &\to k[x]_{<m+n} \\ (\lambda(x), \mu(x)) &\mapsto \lambda(x)P(x) + \mu(x)Q(x) \end{aligned}$$

tenga núcleo no nulo. Eligiendo en cada espacio vectorial $k[x]_{<s}$ la base $\{x^{s-1}, x^{s-2}, \ldots, x, 1\}$, y calculando el determinante de la matriz (transpuesta) de esta aplicación lineal en dichas bases, resulta la condición:

$$\mathscr{E}(P,Q) := \begin{vmatrix} a_0 & \cdots & \cdots & \cdots & \cdots & a_n & & 0 \\ & \ddots & & & & & \ddots & \\ 0 & & a_0 & \cdots & \cdots & \cdots & \cdots & a_n \\ b_0 & \cdots & \cdots & b_m & & & & 0 \\ & \ddots & & & \ddots & & & \\ & & \ddots & & & \ddots & & \\ & & & \ddots & & & \ddots & \\ 0 & & & & b_0 & \cdots & \cdots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{matrix} = 0$$

12. Definición: Diremos que $\mathscr{E}(P,Q)$ es la resultante de Euler (también llamada de Cayley y de Sylvester).

13. Teorema: *La resultante de Euler $\mathscr{E}(P,Q)$ es la resultante:*

$$\mathscr{E}(P,Q) = R(P,Q).$$

Demostración. Podemos suponer que P y Q son polinomios genéricos. Evidentemente $\mathscr{E}(P,Q) \in \mathbb{Z}[a_0,\ldots,a_n,b_o,\ldots,b_m]$ tiene que ser múltiplo de la resultante porque si hacemos $R(P,Q)=0$, entonces $\mathscr{E}(P,Q)=0$ (porque es cero en el cuerpo de fracciones de $\mathbb{Z}[a_0,\ldots,a_n,b_o,\ldots,b_m]/(R(P,Q))$). Además $\mathscr{E}(P,Q)$ es homogéneo de grado m en las a_i y homogéneo de grado n en las b_j, ya que $\mathscr{E}(\lambda P,\mu Q) = \lambda^m\mu^n\mathscr{E}(P,Q)$. Por tanto, $\mathscr{E}(P,Q)$ difiere de $R(P,Q)$ en un entero. Pero es fácil ver que el coeficiente de $\mathscr{E}(P,Q)$ en $a_0^m \cdot b_m^n$ es igual que para $R(P,Q)$, luego dicho entero es 1.

□

14. Observación: Este teorema es válido aunque los coeficientes de los polinomios sean de un anillo y no de un cuerpo.

B. Resultante de Bézout:

15. Teorema: *Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$, $Q(x) = \sum_{i=1}^{m} b_i x^{m-i}$ dos polinomios con coeficientes en un cuerpo k. El determinante del endomorfismo*

$$Q(x)\cdot : k[x]/(P(x)) \to k[x]/(P(x)), \overline{H(x)} \mapsto \overline{Q(x)\cdot H(x)},$$

multiplicado por a_0^m, es igual a $R(P,Q)$.

Demostración. Podemos suponer que P y Q son polinomios genéricos y que k es algebraicamente cerrado. En este caso, $P(x) = a_0\cdot(x-x_1)\cdots(x-x_n)$. Por el teorema chino de los restos $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, $\overline{H(x)} \mapsto (H(x_1),\ldots,H(x_n))$. Por tanto, $\overline{Q(x)}$ es igual a $(Q(x_1),\ldots,Q(x_n))$ en $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, y el determinante $|Q(x)\cdot| = Q(x_1)\cdots Q(x_n)$. Luego, $a_0^m \cdot |Q(x)\cdot| = R(P,Q)$. □

Supongamos ahora que $n=m$. Consideremos en $k[x]/(P(x))$ las dos bases siguientes $\{a_0, a_0\cdot x + a_1, \ldots, a_0x^{n-1}+\cdots+a_{n-1}\}$ y $\{1,x,\ldots,x^{n-1}\}$. Observemos que

$$Q(x)\cdot(a_0x^i+\cdots+a_i) - P(x)\cdot(b_0x^i+\cdots+b_i) = \sum_{j=0}^{n-1} c_{ij}x^j \qquad (*)$$

para ciertos $c_{ij} \in k$ y todo i. Entonces, es fácil ver que

$$R(P,Q) = a_0^m \cdot |Q(x)\cdot| = |(c_{ij})|$$

16. Observación: Como los coeficientes c_{ij} se obtienen algebraicamente a partir de los de P y Q es fácil ver que la fórmula $R(P,Q) = |(c_{ij})|$ es válida para polinomios con coeficientes en un anillo cualquiera (no necesariamente un cuerpo).

17. Observación: Si multiplicamos la ecuación $(*)$ por x y sumamos $Q(x)\cdot a_{i+1} - P(x)\cdot b_{i+1}$, entonces obtenemos

$$\sum_{j=0}^{n-1} c_{i+1\,j}x^j = x\cdot\sum_{j=0}^{n-1} c_{ij}x^j + Q(x)\cdot a_{i+1} - P(x)\cdot b_{i+1}$$

Luego, $c_{i+1,j} = c_{i,j-1} + a_{i+1}b_{n-j} - b_{i+1}a_{n-j}$ (y sabemos que $c_{0j} = a_0 b_{n-j} - b_0 a_{n-j}$).

Si $P(x)$ es de grado n y $Q(x)$ de grado m. Supongamos $m > n$, entonces P y $x^{n-m}Q$ tienen grado n y $R(P,x^{n-m}Q) = R(P,Q)\cdot R(P,x)^{n-m} = a_n^{n-m}R(P,Q)$.

C. Método directo mediante el algoritmo de Euclides:

En este apartado, supondremos que el anillo de coeficientes de los polinomios es íntegro o si se prefiere un cuerpo. Este método se basa en el siguiente lema.

18. Lema: *Sean $C(x)$,$R(x)$ polinomios tales que:*

$$P(x) = C(x)Q(x) + R(x)$$

Entonces se cumple la igualdad

$$R(P,Q) = (-1)^{nm}b_0^{n-grR}R(Q,R),$$

siendo n,m los grados de P, Q respectivamente y b_0 el coeficiente en grado máximo de Q.

Demostración. De la igualdad del enunciado se obtiene $P(y_j) = R(y_j)$, siendo $\{y_j\}$ las raíces de Q, luego:

$$\begin{aligned} &R(P,Q) = (-1)^{nm}R(Q,P) = (-1)^{nm}b_0^n\textstyle\prod_j P(y_j)\\ &= (-1)^{nm}b_0^n\textstyle\prod_j R(y_j) = (-1)^{nm}b_0^n b_0^{-grR}R(Q,R).\end{aligned}$$

□

Dados P,Q como antes denotemos $R_0 = P$, $R_1 = Q$ y por recurrencia se define R_{i+1} el resto de dividir R_{i-1} por R_i:

$$\begin{aligned} P &= C_1Q + R_2\\ Q &= C_2R_2 + R_3\\ R_2 &= C_3R_3 + R_4\\ &\cdots\\ R_{r-2} &= C_{r-1}R_{r-1} + R_r\end{aligned}$$

siendo R_r el primero tal que $grR_r = 0$. Denotemos además $g_i = grR_i$ y d_i el coeficiente en grado máximo de R_i, es decir,

$$R_i(x) = d_i x^{g_i} + \cdots$$

19. Teorema:

$$R(P,Q) = (-1)^{\sum_{i=0}^{r-1} g_i g_{i+1}} \prod_{i=1}^{r} d_i^{g_{i-1}-g_{i+1}}$$

(conviniendo que $g_{r+1} = 0$).

Demostración. Aplicando el lema anterior y recurrencia se prueba fácilmente la fórmula:

$$R(P,Q) = \left[(-1)^{\sum_{i=0}^{h-1} g_i g_{i+1}} \prod_{i=1}^{h} d_i^{g_{i-1}-g_{i+1}} \right] R(R_h, R_{h+1})$$

Para $h = r-1$ es $R(R_{r-1}, R_r) = d_r^{g_{r-1}}$, sustituyendo se concluye.

□

1.3.2. Aplicaciones de la resultante

A. Intersección de dos curvas planas.

Sean $P(x,y), Q(x,y) \in k[x,y]$ dos polinomios en dos variables primos entre sí y sea el sistema de ecuaciones:

$$\begin{array}{l} P(x,y) = a_0(y)\cdot x^n + \cdots + a_{n-1}(y)\cdot x + a_n(y) = 0 \\ Q(x,y) = b_0(y)\cdot x^m + \cdots + b_{m-1}(y)\cdot x + b_m(y) = 0 \end{array} \qquad (a_0(y), b_0(y) \neq 0)$$

que son las ecuaciones de la intersección de las curvas $P(x,y) = 0$ y $Q(x,y) = 0$.

20. Proposición: *Sea $R(y)$ la resultante de P y Q entendidos respectivamente como polinomios en x con coeficientes en $k[y]$. Entonces, β es una raíz de $R(y)$ si y solo si β es una raíz común de $a_0(y)$ y $b_0(y)$, o existe α tal que (α, β) es un punto de corte de las curvas $P(x,y) = 0$ y $Q(x,y) = 0$.*

Demostración. Por la resultante de Euler, $R(y) \subseteq (a_0(y), b_0(y))$, luego si β es una raíz de común de $a_0(y)$ y $b_0(y)$ lo es de $R(y)$. Si β no es una raíz $a_0(y)$, por la resultante de Bezout, $R(\beta) = a_0^{m-\mathrm{gr}Q(x,\beta)} \cdot R(P(x,\beta), Q(x,\beta))$. Por tanto, si $R(\beta) = 0$, tenemos que $R(P(x,\beta), Q(x,\beta) = 0$ y existe α tal que $P(\alpha,\beta) = Q(\alpha,\beta) = 0$.

□

Si $\{(\alpha_1,\beta_1),\ldots,(\alpha_n,\beta_n)\}$ son los puntos de corte de las curvas $P(x,y)=0$ y $Q(x,y)=0$, entonces $\{(\alpha_1,\ldots,\alpha_n\},\{\beta_1,\ldots,\beta_n\}$ son respectivamente raíces de $R(x)$ y $\overline{R}(y)$.

B. Cálculo de las raíces complejas de un polinomio complejo.

Sea $P(z)\in\mathbb{C}[z]$ y escribamos $z=x+i\cdot y$. Entonces, $P(z)=U(x,y)+V(x,y)\cdot i$, con $U(x,y),V(x,y)\in\mathbb{R}[x]$. El número complejo $a+b\cdot i$ es una raíz compleja de $P(z)$ si y solo si (a,b) es una solución del sistema de ecuaciones reales

$$\begin{aligned} U(x,y)&=0\\ V(x,y)&=0 \end{aligned}$$

Por el apartado anterior, si (a,b) es una solución real del sistema de ecuaciones, entonces a es una raíz real de la resultante, $R(x)=R(U(x,y),V(x,y))$, considerados como polinomios en y; y b es una raíz real de la resultante de $\bar{R}(y)=R(U(x,y),V(x,y))$, considerados como polinomios en x. Para calcular las raíces complejas de $P(z)$ basta calcular las raíces reales de $R(x)$ y $\bar{R}(y)$.

C. Solución de un sistema de ecuaciones algebraicas

Consideremos un sistema de ecuaciones algebraicas

$$\begin{aligned} &P_1(x_1,\ldots,x_n)=0\\ &\cdots\\ &P_n(x_1,\ldots,x_n)=0 \end{aligned}$$

Sea $R_i(x_2,\ldots,x_n):=R(P_1(x_1,\ldots,x_n),P_i(x_1,\ldots,x_n))$, para todo $1<i\le n$, considerados P_1 y P_i como polinomios en x_1. Si $(\alpha_1,\ldots,\alpha_n)$ es una solución del sistema de ecuaciones $P_1=\ldots=P_n=0$ entonces $(\alpha_2,\ldots,\alpha_n)$ es una solución del sistema de ecuaciones $R_2=\ldots=R_n=0$.

D. Discriminante.

Sea $P(x)=x^n+a_1x^{n-1}+\cdots+a_n$.

21. Teorema: *Si denotamos por* $P'(x)=nx^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$ *la derivada (formal) de* $P(x)$*, entonces:*

$$\Delta(P)=(-1)^{\binom{n}{2}}R(P,P').$$

Demostración. Como $P(x)=\prod_{i=1}^n(x-x_i)$, entonces $P'(x)=\sum_{j=1}^n\prod_{i\neq j}^n(x-x_i)$ y $P'(x_j)=\prod_{i\neq j}^n(x_j-x_i)$. Por tanto:

$$\begin{aligned} &R(P,P')=\textstyle\prod_{j=1}^n P'(x_j)=\prod_{j=1}^n\prod_{i\neq j}^n(x_j-x_i)=\prod_{i<j}(x_i-x_j)(x_j-x_i)\\ &=\textstyle\prod_{i<j}-(x_i-x_j)^2=(-1)^{\binom{n}{2}}\prod_{i<j}(x_i-x_j)^2=(-1)^{\binom{n}{2}}\Delta(P). \end{aligned}$$

□

E. Racionalización.

Dados $P,Q \in k[x]$ primos entre sí y dada una raíz α de P se trata de *calcular* $\frac{1}{Q(\alpha)}$ *como polinomio en* α. Observemos que

$$R(P,Q) = R(\frac{P(x)}{x-\alpha}(x-\alpha), Q(x)) = R(\frac{P(x)}{x-\alpha}, Q(x)) \cdot R(x-\alpha, Q(x)) = R(\frac{P(x)}{x-\alpha}, Q(x)) \cdot Q(\alpha).$$

Luego,

$$\boxed{\frac{1}{Q(\alpha)} = \frac{1}{R(P,Q)} \cdot R(\frac{P(x)}{x-\alpha}, Q)}$$

F. Polinomio de raíces una función de las raíces de otro polinomio.

Sea $P(x) \in k[x]$ y $\alpha_1, \ldots, \alpha_n \in K \supset k$ las raíces de $P(x)$ y, sea $f(x) = \frac{A(x)}{B(x)} \in k(x)$ una función racional, tal que B es primo con P (para que tenga sentido hacer $x = \alpha_i$ en $f(x)$). *Se trata de calcular otro polinomio* $Q(x) \in k[x]$ *cuyas raíces sean* $f(\alpha_1), \ldots, f(\alpha_n)$.

Para ello se considera el sistema de ecuaciones:

$$\left.\begin{aligned} P(x) &= 0 \\ A(x) - B(x)y &= 0 \end{aligned}\right\}$$

Las raíces del polinomio $R(y) := R(P(x), A(x) - B(x)y)$ son $f(\alpha_1), \ldots, f(\alpha_n)$: La condición necesaria y suficiente para que $R(\beta) = 0$ es que los polinomios $\{P(x), A(x) - B(x)\beta\}$ tengan una raíz común α. Esto es que exista α tal que

$$\left.\begin{aligned} P(\alpha) &= 0 \\ \beta &= \frac{A(\alpha)}{B(\alpha)} \end{aligned}\right\}$$

es decir, que $\beta = f(\alpha)$ para alguna raíz α de $P(x)$.

22. Ejemplo : Sea $P(x) \in k[x]$ de raíces $\alpha_1, \ldots, \alpha_n \in K$. Sea ξ una raíz r-ésima primitiva de la unidad. El polinomio cuyas raíces son $\alpha_1^r, \ldots, \alpha_n^r$ es:

$$\boxed{R(y) = R(P(x), x^r - y) = \prod_{i=1}^{r} P(\xi^i \cdot \sqrt[r]{y})}$$

Si $r = 2$, el polinomio cuyas raíces son los cuadrados de las de $P(x)$ es

$$Q(x) = P(\sqrt{x}) \cdot P(-\sqrt{x})$$

(conviene calcular $P(z) \cdot P(-z)$ y después hacer el cambio $x = z^2$.)

1.3.3. Ejercicios y ejemplos

Ejemplo 1: Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calculemos un polinomio de raíces $\alpha_i + \frac{1}{\alpha_i}$. Sea $y = x + \frac{1}{x} = \frac{x^2+1}{x}$, es decir, $x^2 - yx + 1 = 0$. Consideremos el sistema

$$\left.\begin{aligned} P(x) = 0 \\ Q(x) = x^2 - yx + 1 = 0 \end{aligned}\right\}$$

Las soluciones del sistema son $x = \alpha_i$, $y = \alpha_i + \frac{1}{\alpha_i}$. Luego las raíces de $R(y) := R(P,Q)$ son $y = \alpha_i + \frac{1}{\alpha_i}$. Las raíces de $Q(x)$ son $x, 1/x$ (con $y = x + 1/x$). Luego

$$\boxed{R(y) = P(x) \cdot P(\frac{1}{x})}$$

haciendo el cambio $x + \frac{1}{x} = y$ (o sustituyendo $x = \frac{y+\sqrt{y^2-4}}{2}$ y $\frac{1}{x} = \frac{y-\sqrt{y^2-4}}{2}$).

Ejercicio: *Calcula el polinomio cuyas raíces son*

$$cos\,\frac{2k\pi}{5} \qquad , \quad k = 0,1,2,3,4$$

Solución: La ecuación $x^5 - 1 = 0$ tiene por soluciones las raíces quintas de 1:

$$\varepsilon^k = cos\,\frac{2k\pi}{5} + sen\,\frac{2k\pi}{5}$$

con lo que

$$cos\,\frac{2k\pi}{5} = \frac{1}{2}(\varepsilon^k + \overline{\varepsilon}^k) = \frac{1}{2}(\varepsilon^k + \frac{1}{\varepsilon^k})$$

así que el sistema es

$$\left.\begin{aligned} x^5 - 1 = 0 \\ y = \frac{1}{2}(x + \frac{1}{x}) \end{aligned}\right\}$$

Siguiendo el ejemplo 1, la resultante queda:

$$R(y) = (x^5 - 1)(\frac{1}{x^5} - 1) = -(x^5 + \frac{1}{x^5}) + 2$$

haciendo el cambio $2y = x + x^{-1}$. Elevando $x + x^{-1}$ a 5 y a 3 y después de un pequeño cálculo se obtiene:

$$R(y) = 16y^5 - 20y^3 + 5y - 1$$

Igualmente sabríamos calcular el polinomio de raíces $sen\,\frac{2k\pi}{5}$, con $k = 1,\ldots,5$, ya que $sen\,\frac{2k\pi}{5} = \frac{1}{2i}(\varepsilon^k - \varepsilon^{-k})$ y se aplica el método del ejemplo 1.

Ejemplo 2: Si se busca el *polinomio de raíces* $\alpha_i - \frac{1}{\alpha_i}$, resulta igual que antes que la resultante buscada es

$$\boxed{R(y) = P(x) \cdot P(-\frac{1}{x})}$$

haciendo el cambio $y = x - \frac{1}{x}$ (es decir sustituyendo $x = \frac{y+\sqrt{y^2+4}}{2}$ y $-\frac{1}{x} = \frac{y-\sqrt{y^2+4}}{2}$).

Ejemplo 3 (generalización de 1 y 2): El *polinomio de raíces* $a\alpha_i + \frac{b}{\alpha_i}$, siendo $a, b \in k$ es:

$$\boxed{R(y) = P(x) \cdot P(\frac{b}{ax})}$$

haciendo $ax + \frac{b}{x} = y$ (es decir sustituyendo $x = \frac{y+\sqrt{y^2-4ab}}{2a}$ y $\frac{b}{ax} = \frac{y-\sqrt{y^2-4ab}}{2a}$).

Si x es solución de la ecuación $y = ax + \frac{b}{x}$, entonces $\frac{b}{ax}$ también y se concluye como en los ejemplos 1 y 2.

Ejemplo 4: Sea $P(x) \in k[x]$ y $\alpha_1, \ldots, \alpha_n \in K$ sus raíces. Sea $F(\alpha, \beta) = 0$ una relación de dependencia algebraica sobre k entre dos raíces $\alpha = \alpha_1$ y $\beta = \alpha_2$ (es decir, $F(x, y)$ es un polinomio con coeficientes en k). En esta situación las raíces α, β se pueden calcular.

Para ello sea $R(y) := R(P(x), F(x, y))$ considerados $P(x)$ y $F(x, y)$ como polinomios en x (con coeficientes en $k[y]$). Igual que en los ejemplos anteriores β es raíz de $R(y)$ y de $P(x)$, por tanto, $x - \beta$ es factor común del m.c.d.$(P(x), R(x))$. (Si la relación se verifica únicamente para las raíces α_1, α_2, entonces β es la única raíz común de $P(x), R(x)$ y, por tanto, el m.c.d.$(P, R) = (x - \beta)$. Entonces β se calcula y α será una raíz común de $P(x)$ y $F(x, \beta)$ y, por tanto, de $m.c.d.(P(x), F(x, \beta))$.

Conocidas $\alpha = \alpha_1$ y $\beta = \alpha_2$ se divide $P(x)$ por $(x - \alpha_1)(x - \alpha_2)$. El cociente $P_1(x)$ es de grado $n - 2$. (¡el grado de dificultad ha bajado en 2 unidades!).

Ejemplo 5: El discriminante de $x^2 + ax + b$ es $\Delta = a^2 - 4b$.

Solución: $R_0(x) = x^2 + ax + b$, $R_1(x) = P'(x) = 2x + a$, $R_2(x) = P(-\frac{a}{2}) = -\frac{a^2}{4} + b$, luego $g_0 = 2, g_1 = 1, g_2 = 0$ y $d_0 = 1, d_1 = 2, d_2 = -\frac{a^2}{4} + b$:

$$\Delta = (-1)^{\binom{2}{2}} \cdot R(P, P') = (-1)^{2 \cdot 1 + 1 \cdot 0} \cdot 2^{2-0}(-\frac{a^2}{4} + b)^{1-0} = a^2 - 4b.$$

Ejemplo 6: El discriminante de $x^3 + px + q$ es $\Delta = -(4p^3 + 27q^2)$.

Solución: $R_0(x) = x^3 + px + q$, $R_1(x) = P'(x) = 3x^2 + p$, $R_2(x) = \frac{2}{3}px + q$ y por último $R_3(x) = R_2(-\frac{3}{2}\frac{q}{p}) = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$, luego $g_0 = 3, g_1 = 2, g_2 = 1, g_3 = 0$ y $d_0 = 1, d_1 = 3, d_2 = \frac{2}{3}p, d_3 = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$:

$$\Delta = (-1)^{\binom{3}{2}} \cdot R(P, P') = -(-1)^{3 \cdot 2 + 2 \cdot 1 + 1 \cdot 0} \cdot 3^{3-1}(\frac{2}{3}p)^{2-0}(\frac{3^3}{2^2}\frac{q^2}{p^2} + p) = -(4p^3 + 27q^2).$$

1.4. Problemas

1. Sea $A = \mathbb{Q}[x]/(2x^3+4x^2-x-2)$ y sea $\alpha = \bar{x}$. ¿Son $\alpha+2$ y $\alpha-2$ invertibles en A?.

2. Sea $K = \mathbb{Q}[x]/(x^3-x-1)$ y sea $\alpha = \bar{x}$. Racionaliza $1/(\alpha+2)$ y determina si $(2+\alpha)^3$ es la unidad. ¿Tiene el polinomio x^2-2 alguna raíz en K?. Calcula un polinomio no nulo con coeficientes racionales $p(x)$ que admita la raíz $\beta = \alpha^2+1$.

3. Si $a, b \in \mathbb{Q}$, demuestra que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ precisamente cuando a/b sea un cuadrado en $\mathbb{Q}$.

4. Prueba que $\mathbb{Q}(\sqrt[n]{2})$ tiene grado n sobre $\mathbb{Q}$.

5. Determina las relaciones de inclusión entre los siguientes subcuerpos de $\mathbb{C}$:
$$\mathbb{Q}\ ,\ \mathbb{Q}(1/2)\ ,\ \mathbb{Q}(\sqrt{2})\ ,\ \mathbb{Q}(\sqrt[3]{2})\ ,\ \mathbb{Q}(i)\ ,\ \mathbb{Q}(i+\sqrt{2})\ ,\ \mathbb{Q}(\sqrt{-2})$$

6. Sea $p(x)$ un polinomio irreducible de grado n con coeficientes en un cuerpo k. Si el grado de una extensión finita L de k no es múltiplo de n, entonces $p(x)$ no tiene raíces en L.

7. Demuestra que x^3-3 no tiene raíces en $k = \mathbb{Q}(\sqrt{2})$. Concluye que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ es una extensión de grado 6 de $\mathbb{Q}$ y halla una base sobre $\mathbb{Q}$.

   Sea $\alpha = \sqrt{2}+\sqrt[3]{3}$. Prueba que el grado de un polinomio irreducible en $\mathbb{Q}[x]$ que admita la raíz α es $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 1, 2, 3$, ó 6. Analizando las relaciones de dependencia lineal entre las sucesivas potencias de α, concluir que α es raíz de un polinomio irreducible de grado 6 con coeficientes racionales. Calcula tal polinomio.

8. Sea $K = \mathbb{F}_2[x]/(x^3+x+1)$ y sea $\alpha = \bar{x}$. Prueba que K es un cuerpo con 8 elementos
$$K \ = \ \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$$
   Calcula las raíces de x^3+x+1 en K, y las raíces de x^3+x^2+1 en K.

9. Construir un cuerpo con 4 elementos y otro con 9 elementos.

10. Calcula el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan las raíces complejas del polinomio x^3-1. Análogamente para x^3+1, x^4-1, x^4+1, x^5-1, x^5+1 y x^6-1.

11. Halla el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan todas las raíces complejas del polinomio x^3-2. Análogamente para los polinomios
$$x^4-2\ ,\ x^4+2\ ,\ x^4-x^2+1\ ,\ x^4+x^2-2,\ x^3-4x^2+5$$

12. Calcula un polinomio irreducible con coeficientes en $\mathbb{Q}(i)$ que admita la raíz $\sqrt[4]{2}$. Análogamente sustituyendo $\mathbb{Q}(i)$ por $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$.

13. Sea K una extensión de grado 2 de un cuerpo k. Si la característica de k no es 2, prueba que $K = k(\sqrt{a})$ para algún $a \in k$. ¿Es cierto también cuando $\operatorname{car} k = 2$?

14. Halla un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $\mathbb{Q}(i) \times \mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[x]/(p(x))$.

15. ¿Existe algún polinomio $p(x) \in \mathbb{Q}[x]$ tal que $\mathbb{Q}(i) \times \mathbb{Q}(i) \simeq \mathbb{Q}[x]/(p(x))$?

16. Sean $\alpha_1, \ldots, \alpha_n$ raíces complejas de ciertos polinomios no nulos $p_1(x), \ldots, p_n(x) \in \mathbb{Q}[x]$. Demuestra que $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es una $\mathbb{Q}$-álgebra finita de grado acotado por el producto de los grados de los polinomios $p_1(x), \ldots, p_n(x)$.

17. Una extensión finita $k \to L$ es trivial (i.e., $[L : k] = 1$) si y solo si $L \otimes_k L$ es cuerpo. (*Indicación:* Considerar el morfismo natural $L \otimes_k L \to L$).

18. Sean L, L' dos k-extensiones de cuerpos de k, de grados n y m respectivamente. Prueba que si n y m son primos entre sí, entonces $L \otimes_k L'$ es un cuerpo.

19. Si L y L' son dos extensiones no triviales (i.e., de grado mayor que 1) de un cuerpo k, ¿puede ocurrir que $L' \otimes_k L$ no sea un cuerpo? ¿y que $L' \otimes_k L$ sí sea un cuerpo?

20. Prueba que toda extensión finita L de $\mathbb{C}$ es trivial: $\mathbb{C} \simeq L$. Concluir que toda $\mathbb{C}$–álgebra finita reducida de grado n es isomorfa a $\mathbb{C} \times \overset{n}{\cdots} \times \mathbb{C}$. ¿Es cierto que toda $\mathbb{C}$–álgebra finita es trivial?

21. Prueba que toda extensión finita de $\mathbb{R}$ es isomorfa a $\mathbb{R}$ ó a $\mathbb{C}$. Concluir que toda $\mathbb{R}$-álgebra finita reducida es isomorfa a $\mathbb{R} \times \overset{n}{\cdots} \times \mathbb{R} \times \mathbb{C} \times \overset{m}{\cdots} \times \mathbb{C}$ para ciertos $n, m \in \mathbb{N}$.

22. Determina los automorfismos de los cuerpos $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[5]{2})$ y $\mathbb{Q}(\sqrt[6]{2})$.

23. Determina los automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de $x^3 - 3$. Análogamente para $x^2 - 2$, $x^4 - 4$.

24. Sea $k = \mathbb{Q}(\sqrt[5]{5})$. Prueba que el polinomio mónico mínimo anulador de $e^{\frac{2\pi i}{5}}$ sobre k es $x^4 + x^3 + x^2 + x + 1$.

    Determina el número de automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de $x^5 - 5$.

25. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. Prueba que α es una raíz múltiple de $p(x)$ si y solo si es raíz de $p(x)$ y $p'(x)$. Prueba que si α es una raíz de $p(x)$ de multiplicidad $m \geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad $m-1$, cuando la característica de k es cero. Prueba que si α es una raíz de $p(x)$ de multiplicidad $m \geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad mayor o igual que $m-1$, cuando la característica de k es positiva.

26. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k, de característica nula. Prueba que si m es la multiplicidad de una raíz α del polinomio $d(x) = \text{m.c.d.}\big(p(x), p'(x)\big)$, entonces α es una raíz de $p(x)$ de multiplicidad $m+1$.

    ¿Es cierto este enunciado en los cuerpos de característica positiva?

27. Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo. Prueba que si $p(x)$ tiene alguna raíz múltiple, entonces su derivada $p'(x)$ es nula.

    Si $p(x)$ tiene una raíz simple ¿es cierto que todas sus raíces son simples?. Si $p(x)$ tiene una raíz múltiple ¿es cierto que todas sus raíces son múltiples?

28. Halla las raíces múltiples de los siguientes polinomios con coeficientes racionales, así como sus respectivas multiplicidades ¿y si los coeficientes están en $\mathbb{F}_2$? ¿y en $\mathbb{F}_3$? ¿y en $\mathbb{F}_5$?

$$x^4 + 4x^2 + 1 \quad , \quad 4x^4 - 4x^3 - 3x^2 + 2x + 1.$$

29. Halla los números complejos x, y, z tales que $x+y+z = 1$, $xyz = 1$ y $|x| = |y| = |z| = 1$.

30. Resuelve la ecuación $x^3 - 3\lambda x^2 + 4 = 0$ sabiendo que dos de sus raíces son iguales.

31. Resuelve la ecuación $x^3 - 5x^2 + 16x + 8 = 0$ sabiendo que la suma de dos de sus raíces es 0.

32. Resuelve la ecuación $x^3 - 9x^2 + 23x - 15 = 0$ sabiendo que sus raíces forman una progresión aritmética.

33. Calcula la suma $\sum_{k=0}^{n-1} \frac{1}{cos^2(\frac{2k\pi}{n})}$.

34. Sabiendo que $P(x)$ es un polinomio cuyas raíces $\{\alpha_i\}$ están en progresión geométrica, calcular $P'(\alpha_i)$.

35. Expresa el polinomio $P_4 = x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_4^2 + x_2^2x_3^2 + \cdots$ mediante los polinomios simétricos elementales.

36. Expresa mediante los polinomios simétricos elementales la función racional

$$h = \frac{x_1x_2}{x_3x_4} + \frac{x_1x_3}{x_2x_4} + \frac{x_1x_4}{x_2x_3} + \frac{x_2x_3}{x_1x_4} + \frac{x_2x_4}{x_1x_3} + \frac{x_3x_4}{x_1x_2}$$

37. Calcula las expresiones de las siguientes funciones $\sum_{i=1}^{n} \frac{1}{x_i}$ y $\sum_{i=1}^{n} \frac{1}{x_i^2}$ en función de los polinomios simétricos elementales.

38. Calcula las expresiones siguientes en función de los polinomios simétricos elementales:

$$\sum_{i\neq j}^{n} \frac{x_i}{x_j} \quad , \quad \sum_{i\neq j}^{n} \frac{x_i^2}{x_j} \quad , \quad \sum_{i\neq j, i\neq k, j>k}^{n} \frac{x_jx_k}{x_i}$$

39. Calcula la suma $\sum_{i<j}(x_i + x_j)^n$ en función de las sumas de potencias σ_n.

40. Sea ε una raíz quinta primitiva de la unidad. Calcula el valor de la suma: $\sum_{k=1}^{4} \frac{3\varepsilon^{3k}+2\varepsilon^{2k}+\varepsilon^k}{\varepsilon^{2k}+\varepsilon^k+1}$

41. Calcula los coeficientes del polinomio $P(x) = \sum_{k=0}^{n-1}(x - \varepsilon^k)^n$ siendo ε una raíz n-ésima primitiva de la unidad.

42. Calcula $\prod_{i=1}^{n}(\varepsilon_i^2 + 1)$ siendo $\{\varepsilon_i\}$ las raíces n-ésimas de la unidad.

43. Calcula la suma $s = \sum_{k=1}^{n-1} k\, cos(\frac{2k\pi}{n})$.

44. Calcula la suma $s = cos\,\frac{\pi}{11} + cos\,\frac{3\pi}{11} + cos\,\frac{5\pi}{11} + cos\,\frac{7\pi}{11} + cos\,\frac{9\pi}{11}$.

45. Calcula la suma $\sum_{k=1}^{6} \frac{1}{sen^2\frac{k\pi}{7}}$.

46. Calcula $\prod_{k=1}^{m-1} sen\,\frac{k\pi}{2m}$.

47. Calcula $\sum_{i\neq j\neq k} \frac{\alpha_i^2}{\alpha_j+\alpha_k}$, donde $\{\alpha_i\}$ son las raíces de $x^3 + x^2 - 2x - 1$.

48. Sea $P(x) \in \mathbb{C}[x]$. Prueba que si $\alpha_1 \in \mathbb{C}$ verifica las relaciones $P(\alpha_1) = P''(\alpha_1) = 0$ y $P'(\alpha_1) \neq 0$, entonces $\sum_{i=2}^{n} \frac{1}{\alpha_1-\alpha_i} = 0$.

49. Si $P(x)$ es mónico y $\{\alpha_1, \ldots, \alpha_n\}$, $\{\alpha'_1, \ldots, \alpha'_{n-1}\}$ son las raíces de $P(x), P'(x)$, respectivamente, demuestra que $n^n \prod_{i=1}^{n-1} P(\alpha'_i)$ es igual al término independiente del polinomio de raíces $(\alpha_i - \alpha_j)^2$ (con $i < j$).

50. Prueba que el polinomio $P(x) = \frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1$ no tiene raíces múltiples.

51. Determina la multiplicidad de la raíz 1 de los polinomios $x^{2n} - nx^{n+1} + nx^{n-1} - 1$ y $x^{2n+1} - (2n+1)x^{n+1} + (2n+1)x^n - 1$.

52. Demuestra que el polinomio $x^{n_1} + x^{n_2} + \cdots + x^{n_k}$ es divisible por $x^{k-1} + \cdots + x + 1$ si $n_r = r - 1 \ mod\, k$.

53. Halla los valores de m para los cuales $(x+1)^m - x^m - 1$ es divisible por $x^2 + x + 1$.

54. Halla el discriminante de $\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1$.

55. Demuestra que el discriminante de $x^n + qx + p$ es

$$(-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

56. Calcula todas las raíces reales de $x^3 + 3x^2 - 1$ con un error de una décima.

57. Calcula el número de las raíces reales positivas de $x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$.

58. Calcula los excesos de la fracción $\frac{-4x^5+26x^4+4x^3-33x^2+98x+5}{2x^4-13x^3+10x-49}$ en los intervalos siguientes $(-\infty,-3)$, $(-3,0)$, $(0,3)$ y $(3,\infty)$.

59. Calcula el número de vueltas alrededor del origen de la curva cerrada

$$x = \frac{t^2}{t^2+1},\ y = \frac{t^4 + 2t^3 + 5t^2 - 2t - 1}{t^2+1} \quad (-1 \le t \le 1).$$

60. Calcula el número de vueltas alrededor del punto $(1,1)$ de la curva cerrada

$$x = \frac{t^4 - 1}{t^4+1},\ y = \frac{t^2}{t^2+1} \quad (-1 \le t \le 1).$$

61. Calcula el número de vueltas alrededor del origen de la curva cerrada

$$w = z^5 + z + 1,\ |z| = 1.$$

62. Prueba que:

    a) $a_0t^3 + a_1t^2 + a_2t + a_3$ es de Hurwitz si y solo si a_0, a_1, a_2, a_3 tienen el mismo signo y $a_1a_2 - a_0a_3 > 0$.

    b) $a_0t^4 + a_1t^3 + a_2t^2 + a_3t + a_4$ es de Hurwitz si y solo si a_0, a_1, a_2, a_3, a_4 tienen el mismo signo y $(a_1a_2a_3 - a_3^2a_0 - a_1^2a_4)/a_0 > 0$.

Capítulo 2

Teoría de Galois

2.1. Introducción

Consideremos un polinomio $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$. Las raíces de este polinomio verifican ciertas relaciones $\mathbb{Q}$-algebraicas. El grupo G formado por las permutaciones de las raíces que respetan estas relaciones (es decir, si $\alpha_1, \ldots, \alpha_n$ cumplen cierta relación algebraica y $\sigma \in G$, entonces $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ también la cumplen) se denomina el grupo de la ecuación $p(x) = 0$. Si $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de descomposición de $p(x)$, es decir, es el mínimo subcuerpo de $\mathbb{C}$ que contiene a las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$, se demuestra que G coincide con el grupo de todos los automorfismos de cuerpos de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Se dice que un grupo G es resoluble si existe una cadena de subgrupos

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s = G \qquad (*)$$

de modo que G_{i-1} es normal en G_i y el orden de G_i/G_{i-1} es primo, para todo i.

Se dice que las raíces de $p(x)$ se obtienen por radicales, si pueden expresarse mediante las cuatro operaciones fundamentales (suma, resta, producto y división) y la toma de radicales ($\sqrt[s]{\ }$), de números racionales.

La teoría de Galois prueba que las raíces de $p(x)$ pueden obtenerse por radicales si y solo si el grupo, G, de la ecuación $p(x) = 0$ es resoluble; y si es conocida la cadena $(*)$, da el procedimiento para calcular las raíces de $p(x)$.

En general, los polinomios de grado n tiene como grupo el grupo de permutaciones S_n. Estos grupos, como probaremos, solo son resolubles para $n = 2, 3, 4$. De esto se deduce que las raíces de las ecuaciones de grado $2, 3$ y 4 pueden obtenerse por radicales.

Por ejemplo, probamos que las raíces $\alpha_1, \alpha_2, \alpha_3$ de $p(x) = x^3 + a_1x^2 + a_2x + a_3$ son

$$\alpha_i = \frac{1}{3}\Big(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\Big)$$

Por otra parte, se obtiene que en general las raíces de las ecuaciones de grado superior a 4 no se pueden expresar mediante radicales.

Históricamente al estudiar las raíces de un polinomio aparecieron los cuerpos $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, como objetos que aclaraban y simplificaban la teoría. Aparecieron los grupos: el grupo de las permutaciones "admisibles" de las raíces de $p(x)$. Recordemos que decíamos que el grupo de permutaciones "admisibles" de las raíces coincide con el grupo G de automorfismos del cuerpo $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Apareció la noción de invariantes por la acción de un grupo: Dado un subgrupo $H \subseteq G$, el subcuerpo de los invariantes de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ por H, que denotamos $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^H$, está definido por

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^H := \{a \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \colon h(a) = a,\ \forall h \in H\}$$

Por el teorema de Artin, $\mathbb{Q} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^G$. Si G es un grupo resoluble y tenemos la cadena de subgrupos

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s = G \qquad (*)$$

de modo que G_{i-1} es normal en G_i y el orden de G_i/G_{i-1} es un número primo p_i, para cada i, entonces tenemos la cadena de subcuerpos de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$,

$$\mathbb{Q} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^G \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_{s-1}} \subset \cdots \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_1} \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

El teorema 90 de Hilbert, prueba que existen $a_i \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i}$ (calculables) tales que

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_{i-1}} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} + \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} \cdot \sqrt[p_i]{a_i} + \cdots + \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} \cdot (\sqrt[p_i]{a_i})^{p_i - 1}$$

Así, $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ se podrán expresar mediante radicales, afirmación que hemos enunciado más arriba.

La Teoría de Galois resuelve los clásicos problemas de construcción con regla y compás. Demos algunos ejemplos:

1. Dice qué polígonos regulares podemos construir (con regla y compás). Por ejemplo, los polígonos regulares de n lados que podemos construir, para $n < 50000$ cumplen

$$n = 2^{m_1} \cdot 3^{m_2} \cdot 5^{m_3} \cdot 17^{m_4} \cdot 257^{m_5}, \qquad m_1 \geq 0, 0 \leq m_2, \ldots, m_5 \leq 1$$

2. Demuestra que la cuadratura del círculo es imposible. No se puede construir con regla y compás un cuadrado de área la del círculo unidad.

3. Demuestra que no se puede construir un cubo de volumen 2.

4. Demuestra que en general, los ángulos no se pueden trisectar.

El estudio de las raíces del polinomio $p(x)$ es equivalente al estudio de la $\mathbb{Q}$-álgebra conmutativa $\mathbb{Q}[x]/(p(x))$. Pasar del Álgebra Conmutativa a la Geometría Algebraica es pasar de estudiar los anillos $A = \mathbb{Q}[x_1,\dots,x_n]/(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))$ a estudiar sus espectros primos, $X = \operatorname{Spec} A$, y recíprocamente, pasar de Geometría Algebraica al Álgebra Conmutativa es pasar de estudiar las variedades algebraicas a estudiar los anillos de funciones algebraicas de dichas variedades.

Sea $A = \mathbb{Q}[x]/(p(x))$ y $K \subseteq \mathbb{C}$ un subcuerpo. El teorema chino de los restos muestra que $A \otimes_{\mathbb{Q}} K$ es isomorfa a un "álgebra trivial" $K \times \overset{n}{\cdots} \times K$ si y solo si K contiene todas las raíces, $\alpha_1,\dots,\alpha_n$, de $p(x)$ (estamos suponiendo que $p(x)$ no tiene raíces múltiples, por ejemplo cuando sea irreducible). $K = \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ es el mínimo cuerpo tal que $A \otimes_{\mathbb{Q}} K$ es trivial. Además, probamos que $K' \subset \mathbb{C}$ es un subcuerpo de $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ si solo si $K' \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ es trivial. $K \subset \mathbb{C}$ es igual al cuerpo de descomposición de un polinomio si y solo si $K \otimes_{\mathbb{Q}} K$ es trivial.

Así pues, si $X = \operatorname{Spec} k[x]/(p(x))$ entonces $Z = \operatorname{Spec} k(\alpha_1,\dots,\alpha_n)$ es la mínima variedad tal que $X \times Z = Z \coprod \overset{n}{\cdots} \coprod Z$. Además se cumple que $Z \times Z = Z \coprod \overset{m}{\cdots} \coprod Z$ y que para todo epimorfismo $Z \to Z'$ entonces $Z' \times Z = Z \coprod \overset{r}{\cdots} \coprod Z$.

En la Teoría de Galois hay dos procesos fundamentales. El proceso de "trivialización", que consiste en cambiar de cuerpo base, de $\mathbb{Q}$ a $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$, es decir, tensar por $\otimes_{\mathbb{Q}}\mathbb{Q}(\alpha_1,\dots,\alpha_n)$, y el proceso inverso de toma de invariantes por el grupo G. Múltiples cuestiones se resuelven primero por cambio de base de $\mathbb{Q}$ a $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$, y por toma de invariantes por G volvemos a $\mathbb{Q}$. Geométricamente: Sea G el grupo de automorfismos de $Z = \operatorname{Spec} \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ y sea un epimorfismo $Z \to Z'$, entonces tenemos los procesos

$$Z' \rightsquigarrow Z' \times Z = Z \coprod \cdots \coprod Z \rightsquigarrow (Z' \times Z)/G = Z'$$

Tanto $k[x]/(p(x))$ como $k(\alpha_1,\dots,\alpha_n)$ son k-álgebras finitas. En el estudio de las variedades algebraicas es obligado comenzar con las variedades algebraicas de dimensión cero, es decir, con el estudio (del espectro primo) de las k-álgebras finitas. Puede decirse que la Teoría de Galois estudia las variedades algebraicas de dimensión cero.

En Topología (y Geometría Diferencial) hay la correspondiente teoría de Galois de revestimientos. Aquí, en vez de tratar con los anillos vamos a tratar con los espacios topológicos. Un revestimiento es una aplicación continua epiyectiva $f : X \to Y$ (suele suponerse Y conexo), de modo que para cada punto $y \in Y$ existe un entorno U_y de y, de modo que $f^{-1}(U_y) = U_y \coprod \overset{n}{\cdots} \coprod U_y$. Si $f' : Y' \to Y$ es una aplicación continua, se

define $X \times_Y Y' := \{(x, y') \in X \times Y' : f(x) = f'(y')\}$. Si consideramos la inclusión $U_y \hookrightarrow Y$, se cumple que $f^{-1}(U_y) = X \times_Y U_y$. Pues bien, si $f : X \to Y$ es un revestimiento existe un revestimiento mínimo $f' : Y' \to Y$, de modo que $X \times_Y Y' = Y' \coprod \overset{n}{\cdots} \coprod Y'$, además se cumple que $Y' \times_Y Y' = Y' \coprod \overset{m}{\cdots} \coprod Y'$. En el estudio del revestimiento $X \to Y$ es fundamental el estudio del grupo $G = \mathrm{Aut}_Y(Y') := \{$ Homeomorfismos $\sigma : Y' \to Y'$, tales que $f' \circ \sigma = f'\}$. El estudio de los revestimientos de los espacios topológicos, la teoría de Galois de los revestimientos topológicos, es fundamental para la clasificación de los espacios topológicos.

La noción de revestimiento equivalente en Geometría Algebraica será la de morfismo finito plano. Los morfismos finitos son los morfismos cerrados de fibras finitas. Si imponemos además, que el número de puntos de las fibras sea localmente constante, estaremos considerando morfismos finitos planos. Por último, si queremos que las fibras sean puntos separados, es decir, que no aparezcan multiplicidades, tendremos que imponer que $\Omega_{Y/X} = 0$ (que ya definiremos con precisión). En Geometría Algebraica, $f : Y \to X$ es un revestimiento no ramificado, si es un morfismo finito, plano y $\Omega_{Y/X} = 0$. Ahora bien, el lector no debe engañarse, pues no es cierto que para cada punto $x \in X$, existe un entorno abierto U de x de modo que $f^{-1}(U) = U \coprod \overset{n}{\cdots} \coprod U$. Una intuición genial de Grothendieck, fue la de llamar abierto a los morfismos planos. Ahora sí, para cada $y \in Y$ existirá un morfismo plano $i : U \to X$, con $x \in i(U)$, de modo que $f^{-1}(U) := Y \times_X U = U \coprod \overset{n}{\cdots} \coprod U$.

Breve reseña histórica: Una tablilla babilónica del 1600 antes de Cristo plantea problemas que se reducen al problema de resolver ecuaciones de segundo grado, y da métodos para resolverlas, si bien no usaban aún ninguna notación algebraica. Los antiguos griegos resolvieron ecuaciones de segundo grado por medios geométricos. Incluso desarrollaron métodos aplicables a ecuaciones de tercer grado, mediante el corte de cónicas, de nuevo sin ninguna formulación algebraica.

Ya en el Renacimiento italiano, parece ser que Scipio del Ferro resolvió las ecuaciones cúbicas (ya con notación algebraica). En 1535, en una competición pública, Tartaglia frente a Fior (discípulo de Ferro) demostró haber redescubierto el método de resolución de las ecuaciones cúbicas, pero se negó a contar los detalles. Se los contó bajo secreto de juramento a Cardano, el cual publicó en su Ars Magna. El Ars Magna contenía también un método, debido a Ferrari, para resolver la ecuación de cuarto grado, reduciéndola a una cúbica.

A partir de entonces mucho matemáticos intentaron resolver las ecuaciones de quinto grado. Euler fracasó en el intento de resolverlas, pero encontró nuevos métodos para resolver las cuárticas. Lagrange en 1770 mostró que el método de resolución de las cúbicas y cuárticas dependía de encontrar ciertas funciones en las raíces que fueran invariantes por ciertas permutaciones de éstas; y mostró que este método fallaba con las quínticas. Abel en 1824 probó que la ecuación general de quinto grado no es

resoluble por radicales. Por último, Galois ("desenterrado" para la Historia en 1843 por Liouville) resolvió con éxito el problema de determinar cuándo las raíces de una ecuación polinómica pueden resolverse por radicales.

2.2. k-álgebras finitas triviales y racionales

Sea A una k-álgebra finita. Por el teorema 0.6.70, $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ es un número finito de puntos cerrados y $A = A_{x_1} \times \cdots \times A_{x_n}$. Además, A es reducida si y solo si es producto directo de un número finito de cuerpos y A es íntegra si y solo si es cuerpo. Por último, si $f : A \hookrightarrow B$ es un morfismo de anillos inyectivo, entonces $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo.

1. Definición: Diremos que una k-álgebra finita A es trivial si existe un isomorfismo de k-álgebras

$$A \simeq k \times \ldots \times k.$$

Si $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, con $\alpha_i \neq \alpha_j$ cuando $i \neq j$, entonces por el teorema chino de los restos 0.3.10

$$k[x]/(p(x)) = k[x]/(x - \alpha_1) \times \overset{n}{\cdots} \times k[x]/(x - \alpha_n) = k \times \overset{n}{\cdots} \times k$$

es una k-álgebra trivial.

2. Ejercicio: Prueba:

1. Si A es una k-álgebra finita trivial, entonces A_K es una K-álgebra trivial, para toda extensión de cuerpos $k \to K$.
2. El producto tensorial y el producto directo de dos k-álgebras finitas triviales es una k-álgebra finita trivial.

3. Proposición: *El cociente de una k-álgebra finita trivial por un ideal es una k-álgebra finita trivial.*

Demostración. Dado un ideal $I \subseteq k \times \overset{n}{\cdots} \times k$, tenemos que $I = I_1 \times \cdots \times I_n$, donde los ideales $I_i \subseteq k$ o son nulos o iguales a k. Por tanto,

$$(k \times \overset{n}{\cdots} \times k)/I = (k/I_1) \times \cdots \times (k/I_n)$$

es una k-álgebra trivial □

4. Proposición: *Las subálgebras de una k-álgebra finita trivial son triviales.*

Demostración. Si $A \subseteq k^n$ entonces $\operatorname{rad} A \subseteq \operatorname{rad} k^n = 0$. Por tanto, $A = K_1 \times \cdots \times K_r$ es producto directo de cuerpos. Sean $\pi_i \colon k^n \to k$ la proyección en el factor i-ésimo. Sea i, tal que la composición $K_1 = K_1 \times 0 \times \cdots \times 0 \hookrightarrow A \hookrightarrow k^n \xrightarrow{\pi_i} k$ no es nula. Como el núcleo de la composición es un ideal, que no es K_1, ha de ser 0. Luego, $K_1 = k$, e igual decimos de $K_2, \ldots, K_r$. □

5. Proposición: *Sea A una k-álgebra finita A. Entonces*

$$\#\operatorname{Spec} A \leq \dim_k A.$$

Además, $\#\operatorname{Spec} A = \dim_k A$ si y solo si A es trivial.

Demostración. Si $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$, entonces (0.6.64)

$$A = A_{x_1} \times \ldots \times A_{x_n}.$$

Así pues, $\#\operatorname{Spec} A \leq \dim_k A$. Además, $\#\operatorname{Spec} A = \dim_k A$ si y solo si $\dim_k A_{x_i} = 1$, para todo i, es decir, si y solo si A es trivial. □

Recordemos que dada una k-álgebra A, decimos que $x \in \operatorname{Spec} A$ es un punto racional si $A/\mathfrak{p}_x = k$.

6. Definición: Sea A una k-álgebra finita. Diremos que A es racional si todos los puntos de su espectro son racionales. Diremos que una extensión de cuerpos $k \hookrightarrow K$ racionaliza a una k-álgebra A si $A \otimes_k K$ es una K-álgebra racional.

7. Ejemplo: $k[x]/(x^n)$ es una k-álgebra racional.

8. Observaciones:

1. Una k-álgebra finita A es racional si y solo si $A_{\mathrm{red}} = A/(\operatorname{rad} A)$ es trivial: Observemos que si A es una k-álgebra finita entonces $A = A_1 \times \cdots \times A_n$, con A_i locales (de ideales maximales $\mathfrak{p}_i$). Luego, $\operatorname{rad} A = \operatorname{rad} A_1 \times \cdots \operatorname{rad} A_n = \mathfrak{p}_1 \times \cdots \times \mathfrak{p}_n$ y y $A/\operatorname{rad} A = A_1/\mathfrak{p}_1 \times \cdots \times A_n/\mathfrak{p}_n$.

2. Si A es una k-álgebra finita racional y $k \hookrightarrow K$ una extensión de cuerpos, entonces $A \otimes_k K$ es una K-álgebra finita racional. En efecto, los elementos del ideal $(\operatorname{rad} A) \otimes_k K$ son nilpotentes, luego la K-álgebra $(A \otimes_k K)_{\mathrm{red}}$ es el cociente de $(A \otimes_k K)/(\operatorname{rad} A) \otimes_k K) = (A/\operatorname{rad} A) \otimes_k K$, que es una K-álgebra trivial, por su radical, que es nulo. Luego $(A \otimes_k K)_{\mathrm{red}} = A_{\mathrm{red}} \otimes_k K$ y es trivial.

3. Toda subálgebra y todo cociente de una k-álgebra racional es racional, porque toda subálgebra y todo cociente de una k-álgebra trivial es trivial.

4. El producto tensorial de dos k-álgebras finitas racionales es una k-álgebra finita racional.

9. Ejercicio : Sea $A = k[x]/(p(x))$. Prueba que A es racional si y solo si $p(x)$ descompone en producto de factores simples $(x - \alpha_i)$ (repetidos o no). Prueba que $A \otimes_k K$ es una K-álgebra racional si y solo si K contiene todas las raíces de $p(x)$.

10. Teorema (Kronecker) : *Si $k \hookrightarrow A$ es una k-álgebra finita, existe una extensión finita de cuerpos $k \hookrightarrow K$, de modo que $A \otimes_k K$ es una K-álgebra finita racional.*

Si $k \hookrightarrow K'$ es otra extensión de cuerpos que racionaliza a la k-álgebra A entonces $\#\operatorname{Spec}(A \otimes_k K') = \#\operatorname{Spec}(A \otimes_k K)$.

Demostración. Procedemos por inducción sobre la dimensión de A, siendo el caso de dimensión uno inmediato. Sea K un cuerpo residual de A, que es una extensión finita de k. Por la fórmula de los puntos, el morfismo de paso al cociente $A \to K$ se corresponde con un punto racional de A_K. Por el teorema de descomposición se tiene que A_K descompone

$$A_K = A' \times A''$$

con A' una K-álgebra finita local y racional. Ahora,

$$\dim_K A'' < \dim_K A_K = \dim_k A$$

luego por inducción existe una extensión finita de cuerpos $K \to \Sigma$ que racionaliza a A''. Entonces $k \to \Sigma$ es una extensión finita de cuerpos que racionaliza a A; en efecto:

$$A \underset{k}{\otimes} \Sigma = (A \underset{k}{\otimes} K) \underset{K}{\otimes} \Sigma = (A' \times A'')_\Sigma = A'_\Sigma \times A''_\Sigma$$

que es una Σ-álgebra racional.

Si K'' es una extensión de cuerpos de K entonces racionaliza a A, ya que $A \otimes_k K'' = (A \otimes_k K) \otimes_K K''$. Además, $(A \otimes_k K)_{red} = K^n$, luego $(A \otimes_k K'')_{red} = (A \otimes_k K)_{red} \otimes_K K'' = K''^n$ y por tanto $\#\operatorname{Spec}(A \otimes_k K'') = n = \#\operatorname{Spec}(A \otimes_k K)$.

Si K' es una extensión racionalizante de A, sea K'' un compuesto de K y K'. Entonces, $\#\operatorname{Spec}(A \otimes_k K') = \#\operatorname{Spec}(A \otimes_k K'') = \#\operatorname{Spec}(A \otimes_k K)$.

□

Dado un punto racional $x \in \operatorname{Spec} A$ tenemos definido el morfismo de paso al cociente $A \to A/\mathfrak{p}_x = k$. Recíprocamente, dado un morfismo $\phi\colon A \to k$, entonces $\mathfrak{p}_x = \operatorname{Ker}\phi$ es un punto racional. En conclusión,

$$\operatorname{Hom}_{k-alg}(A, k) = \{\text{Puntos racionales de } A\} \subseteq \operatorname{Spec} A$$

11. Ejercicio: Demuestra la igualdad $\mathrm{Hom}_{k-alg}(k[x]/(p(x)),K) = \{\text{Raíces de } p(x) \text{ en } K\}$, $f \mapsto f(\bar{x})$.

12. Fórmula de los puntos: *Sea A una k-álgebra y $k \to K$ una extensión de cuerpos. Entonces*

$$\mathrm{Hom}_{k-alg}(A,K) \overset{0.8.13}{=} \mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \{\textit{Puntos } K\textit{-racionales de } A \otimes_k K\}$$

En particular, $\#\mathrm{Hom}_{k-alg}(A,K) \leq \#\mathrm{Spec}(A \otimes_k K)$.

La fórmula de los puntos puede entenderse como la correspondencia biunívoca que hay entre los morfismos y sus gráficas (véase 3.8.18).

13. Definición: Diremos que $\mathrm{Hom}_{k-alg}(A,K)$ son los puntos de A con valores en K.

Si $A = k[x]/(p(x))$, sus puntos con valores en K son las raíces de $p(x)$ en K.

14. Proposición: *Una k-álgebra finita A es racional si y solo si* $\#\mathrm{Hom}_{k-alg}(A,k) = \#\mathrm{Spec}A$. *Una extensión de cuerpos $k \hookrightarrow K$ racionaliza a la k-álgebra finita A si y solo si* $\#\mathrm{Hom}_{k-alg}(A,K) = \#\mathrm{Spec}(A \otimes_k K)$.

Demostración. La primera parte es inmediata y la segunda es consecuencia de la fórmula de los puntos. □

15. Lema: *Sea A una k-álgebra finita, K una extensión de cuerpos de k que racionalice a A y $n = \#\mathrm{Spec}(A \otimes_k K) = \#\mathrm{Hom}_{k-alg}(A,K)$. Dada una extensión de cuerpos $k \hookrightarrow \Sigma$ se cumple que*

$$\#\mathrm{Hom}_{k-alg}(A,\Sigma) \leq n$$

y se cumple la igualdad si y solo si Σ racionaliza a A.

Demostración. Si $k \hookrightarrow K'$ racionaliza a A, entonces

$$\#\mathrm{Hom}_{k-alg}(A,K') = \#\mathrm{Spec}(A \otimes_k K') \overset{2.2.10}{=} \#\mathrm{Spec}(A \otimes_k K) = \#\mathrm{Hom}_{k-alg}(A,K).$$

Sea Σ' un compuesto de Σ y K. Entonces

$$\#\mathrm{Hom}_{k-alg}(A,\Sigma) \leq \#\mathrm{Hom}_{k-alg}(A,\Sigma') = n$$

Si $\#\mathrm{Hom}_{k-alg}(A,\Sigma) = n$, como $\#\mathrm{Spec}(A \otimes_k \Sigma) \leq \#\mathrm{Spec}(A \otimes_k \Sigma') = n$, tendremos que $\#\mathrm{Hom}_{k-alg}(A,\Sigma) = \#\mathrm{Spec}(A \otimes_k \Sigma)$ y Σ racionaliza a A.

□

16. Definición: Se dice que una extensión finita de cuerpos $k \hookrightarrow K$ es normal si $K \otimes_k K$ es una K-álgebra racional.

17. Teorema: *Sea $k \hookrightarrow A$ una k-álgebra finita. Existe una extensión mínima de cuerpos que racionaliza a A. Además, es única salvo isomorfismos y es normal.*

Demostración. Sea $k \hookrightarrow K$ una extensión que racionalice a A. Entonces,

$$\#\mathrm{Hom}_{k-alg}(A,K) = \#\mathrm{Spec}(A \otimes_k K) = n.$$

Sea $\{\phi_1,\ldots,\phi_n\} = \mathrm{Hom}_{k-alg}(A,K)$ y $\phi\colon A \otimes_k \overset{n}{\ldots} \otimes_k A \to K$, el morfismo de k-álgebras definido por $\phi(a_1 \otimes_k \ldots \otimes_k a_n) := \phi_1(a_1)\cdot\ldots\cdot\phi_n(a_n)$. $\Sigma = \mathrm{Im}\,\phi$, es una extensión que racionaliza a A, porque $\#\mathrm{Hom}_{k-alg}(A,\Sigma) = n$. Σ es un cociente de $A \otimes_k \ldots \otimes_k A$, que está racionalizada por Σ, luego Σ racionaliza a Σ, es decir, es normal. De nuevo, si una extensión racionaliza a A, racionalizará a Σ, en particular, la contiene. De aquí se obtiene la unicidad y minimalidad de Σ. □

18. Definición: Si $k \hookrightarrow A$ es una k-álgebra finita, denominaremos envolvente normal de A sobre k, a la extensión mínima racionalizante de A. Si $A = k[x]/(p(x))$, la extensión mínima que racionaliza a A, es el mínimo cuerpo que contiene a las raíces de $p(x)$. Cuerpo que denominaremos cuerpo de descomposición de $p(x)$, que es una extensión normal de k.

19. Observación: La envolvente normal está caracterizada por ser la única extensión (salvo isomorfismos) que racionaliza a A y que es un cociente de un producto tensorial $A \otimes_k \cdots \otimes_k A$. En efecto, si $k \to \Omega$ es otra extensión que racionalice a A y que sea cociente de $A \otimes_k \cdots \otimes_k A$, entonces K racionaliza a Ω (pues racionaliza a A, luego a $A \otimes_k \cdots \otimes_k A$, luego a Ω por ser un cociente) y análogamente Ω racionaliza a K. Por tanto

$$\prod K \simeq (K \otimes_k \Omega)_{\mathrm{red}} \simeq \prod \Omega$$

luego $K \simeq \Omega$.

20. Proposición: *Sea $k \to K$ una extensión finita. Las siguientes condiciones son equivalentes:*

1. *K es una extensión normal de k.*
2. *Si $p(x) \in k[x]$ es un polinomio irreducible que tiene una raíz en K, entonces todas las raíces de $p(x)$ están en K (definición clásica de extensión de normal).*
3. *K es el cuerpo de descomposición de un polinomio.*

4. *"Agujero único en el cierre algebraico": Existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de k-álgebras de K.*

Demostración. 1. $\Rightarrow$ 2.. Sea K una extensión normal de k, y sea $p(x) \in k[x]$ un polinomio irreducible que tiene una raíz en K. Dar una raíz equivale a dar un morfismo

$$k[x]/(p(x)) \to K$$

necesariamente inyectivo, pues $k[x]/(p(x))$ es cuerpo, ya que $p(x)$ es irreducible. Tensando por K obtenemos

$$K[x]/(p(x)) = k[x]/(p(x)) \underset{k}{\otimes} K \hookrightarrow K \underset{k}{\otimes} K$$

y como $K \underset{k}{\otimes} K$ es racional, $K[x]/(p(x))$ también, es decir $p(x)$ tiene todas sus raíces en K.

2. $\Rightarrow$ 3. $K = k[\alpha_1, \dots, \alpha_n]$ y sea $p_i(x)$ el polinomio mínimo anulador de α_i, para cada i. Todas las raíces de $p_i(x)$ están en K. Obviamente, K es el cuerpo de descomposición de $p(x) := p_1(x) \cdots p_n(x)$.

3 $\Rightarrow$ 1. Obvio.

1. $\Leftrightarrow$ 4. K es normal si y solo K la racionaliza. Por el Lema 2.2.15, K racionaliza a K si y solo si $\mathrm{Hom}_{k-alg}(K, \bar{k}) = \mathrm{Hom}_{k-alg}(K, K)$.

□

21. Teorema de prolongación: *Sea $i : K' \hookrightarrow K$ un morfismo entre k-extensiones finitas de cuerpos, con $k \hookrightarrow K$ normal. El morfismo natural*

$$\mathrm{Hom}_{k-alg}(K, K) \to \mathrm{Hom}_{k-alg}(K', K), \qquad \phi \mapsto \phi \circ i$$

es epiyectivo.

Demostración. Por cambio de base tenemos el morfismo inyectivo $K' \otimes_k K \hookrightarrow K \otimes_k K$. Como $K \otimes_k K$ es K-racional entonces $K' \otimes_k K$ es K-racional. Ahora ya, por la fórmula de los puntos,

$$\begin{array}{ccc} \mathrm{Hom}_{k-alg}(K, K) & \longrightarrow & \mathrm{Hom}_{k-alg}(K', K) \\ \| & & \| \\ \mathrm{Spec}(K \otimes_k K) & & \mathrm{Spec}(K' \otimes_k K) \end{array}$$

concluimos el epimorfismo, por 0.6.67. □

2.3. k-álgebras finitas separables. Trivialización

1. Definición: Se dice que una k-álgebra finita A es separable si existe una extensión cuerpos $k \hookrightarrow K$ tal que $A \otimes_k K = \prod_i K$. También se dice que A es separable sobre k.

Las k-álgebras finitas triviales son k-álgebras finitas separables.

2. Ejercicio: La k-álgebra $k[x]/(p(x))$ es separable si y solo si $p(x)$ y $p'(x)$ son primos entre sí, es decir, $p(x)$ no tiene raíces múltiples.

3. Observación: Si Σ trivializa a A cualquier extensión, Σ', de Σ también trivializa a A, porque $A \otimes_k \Sigma' = (A \otimes_k \Sigma) \otimes_\Sigma \Sigma'$.

4. Ejercicio: Prueba:

- $A \times B$ es separable si y solo si A y B lo son.

- El producto tensorial (sobre k) de álgebras separables (sobre k) es separable (sobre k).

- Subálgebras y cocientes de álgebras separables son separables.

5. Proposición: *Sea A una k-álgebra finita y $k \to K$ una extensión de cuerpos. Entonces A es separable sobre k si y solo si A_K es separable sobre K.*

Demostración. Si A es separable, sea Σ una extensión trivializante de A y Σ' un compuesto de K y Σ, entonces $(A \otimes_k K) \otimes_K \Sigma' = A \otimes_k \Sigma'$ es Σ'-trivial y $A \otimes_k K$ es K-separable.

Si A_K es una K-álgebra separable, sea Σ una K-extensión trivializante de A_K. Entonces, $A \otimes_k \Sigma = A_K \otimes_K \Sigma$ es Σ-trivial y A es k-separable.

□

6. Proposición: *Una k-álgebra finita es separable si y solo si A_K es reducida, para toda extensión $k \to K$.*

Demostración. Sea A separable sobre k y $k \to K'$ una extensión cualquiera. Veamos que $A \otimes_k K'$ es reducida. Sea $k \to K$ una extensión que trivializa a A y K'' un compuesto de K y K'. Entonces

$$(A \otimes_k K') \otimes_{K'} K'' = A \otimes_k K'' = (A \otimes_k K) \otimes_K K'' = \prod K''$$

Ahora bien, $A \otimes_k K'$ es una subálgebra de $\prod K''$, luego es reducida.

Recíprocamente, si A es reducida por todo cambio de base, considerando un cambio de base $k \to K$ racionalizante, se obtiene que A_K es racional y reducida, luego trivial.

□

7. Proposición: *Una extensión de cuerpos $k \hookrightarrow K$ trivializa a una k-álgebra finita A si y solo si*

$$\#\mathrm{Hom}_{k-alg}(A,K) = \dim_k A.$$

Demostración. Por la fórmula de los puntos, $\mathrm{Hom}_{k-alg}(A,K)$ son los puntos K-racionales de $A \otimes_k K$. Ahora bien, $A \otimes_k K$ es una K-álgebra trivial si y solo si el número de sus puntos K-racionales coincide con $\dim_K A_K$. Como $\dim_k A = \dim_K A_K$, se concluye. □

8. Proposición: *Sea k un cuerpo con infinitos elementos y A una k-álgebra finita separable. Existe un elemento $a \in A$ tal que $A = k[a]$. Dicho elemento se denomina elemento primitivo de A.*

Demostración. Sea $k \to K$ una extensión de cuerpos que trivialice a A. Si $\dim_k A = n$, entonces A tiene n puntos con valores en K. Escribamos $\{\phi_1,\dots,\phi_n\} = \mathrm{Hom}_{k-\text{álg}}(A,K)$. Consideremos en A los hiperplanos $H_{ij} = \mathrm{Ker}(\phi_i - \phi_j)$, $i \neq j$. Sea $a \in A$ un elemento que no pertenezca a ninguno de dichos hiperplanos. Entonces, las restricciones de ϕ_i y ϕ_j a $k[a]$ son distintas, para todo $i \neq j$. Por tanto, $k[a]$ tiene al menos n puntos con valores en K, luego su dimensión es mayor o igual que n, luego $A = k[a]$. □

9. Definición: Sea A una k-álgebra finita. Se dice que un elemento $a \in A$ es separable (sobre k) si $k[a]$ es una k-álgebra separable (es decir, si el polinomio anulador mínimo de a no tiene raíces múltiples).

10. Proposición: *Una k-álgebra finita A, es separable si y solo si todos sus elementos son separables.*

Demostración. Toda subálgebra de una k-álgebra separable es separable, luego todo elemento de una k-álgebra separable es separable.

Recíprocamente, veamos que si todo elemento es separable el álgebra es separable. Si $a_1,\dots,a_r$ es una base, entonces A es un cociente de $k[a_1] \underset{k}{\otimes} \cdots \underset{k}{\otimes} k[a_n]$, luego es separable. □

Consideremos el morfismo de anillos

$$\varphi\colon \mathbb{Z} \to k,\ \varphi(n) = \begin{cases} 1 + \overset{n}{\dots} + 1 & \text{si } n > 0 \\ (-1) + \overset{-n}{\dots} + (-1) & \text{si } n < 0 \\ 0 & \text{si } n = 0 \end{cases}$$

11. Definición: Si $\operatorname{Ker}\varphi = 0$, se dice que k es un cuerpo de característica cero. En este caso, tendremos una inyección canónica $\mathbb{Q} \hookrightarrow k$. Si $\operatorname{Ker}\varphi \neq 0$, entonces $\operatorname{Ker}\varphi = (p)$, p primo. En este caso se dice que k es de característica p y tenemos una inyección canónica $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$.

12. Proposición: *Sea k un cuerpo de característica cero. Una k-álgebra finita A es separable si y solo si es reducida.*

Demostración. Si A es separable es reducida por 2.3.6.

Si A es reducida entonces es producto directo de cuerpos. En característica cero las extensiones finitas de cuerpos son separables, porque todos sus elementos son separables: En efecto, el polinomio anulador $p(x)$ de un elemento es un polinomio irreducible, luego primo con su derivada $p'(x)$ (en característica cero $p'(x) \neq 0$), luego sin raíces múltiples.

□

13. Ejemplo: Sea $\mathbb{Q} \hookrightarrow K$ una extensión finita de cuerpos y $p(x) \in K[x]$. Demos un procedimiento para descomponer $p(x)$ en producto de polinomios irreducibles en $K[x]$. Podemos suponer que $p(x)$ no tiene raíces múltiples. $A := K[x]/(p(x))$ es una $\mathbb{Q}$-álgebra finita reducida, luego separable. Sea $a \in A$ un elemento primitivo y $q(x) \in \mathbb{Q}[x]$ el polinomio mínimo anulador de a (que es igual al polinomio característco del endomorfismo $\mathbb{Q}$-lineal $A \to A$, $b \mapsto ab$). Sea $q(x) = q_1(x) \cdots q_m(x)$ la descomposición en producto de polinomios irreducibles en $\mathbb{Q}[x]$. Tenemos

$$A = K[x]/(p(x)) = \mathbb{Q}[x]/(q(x)) = \mathbb{Q}[x]/(q_1(x)) \times \cdots \times \mathbb{Q}[x]/(q_m(x)).$$

Isomorfismos que los podemos considerar como isomorfismos de K-álgebras. Vía estos isomorfismos tenemos que $\bar{x} = (\overline{y_1}, \ldots, y_m)$. Consideremos los endomorfismos K-lineales $y_i \cdot : \mathbb{Q}[x]/(q_i(x)) \to \mathbb{Q}[x]/(q_i(x))$, $\overline{q(x)} \mapsto y_i \cdot \overline{q(x)}$ y sus polinomios característicos $c_{y_i \cdot}(x)$. Entonces,

$$p(x) = c_{\bar{x}\cdot}(x) = c_{y_1 \cdot}(x) \cdots c_{y_m \cdot}(x)$$

es la descomposición de $p(x)$ en factores irreducibles.

14. Notación: Sea k un cuerpo de característica $p > 0$ y A una k-álgebra finita. Denotemos $A^p := \{a^p \in A, \text{ para todo } a \in A\}$. Denotemos $k \cdot A^p$ la subálgebra de A, definida por

$$k \cdot A^p = \{\sum_i \lambda_i a_i^p,\ \lambda_i \in k, a_i \in A\}$$

Es fácil ver que esta construcción cambia de base: $(k \cdot A^p) \otimes_k K = K \cdot (A \otimes_k K)^p$.

15. Proposición: *Sea k un cuerpo de característica $p>0$ y A una k-álgebra finita. A es separable si y solo si $A = k\cdot A^p$.*

Demostración. Cambiando de base podemos suponer que A es una k-álgebra racional. Es más podemos suponer que A es local y racional. Sea $\mathfrak{m}$ el ideal maximal de A. Tenemos $A = k\oplus\mathfrak{m}$ y $k\cdot A^p \subseteq k\oplus\mathfrak{m}^p$. Por el lema de Nakayama, $A = k\cdot A^p$ si y solo si $A = k$, es decir, si y solo si A es separable. □

2.3.1. Cuerpos perfectos

16. Definición: Un cuerpo k se dice que es perfecto si y solo si toda extensión finita de k es separable.

17. Teorema: *Los cuerpos de característica cero son perfectos.*

Demostración. Es consecuencia de la proposición 2.3.12 □

Que existan extensiones finitas de cuerpos no separables es una patología de la característica p. Por ejemplo, si $k = \mathbb{Z}/\mathfrak{p}\mathbb{Z}(x)$, entonces $k \hookrightarrow K = k[y]/(y^p - x)$ es una extensión finita de cuerpos no separable.

18. Proposición: *Sea k un cuerpo de característica $p>0$. Entonces k es perfecto si y solo si $k = k^p$, es decir, para todo $\alpha\in k$, $\sqrt[p]{\alpha}\in k$.*

Demostración. Supongamos que k es perfecto. Dado $\alpha\in k$, la extensión $k\hookrightarrow k[\sqrt[p]{\alpha}]$ es separable. El polinomio mínimo anulador de $\sqrt[p]{\alpha}$ es separable y divide a $x^p-\alpha$, que solo tiene la raíz $\sqrt[p]{\alpha}$, luego ha de ser $x-\sqrt[p]{\alpha}$ y $\sqrt[p]{\alpha}\in k$.

Veamos el recíproco. Sea $k\hookrightarrow K$ una extensión de cuerpos. Sea $\alpha\in K$ y $p(x)$ el polinomio mínimo anulador de α sobre k. Si α es un elemento no separable entonces $p'(x)=0$. Por tanto, $p(x) = q(x^p)$. El polinomio $r(x) = \sqrt[p]{q(x^p)}\in k[x]$, anula a α y es de grado menor que el de $p(x)$, lo que es contradictorio. En conclusión, toda α es separable y K es separable. □

2.3.2. Subálgebra separable maximal

19. Definición: Sea A una k-álgebra finita. Denotaremos $\pi_0^k(A)$ al conjunto de los elementos separables de A. Obviamente, $\pi_0^k(A)$ es la subálgebra separable maximal de A.

Si $A = A_1 \times A_2$ entonces $\pi_0^k(A) = \pi_0^k(A_1) \times \pi_0^k(A_2)$. Si A es local y distinta de cero, entonces $\pi_0^k(A)$ es local y no nula, pues $k \subset \pi_0^k(A)$. Con todo,

$$\operatorname{Spec} A = \operatorname{Spec} \pi_0^k(A).$$

Si la característica de k es cero y A es reducida entonces $\pi_0^k(A) = A$.

20. Proposición: *Sea k un cuerpo de característica $p > 0$ y A una k-álgebra finita. Para todo $n >> 0$, $\pi_0^k(A) = k \cdot A^{p^n}$.*

Demostración. Tenemos que $\pi_0^k(A) = k \cdot \pi_0^k(A)^p \subseteq k \cdot A^p$. Por tanto, $\pi_0^k(A) \subseteq k \cdot \pi_0^k(A)^p \subseteq k \cdot A^{p^2}$. Recurrentemente, $\pi_0^k(A) \subseteq k \cdot A^{p^n}$, para todo n. Para $n >> 0$, tendremos que $k \cdot A^{p^n} = k \cdot A^{p^{n+1}}$, luego $k \cdot A^{p^n}$ es separable y ha de coincidir con $\pi_0^k(A)$. □

21. Definición: Se dice que una k-álgebra finita A, es puramente inseparable si $\pi_0^k(A) = k$.

Si la característica de k es $p > 0$, entonces A es puramente inseparable si y solo si $k \cdot A^{p^n} = k$, para $n >> 0$.

22. Lema: *1. La composición de dos extensiones finitas de cuerpos separables es separable.*

2. Se cumple que $\pi_0^k(A) = \pi_0^k(A/\operatorname{rad} A)$. Con mayor generalidad, $\pi_0^k(A) = \pi_0^k(A/I)$ para todo ideal $I \subseteq \operatorname{rad} A$.

Demostración. 1. Sean $k \hookrightarrow K$, $K \hookrightarrow K'$ dos extensiones finitas de cuerpos separables. Sea $\bar{k}$ el cierre algebraico de k. Entonces

$$K' \otimes_k \bar{k} = K' \otimes_K K \otimes_k \bar{k} = K' \otimes_K (\prod \bar{k}) = \prod (K' \otimes_K \bar{k}) = \prod \bar{k}$$

Luego K' es una extensión k-separable.

2. Obviamente tenemos un morfismo natural $\pi_0^k(A) \to \pi_0^k(A/\operatorname{rad} A) \subset A/\operatorname{rad} A$ que es inyectivo. Nos falta probar que es epiyectivo.

Probemos en primer lugar que si $I \subset A$ es un ideal tal que $I^2 = 0$ entonces $\pi_0^k(A) = \pi_0^k(A/I^2)$: Sea $\bar{a} \in A/I$ un elemento k-separable de polinomio mínimo anulador $p(x)$. Para todo $i \in I$ tenemos que $p(a+i) = p(a) + ip'(a)$. Observemos que $p(a) \in I$ porque $\overline{p(a)} = p(\bar{a}) = 0$ en A/I. Además $p'(a)$ es invertible. En efecto, $p(x)$ y $p'(x)$ son primos entre sí, luego existen polinomios $\lambda(x)$ y $\mu(x)$ de modo que $\lambda(x)p(x) + \mu(x)p'(x) = 1$, luego $\lambda(a)p(a) + \mu(a)p'(a) = 1$, y módulo I tenemos $\mu(\bar{a})p'(\bar{a}) = 1$, es decir, $p'(a)$ módulo nilpotentes es invertible, luego es invertible. Por tanto, si tomamos $i' = -p(a)/p'(a)$

tenemos que $p(a+i') = p(a) + i'p'(a) = 0$. Por tanto, $a+i'$ es un elemento separable de A que módulo I coincide con $\bar{a}$. En conclusión, $\pi_0^k(A) = \pi_0^k(A/I)$.

Ahora en general, sea $m \in \mathbb{N}$ tal que $I^{2^m} = 0$. Entonces,

$$\pi_0^k(A/I) = \pi_0^k(A/I^2) = \pi_0^k(A/I^4) = ... = \pi_0^k(A/I^{2^m}) = \pi_0^k(A).$$

□

23. Teorema: *Si A es una k-álgebra finita y $k \hookrightarrow K$ una extensión finita de cuerpos, entonces*

$$\pi_0^k(A) \otimes_k K = \pi_0^K(A \otimes_k K).$$

Demostración. Si la característica de k es $p > 0$, entonces para todo $n >> 0$

$$\pi_0^k(A) \otimes_k K = (kA^{p^n}) \otimes_k K = K(A \otimes_k K)^{p^n} = \pi_0^K(A \otimes_k K).$$

Supongamos que la característica de $k = 0$. Por el lema anterior podemos suponer que A es reducida. En este caso A es separable y $A \otimes_k K$ también y el teorema es trivial. □

24. Corolario: *Sean A y B k-álgebras finitas. Entonces,*

$$\pi_0^k(A \otimes_k B) = \pi_0^k(A) \otimes_k \pi_0^k(B).$$

Demostración. Tenemos la inclusión $\pi_0^k(A) \otimes_k \pi_0^k(B) \hookrightarrow \pi_0^k(A \otimes_k B)$. Para ver que es epiyectivo basta verlo por cambio de base. Podemos suponer que A y B son racionales. Módulo nilpotentes, podemos suponer que A y B son triviales. En tal caso el corolario es inmediato. □

25. Corolario: *Sea A una k-álgebra finita y K una extensión de k que racionalice a A. Entonces,*

$$\dim_k \pi_0^k(A) = \#\operatorname{Spec}(A \otimes_k K) = \#\operatorname{Hom}_{k-alg}(A, K).$$

Demostración. En efecto,

$$\begin{aligned}\dim_k \pi_0^k(A) &= \dim_K(\pi_0^k(A) \otimes_k K) = \dim_K(\pi_0^K(A \otimes_k K)) = \dim_K((A \otimes_k K)/\operatorname{rad}(A \otimes_k K)) \\ &= \#\operatorname{Spec}(A \otimes_k K).\end{aligned}$$

□

26. Teorema: *Sea A una k-álgebra finita y $k \hookrightarrow K$ una extensión de cuerpos. Se cumple*

$$\#\mathrm{Hom}_{k-alg}(A,K) \leq \#\mathrm{Hom}_{k-alg}(\pi_0^k(A),K)$$

y,

$$\#\mathrm{Hom}_{k-alg}(A,K) = \dim_k \pi_0^k(A)$$

si y solo si K racionaliza a A (en este caso $\mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{k-alg}(\pi_0^k(A),K)$).

Demostración. Es consecuencia de 2.3.25 y 2.2.15.

□

2.3.3. Métrica de la traza

27. Definición: Sea $k \hookrightarrow A$ una k-álgebra finita. Todo elemento $a \in A$ define la homotecia $h_a : A \to A$, $h_a(a') = a \cdot a'$. Definimos el morfismo traza

$$\mathrm{tr} : A \to k,\ a \mapsto \mathrm{tr}(a) := \mathrm{Tr}(h_a) = \text{ traza del endomorfismo lineal } (h_a)$$

que es una aplicación k-lineal. Se define la norma como la aplicación

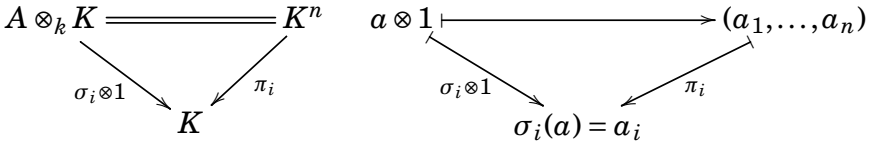
$$N : A \to k,\ a \mapsto N(a) := \det(h_a).$$

Si E es un k-espacio vectorial de dimensión finita, $T : E \to E$ un endomorfismo, $k \hookrightarrow K$ un cambio de cuerpo base y $T \otimes_k 1 : E \otimes_k K \to E \otimes_k K$, $T \otimes_k 1(e \otimes \lambda) = \lambda T(e)$, entonces la matriz asociada a la aplicación k-lineal T en una base $\{e_i\}$ coincide con la matriz asociada a la aplicación K-lineal $T \otimes 1$ en la base $\{e_i \otimes 1\}$. Por tanto, las aplicaciones traza y norma son estables por cambio de cuerpo base.

Sea A una k-álgebra separable de grado n, $k \hookrightarrow K$ una extensión de cuerpos que trivializa a A y $\mathrm{Hom}_{k-alg}(A,K) = \{\sigma_1,\ldots,\sigma_n\}$. Explicitemos el isomorfismo $A \otimes_k K = K \times \overset{n}{\cdots} \times K$. Tenemos,

$$\{\sigma_1,\ldots,\sigma_n\} = \mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \mathrm{Hom}_{K-alg}(K^n,K) = \{\pi_1,\ldots,\pi_n\}$$

donde π_i es la proyección en el factor i. De los diagramas conmutativos



se deduce, que el isomorfismo $A \otimes_k K = K^n$, asigna $a \otimes \lambda$ en $(\sigma_1(a) \cdot \lambda, \ldots, \sigma_n(a) \cdot \lambda)$.

28. Proposición: *Sea A una k-álgebra finita separable. Sea K una extensión finita de cuerpos de k, que trivialice a A. Escribamos $\{\sigma_1,\dots,\sigma_n\} = \mathrm{Hom}_{k-alg}(A,K)$. Entonces,* $\mathrm{tr}(a) = \sum_i \sigma_i(a)$ *y* $N(a) = \prod_i \sigma_i(a)$.

Demostración. Consideremos el isomorfismo

$$\phi\colon A \otimes_k K = K \times \overset{m}{\dots} \times K,\ \phi(a\otimes 1) := (\sigma_1(a),\dots,\sigma_n(a)).$$

Por tanto, $\mathrm{tr}(a) = Tr(h_a) = \mathrm{Tr}(h_{a\otimes 1}) = \mathrm{Tr}_{h_{(\sigma_1(a),\dots,\sigma_n(a))}} = \sum_i \sigma_i(a)$ e igualmente $N(a) = \prod_i \sigma_i(a)$. □

Definamos la métrica de la traza T_2^k en A:

$$T_2^k(a,a') := \mathrm{tr}(a\cdot a').$$

Como la matriz de una aplicación lineal es estable por cambio de base, tendremos que la métrica de la traza es estable por cambio de base. Es decir, para toda extensión $k \to K$ se tiene el diagrama conmutativo [1]

$$\begin{array}{ccc} A\otimes_k K & \xrightarrow{T_2^K} & A^*\otimes_k K = \mathrm{Hom}_K(A\otimes_k K, K) \\ \uparrow & & \uparrow \\ A & \xrightarrow{T_2^k} & A^* = \mathrm{Hom}_k(A,k) \end{array}$$

29. Proposición: *Sea A una k-álgebra finita. Entonces A es separable si y solo si la métrica de la traza no tiene radical.*

Demostración. Tanto la separabilidad como el radical de la métrica son estables por cambio de cuerpo de base, luego podemos suponer que A es racional. Además, la descomposición de A en producto de álgebras locales es una descomposición ortogonal para la métrica de la traza. En conclusión, podemos suponer que A es una k-álgebra finita local y racional. Sea $\mathfrak{m}$ el ideal maximal. Los elementos $a \in \mathfrak{m}$ son nilpotentes. Por tanto, la homotecia h_a, con $a \in \mathfrak{m}$, es nilpotente y su traza es nula. En conclusión, $\mathfrak{m}$ está contenido en el radical de la métrica. Si la métrica no tiene radical, entonces $\mathfrak{m} = 0$ y $A = k$, que es separable. Recíprocamente, si A es separable, entonces $\mathfrak{m} = 0$, luego $A = k$ y la métrica no tiene radical. □

[1] Denotamos igual la métrica de la traza, que la polaridad definida por la métrica de la traza.

30. Ejemplo: Consideremos $A = k[x]/(p(x))$ y sea $n = \dim_k A$ =grado de $p(x)$. Consideremos la base $1, x, x^2, \ldots, x^{n-1}$. Denotemos $\alpha_1, \ldots, \alpha_n$ a las raíces de $p(x)$. Veamos que la matriz de la métrica de la traza en dicha base es:

$$\begin{pmatrix} \sigma_0 & \sigma_1 & \ldots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \ldots & \sigma_n \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_{n-1} & \sigma_n & \ldots & \sigma_{2n-2} \end{pmatrix}$$

siendo $\sigma_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_n^i$, que es una función simétrica en $\alpha_1, \ldots, \alpha_n$ y por tanto es un polinomio en los coeficientes de $p(x)$, luego $\sigma_i \in k$. En efecto, sea $\bar{k}$ el cierre algebraico de k, el cual trivializa la k-álgebra A. $\mathrm{Hom}_{k-alg}(A, \bar{k}) = \{\sigma_1, \ldots, \sigma_n\}$ y $\sigma_i(x) = \alpha_i$, para todo i. Luego, $T_2^k(x^r, x^s) = \mathrm{tr}(x^r \cdot x^s) = \sum_i \sigma_i(x^{r+s}) = \sum_i \alpha_i^{r+s} = \sigma_{r+s}$ y se concluye.

Por último, $|T_2^k| = \Delta(p(x))$, por el teorema 1.1.10.

2.4. Extensiones de Galois

1. Definición: Diremos que una extensión finita $k \to K$ es de *Galois* si se trivializa a si misma, esto es

$$K \underset{k}{\otimes} K \simeq K \times \cdots \times K$$

Se llama *grupo* de la extensión al grupo de automorfismos de K sobre k. En resumen, diremos que $k \to K$ *es una extensión de Galois de grupo* G, si es de Galois y $G = \mathrm{Aut}_{k-alg} K$.

2. Proposición: *Una k-extensión finita de cuerpos es de Galois si y solo si es separable y normal.*

Demostración. Es inmediata. □

3. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos. Entonces, K es una k-extensión de Galois si y solo si es el cuerpo de descomposición de un polinomio separable (es decir, sin raíces múltiples).*

Demostración. Si $p(x)$ es un polinomio separable (es decir, sin raíces múltiples) entonces el cuerpo de descomposición de $p(x)$, es separable (pues es un cociente de la k-álgebra $k[x]/p(x) \otimes \overset{n}{\cdots} \otimes k[x]/p(x)$) y es normal, luego es de Galois. Recíprocamente, supongamos K que es una k-extensión de Galois. $K = k(\alpha_1, \ldots, \alpha_n)$ y sea $p_i(x)$ el polinomio mínimo anulador de α_i, que es separable, para todo i. El polinomio $p(x) = m.c.m(p_1(x), \ldots, p_n(x))$ es separable y K es el cuerpo descomposición de $p(x)$. □

Si $k \to K$ es de Galois, entonces $K \underset{k}{\otimes} K \simeq K \times \overset{n}{\ldots} \times K$, y $n = \dim_K(K \underset{k}{\otimes} K) = \dim_k K =$ grado de la extensión.

4. Proposición: *Una extensión $k \to K$ es de Galois si y solo si el grado de la extensión coincide con el número de automorfismos, es decir,*

$$\dim_k K = \mathrm{Aut}_{k-alg} K$$

Demostración. Sabemos por la proposición 2.3.7, que K se trivializa a sí misma si y solo tiene tantos endomorfismos (de k-álgebras) como grado. Como todo endomorfismo de k-álgebras de K es un automorfismo, se concluye. □

Si $k \hookrightarrow A$ es una k-álgebra separable, la extensión mínima trivializante de A es de Galois, pues es normal y es separable porque es un cociente de $A \otimes_k \cdots \otimes_k A$. Por ello la envolvente normal de un álgebra separable se denomina envolvente de Galois. Si $p(x) \in k[x]$ es un polinomio separable y $A = k[x]/(p(x))$, entonces la envolvente de Galois de A es $k(\alpha_1, \ldots, \alpha_n)$, siendo $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$ (en el cierre algebraico de k).

5. Teorema: *Sea $\varepsilon_n \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Entonces,*

1. *$\mathbb{Q}(\varepsilon_n)$ es una $\mathbb{Q}$-extensión de Galois y $\mathbb{Q}(\varepsilon_n) = \mathbb{Q}[x]/(\Phi_n(x))$ (donde $\Phi_n(x)$ es el n-ésimo polinomio ciclotómico).*

2. *El grupo de Galois de $\mathbb{Q}(\varepsilon_n)$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración. 1. $\mathbb{Q}(\varepsilon_n)$ es una extensión normal, pues es el cuerpo de descomposición de $x^n - 1$ y es separable porque es cociente de $\mathbb{Q}[x]/(x^n - 1)$, luego es de Galois. $\Phi_n(x)$ es un polinomio mónico irreducible en $\mathbb{Z}[x]$, luego por el teorema de Gauss es irreducible en $\mathbb{Q}[x]$. Por tanto, $\Phi_n(x)$ es el polinomio con coeficiente en $\mathbb{Q}$ mínimo anulador de ε_n. Luego, $\mathbb{Q}[x]/(\Phi_n(x)) = \mathbb{Q}(\varepsilon_n)$.

2. Si $\tau \in \mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(\varepsilon_n))$, entonces $\tau(\varepsilon_n) = \varepsilon_n^k$, para cierto $0 < k < n$, cumpliendo $(k, n) = 1$ y τ queda determinado por este exponente k. Es decir, el morfismo de grupos $\mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(\varepsilon_n)) \to (\mathbb{Z}/n\mathbb{Z})^*$, $\tau \mapsto \bar{k}$ es inyectivo. Por órdenes, ha de ser epiyectivo, luego es un isomorfismo.

□

2.4.1. Cuerpos finitos

6. Definición: Diremos que un cuerpo es finito si tiene un número finito de elementos.

Observemos que la característica de un cuerpo finito K es un número primo $p > 0$, porque el morfismo $\mathbb{Z} \to K$, $n \mapsto n$, tiene núcleo no nulo, que ha de ser un ideal primo $p\mathbb{Z}$, luego con $p > 0$, primo. Por tanto, K es una extensión finita de cuerpos de $\mathbb{Z}/p\mathbb{Z}$. Sea $n = \dim_{\mathbb{Z}/p\mathbb{Z}} K$, entonces K es isomorfo como espacio vectorial a $(\mathbb{Z}/p\mathbb{Z})^n$, luego

$$\#K = p^n$$

Consideremos el grupo conmutativo $K^* = K \setminus \{0\}$ con la multiplicación. Como $\#K^* = p^n - 1$, se tiene que para todo $\alpha \in K^*$, $\alpha^{p^n-1} = 1$. Por tanto, para todo $\alpha \in K$, $\alpha^{p^n} = \alpha$. Es decir, K coincide con el conjunto de todas las raíces del polinomio de grado p^n, $x^{p^n} - x$. Polinomio que es separable. Así pues, K es el cuerpo de descomposición de $x^{p^n} - x$ y es una $\mathbb{Z}/p\mathbb{Z}$-extensión de Galois.

Hemos probado el siguiente teorema.

7. Teorema: *Sea $p > 0$ primo y $n > 0$. Entonces, solo existe un cuerpo finito (salvo isomorfismos) de orden p^n, que denotaremos $\mathbb{F}_{p^n}$, y es precisamente el conjunto de las raíces (en el cierre algebraico de $\mathbb{F}_p$) del polinomio $x^{p^n} - x$. Luego, $\mathbb{F}_{p^n}$ es el cuerpo de descomposición de $x^{p^n} - x$, y los cuerpos finitos son extensiones de Galois de $\mathbb{F}_p$.*

8. Proposición: $\mathbb{F}^*_{p^n} = \mathbb{F}_{p^n} \setminus \{0\}$ *es un grupo (multiplicativo) cíclico.*

Demostración. Basta ver que existe $\alpha \in \mathbb{F}^*_{p^n}$ de orden $p^n - 1$. Basta ver que el anulador del grupo conmutativo (multiplicativo) $\mathbb{F}^*_{p^n}$ es $p^n - 1$. Sea d el anulador de $\mathbb{F}^*_{p^n}$. Se verifica que d es un divisor de $p^n - 1$ y que $\alpha^d = 1$, para todo $\alpha \in \mathbb{F}^*_{p^n}$. Por tanto, $\mathbb{F}^*_{p^n}$ es un subconjunto del conjunto de raíces de $x^d - 1$, luego

$$\#\mathbb{F}_{p^n} \leq d + 1 \leq p^n$$

y por tanto $d = p^n - 1$. □

En consecuencia, $\mathbb{F}^*_{p^n} = <\alpha>$, luego $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, es decir,

$$\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(p(x))$$

siendo $p(x)$ un polinomio irreducible sobre $\mathbb{F}_p$ de grado n.

9. Definición: Sea K un cuerpo de característica $p > 0$. Llamaremos *automorfismo de Fröbenius* al automorfismo de $\mathbb{F}_p$-álgebras

$$F : K \to K$$

definido por $F(\lambda) = \lambda^p$.

10. Teorema: *Sea $k \to K$ una extensión finita entre cuerpos finitos. Sea $k = \mathbb{F}_{p^n}$. El grupo de automorfismos,* $\mathrm{Aut}_{k-alg}K$*, es un grupo cíclico generado por la potencia n-ésima del automorfismo de Fröbenius,*

$$\mathrm{Aut}_{k-alg}K = < F^n >$$

Demostración. F^n sobre $k = \mathbb{F}_{p^n}$ es el morfismo identidad. Si K es una k-extensión de grado m, $\#K = (\#k)^m = p^{nm}$. Entonces $K = \mathbb{F}_{p^{nm}}$. El orden de F^n (como automorfismo de K) es m, por tanto

$$\#\langle F^n \rangle = m = \dim_k K$$

Por tanto, K es una extensión de Galois de grupo $\langle F^n \rangle$.

□

2.5. Teorema de Galois categorial

1. Teorema: *La categoría de las k-álgebras finitas triviales, $\mathscr{C}_{AlgTrv}$ es anti-equivalente a la categoría de conjuntos finitos, $\mathscr{C}_{Conj}$. Los funtores que dan la anti-equivalencia son $F : \mathscr{C}_{Conj} \rightsquigarrow \mathscr{C}_{AlgTrv}$, donde $F(X) := \mathrm{Aplic}(X,k)$, para cada conjunto finito X y $F' : \mathscr{C}_{AlgTrv} \rightsquigarrow \mathscr{C}_{Conj}$, donde $F'(A) := \mathrm{Hom}_{k-alg}(A,k) = \mathrm{Spec}A$, para cada k-álgebra trivial A.*

Demostración. Tenemos que probar que existen isomorfismos $\mathrm{Id} \overset{\theta}{\simeq} F \circ F'$ y $\mathrm{Id} \overset{\theta'}{\simeq} F' \circ F$.

Sea $\theta_A : A \to (F \circ F')(A) = \mathrm{Aplic}(\mathrm{Hom}_{k-alg}(A,k),k)$, $\theta_A(a) := \tilde{a}$, donde $\tilde{a}(\phi) := \phi(a)$, para cada $\phi \in \mathrm{Hom}_{k-alg}(A,k)$. θ_A es isomorfismo: F' transforma producto directos en uniones disjuntas y F uniones disjuntas en productos directos, por tanto basta comprobar que θ_A es isomorfismo cuando $A = k$, lo cual es obvio.

En conclusión, $\mathrm{Id} \overset{\theta}{\simeq} F \circ F'$.

Sea $\theta'_X : X \to (F' \circ F)(X) = \mathrm{Hom}_{k-alg}(\mathrm{Aplic}(X,k),k)$, $\theta'_X(x) := \tilde{x}$, donde $\tilde{x}(f) := f(x)$, para cada $f \in \mathrm{Aplic}(X,k)$. θ'_X es una biyección: F' transforma producto directos en uniones disjuntas y F uniones disjuntas en productos directos, por tanto basta comprobar que θ'_X es biyectivo cuando $X = \{x\}$, lo cual es obvio.

En conclusión, $\mathrm{Id} \overset{\theta'}{\simeq} F' \circ F$.

□

2. Definición: Sea K una k-extensión de Galois de grupo G. G opera en K de modo obvio. Diremos que una K-álgebra B es una GK-álgebra si G opera en B, como morfismos de k-álgebras, de modo que

$$g(\lambda \cdot b) = g(\lambda) \cdot g(b), \quad \forall\, g \in G, \lambda \in K \text{ y } b \in B.$$

Diremos que una aplicación $f : B \to B'$ entre GK-álgebras es un morfismo de GK-álgebras si f es un morfismo de K-álgebras y de G-conjuntos.

La categoría cuyos objetos son las GK-álgebras que sean K-álgebras finitas triviales y cuyos morfismos sean los morfismos de GK-álgebras la denotaremos $\mathscr{C}_{GK-Trv}$.

3. Teorema: *Sea K una k-extensión de Galois de grupo G. La categoría de las GK-álgebras finitas triviales, $\mathscr{C}_{GK-Trv}$ es anti-equivalente a la categoría de G-conjuntos finitos, $\mathscr{C}_{G-Conj}$. Los funtores que dan la anti-equivalencia son*

$$F : \mathscr{C}_{G-Conj} \rightsquigarrow \mathscr{C}_{GK-Trv},\ F(X) := \mathrm{Aplic}(X, K),$$

donde G opera en $\mathrm{Aplic}(X,K)$ como sigue: $(g \cdot f)(x) := g \cdot (f(g^{-1} \cdot x))$, para toda $g \in G$, $f \in \mathrm{Aplic}(X,K)$ y $x \in X$; y

$$F' : \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{G-Conj},\ F'(A) := \mathrm{Hom}_{K-alg}(A, K) = \mathrm{Spec}\, A,$$

donde G opera en $\mathrm{Hom}_{K-alg}(A,K)$ como sigue: $(g \cdot \phi)(a) := g \cdot (\phi(g^{-1} \cdot a))$, para toda $a \in A$, $g \in G$ y $\phi \in \mathrm{Hom}_{K-alg}(A,K)$ (o equivalentemente, dado $x \in \mathrm{Spec}\, A$, $g \cdot x := g^{*-1}(x)$).

Demostración. Ya hemos probado en 2.5.1 que $F \circ F'$ y $F' \circ F$ son isomorfos al funtor identidad.

□

Dado un morfismo de anillos $A \to B$ y un grupo $G \subseteq \mathrm{Aut}_{A-alg}(B)$, denotaremos $B^G := \{b \in B : g(b) = b, \text{ para todo } g \in G\}$.

4. Lema: *Sea $A \to B$ un morfismo de anillos, $G \subseteq \mathrm{Aut}_A(B)$ un grupo finito de automorfismos y $A \to C$ un morfismo plano. Entonces, $(B \otimes_A C)^G = B^G \otimes_A C$.*

Demostración. La sucesión

$$\begin{array}{ccccccc} 0 & \to & B^G & \to & B & \to & B \overset{G}{\oplus \cdots \oplus} B \\ & & & & b & \to & (g(b))_{g \in G} \end{array}$$

es exacta, luego

$$0 \to B^G \otimes_A C \to B \otimes_A C \to (B \otimes_A C) \overset{G}{\oplus \cdots \oplus} (B \otimes_A C)$$

es exacta, y por tanto $(B \otimes_A C)^G = B^G \otimes_A C$. □

5. Lema : *Sea K una k-extensión de Galois de grupo G. Si B es una GK-álgebra, entonces el morfismo natural*

$$B^G \otimes_k K \to B,\ b \otimes \lambda \mapsto b \cdot \lambda,$$

es un isomorfismo.

Demostración. $B \otimes_k K = B \otimes_K (K \otimes_k K) = B \otimes_K \prod^G K = \prod^G B$, $b \otimes \lambda \mapsto (b \cdot g(\lambda))_g$. La operación de G en $B \otimes_k K$ en el primer factor se traduce en $\prod^G B$ en la operación de G en G (por la izquierda) y la operación natural en cada factor B de $\prod^G B$. Como $(\prod^G B)^G = \{(g(b))_{g\in G} \in \prod^G B, \text{ con } b \in B\} = B$, entonces

$$B^G \otimes_k K = (B \otimes_k K)^G = (\prod^G B)^G = B,\ b \otimes \lambda \mapsto b \cdot \lambda.$$

□

6. Corolario: *Sea K una k-extensión de Galois de grupo G. Entonces, $K^G = k$.*

Demostración. Por el lema 2.5.5, $K^G \otimes_k K = K$. Entonces, $\dim_k K^G = 1$ y $K^G = k$. □

7. Corolario: *Sea K una extensión de Galois de grupo G. Sea $K' \hookrightarrow K$ una k-subextensión y $H = \{g \in G : g(\lambda) = \lambda,\ \forall \lambda \in K'\}$. Entonces, $K' \hookrightarrow K$ es una extensión de Galois de grupo H. En particular, $K^H = K'$.*

Demostración. $K \otimes_{K'} K$ es una K-álgebra trivial, porque es cociente de la K-álgebra trivial $K \otimes_k K$ (considérese el epimorfismo $K \otimes_k K \to K \otimes_{K'} K$, $a \otimes b \mapsto a \otimes b$). Por tanto, K es una K'-extensión de Galois, de grupo de Galois $\mathrm{Hom}_{K'-alg}(K,K) = H$.

□

8. Teorema: *Sea K una k-extensión de Galois de grupo G. La categoría de las GK-álgebras finitas triviales, $\mathscr{C}_{GK-Trv}$ es equivalente a la categoría de k-álgebras finitas trivializadas por K, $\mathscr{C}_{K/k}$. Los funtores que dan la equivalencia son*

$$H : \mathscr{C}_{K/k} \rightsquigarrow \mathscr{C}_{GK-Trv},\ H(A) := A \otimes_k K, \quad H' : \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{K/k},\ H'(B) = B^G$$

Demostración. $H' \circ H \simeq \mathrm{Id}$, porque $K^G = k$ y por el lema 2.5.4. $H \circ H' \simeq \mathrm{Id}$ por el lema 2.5.5 □

9. Teorema de Galois categorial: *Sea $k \hookrightarrow K$ una extensión de Galois de grupo G. Denotemos $C_{K/k}$ la categoría de k-álgebras finitas trivializadas por K, y por C_{G-conj} la categoría de G-conjuntos finitos. Los funtores*

$$\begin{aligned} P &: C_{K/k} \rightsquigarrow C_{G-conj} \quad P(A) := \mathrm{Hom}_{k-alg}(A,K) \\ \bar{P} &: C_{G-conj} \rightsquigarrow C_{K/k} \quad \bar{P}(Z) := \mathrm{Hom}_{G}(Z,K) \end{aligned}$$

establecen una anti-equivalencia entre las categorías $C_{K/k}$ y C_{G-conj}.

Demostración. Tenemos las equivalencias

$$\begin{aligned} \mathscr{C}_{K/k} &\overset{H}{\rightsquigarrow} \mathscr{C}_{GK-Trv} \overset{F'}{\rightsquigarrow} \mathscr{C}_{G-conj} \\ \mathscr{C}_{K/k} &\overset{H'}{\leftsquigarrow} \mathscr{C}_{GK-Trv} \overset{F}{\leftsquigarrow} \mathscr{C}_{G-conj} \end{aligned}$$

Observemos que $F' \circ H = P$, porque $(F' \circ H)(A) = F'(A \otimes_k K) = \mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \mathrm{Hom}_{k-alg}(A,K) = P(A)$, y que $H' \circ F = \bar{P}$, porque

$$(H' \circ F)(X) = H'(\mathrm{Aplic}(X,K)) = \mathrm{Aplic}(X,K)^G = \mathrm{Hom}_G(X,K) = \bar{P}(X).$$

Recordemos que si X e Y son dos G-conjuntos y consideramos la operación de G en $\mathrm{Aplic}(X,Y)$ definida por $(g \cdot f)(x) = g \cdot (f(g^{-1} \cdot x))$, para toda $g \in G$, $f \in \mathrm{Aplic}(X,Y)$ y $x \in X$, entonces

$$\mathrm{Aplic}(X,Y)^G = \mathrm{Hom}_G(X,Y).$$

□

10. Corolario: *Sea K una extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. Entonces,*

$$\mathrm{Hom}_{k-alg}(K^H, K) = G/H.$$

Demostración. $\bar{P}(G/H) = \mathrm{Hom}_G(G/H, K) = K^H$. Luego, por la equivalencia categorial de Galois se cumple que $\mathrm{Hom}_{k-alg}(K^H,K) = \mathrm{Hom}_G(G, G/H) = G/H$. □

11. Teorema clásico de Galois: *Sea K una k-extensión de Galois de grupo G. La asignación*

$$[\textit{Conjunto de subgrupos de } G] \to [\textit{Conjunto de } k\textit{-subextensiones de } K],\ H \mapsto K^H$$

es biyectiva.

Demostración. Si $K^H = K^{H'}$, entonces $G/H = \mathrm{Hom}_{k-alg}(K^H,K) = \mathrm{Hom}_{k-alg}(K^{H'},K) = G/H'$, y $H = H'$. Luego, la asignación es inyectiva. Por el corolario 2.5.7, la asignación es epiyectiva.

□

12. Proposición de Artin: *Sea K un cuerpo y $G \subseteq \mathrm{Aut}_{anillos} K$ un subgrupo finito. Entonces, K es una K^G-extensión de Galois de grupo G. Además, si K es una k-extensión de Galois de grupo G, entonces $K^G = k$.*

Demostración. Sean $a_i \in K$ cualesquiera, para $i = 1, \ldots, n$. Sea $H_i \subseteq G$ el subgrupo de isotropía de a_i. Entonces, $p_i(x) := \prod_{\bar{g} \in G/H_i} (x - g(a_i)) \in K^G[x]$. El cuerpo de descomposición del polinomio $p(x) := m.c.m.(p_1(x), \ldots, p_n(x))$,

$$K' := K^G[g(a_i)]_{i \in \{1,\ldots,n\}, \bar{g} \in G/H_i} \subseteq K$$

es una K^G-extensión de Galois, que contiene a $K^G(a_1, \ldots, a_n)$. Consideremos el subgrupo $H := \{g \in G \colon g(\lambda) = \lambda \text{ para todo } \lambda \in K'\}$, entonces $K'^{G/H} = K'^G = K^G$, luego $\dim_{K^G} K' = \#G/\#H \leq \#G$. Luego, $\dim_{K^G} K \leq \#G$. Por tanto, K es una K^G-extensión de Galois de grado $\#G$ y grupo G.

La última afirmación ya ha sido probada.

□

13. Sea $k \hookrightarrow K$ una extensión de Galois de grupo G, $\alpha \in K$ y I_α el subgrupo de isotropía de α. El polinomio mínimo anulador de α con coeficientes en k, es el polinomio

$$p(x) = \prod_{\bar{g} \in G/I_\alpha} (x - g(\alpha))$$

En efecto, consideremos la operación natural de G en $K[x]$, $g(\sum_i a_i x^i) := \sum_i g(a_i) x^i$. Por el teorema de Artin, $q(x) \in K[x]$ es invariante por G si y solo si $q(x) \in k[x]$. Es claro que $p(x)$ es invariante por G, luego $p(x) \in k[x]$. Además, $p(x)$ anula a α. Si α es una raíz de $q(x) \in k[x]$, entonces $g(\alpha)$ es una raíz de $g(q(x)) = q(x)$, para todo $g \in G$. Por tanto, el polinomio mínimo anulador de α es $p(x)$.

14. Corolario: *Sea $k \hookrightarrow K$ una extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. $k \hookrightarrow K^H$ es una extensión de Galois (de grupo de grupo de Galois G/H) si y solo si H es un subgrupo normal de G.*

Demostración. Por el teorema de Galois, $\mathrm{Aut}_{k-alg}(K^H) = \mathrm{Aut}_G(G/H) = N(H)/H$, donde $N(H)$ es el normalizador de H en G. Por otro lado, $k \to K$ es una extensión de Galois de grado $\#G$ y $K^H \to K$ es una extensión de grado $\#H$, luego $k \to K^H$ es una extensión de grado $\#G/\#H$. Por tanto

$$\begin{aligned} K^H \text{ es de Galois} &\iff \#(N(H)/H) = \#(G/H) \iff \#N(H) = \#G \\ &\iff H \text{ es normal en } G. \end{aligned}$$

□

15. Teorema: *Sea $k \hookrightarrow K$ una extensión finita de cuerpos y $G = \mathrm{Aut}_{k-alg} K$. Entonces, K es normal $\iff$ $K = K_1 \otimes_k K_2$, siendo K_1 una extensión de Galois y K_2 una extensión puramente inseparable.*

Además, si K es normal, entonces $K_1 = \pi_0^k(K)$, $K_2 = K^G$ y $G = \mathrm{Aut}_{k-alg} K_1$.

Demostración. $\Leftarrow$) Las k-álgebras puramente inseparables son locales para todo cambio de base y las separables son reducidas para todo cambio de base. Por tanto, $K_1 \otimes_k K_2$ es local y reducida, luego cuerpo. Además, $K_1 \otimes_k K_2$ es el compuesto de dos extensiones normales, luego es normal por el teorema del agujero único.

$\Rightarrow$) K trivializa a $\pi_0^k(K)$, luego la mínima extensión que trivializa a $\pi_0^k(K)$ es $\pi_0^k(K)$, luego es de Galois. Por el teorema de prolongación, el morfismo

$$\mathrm{Aut}_{k-alg}(K) \to \mathrm{Aut}_{k-alg}(\pi_0^k(K)),\ \tau \mapsto \tau_{|\pi_0^k(K)}$$

es epiyectivo, de núcleo $\mathrm{Aut}_{\pi_0^k(K)}(K)$, que es igual a $\{Id\}$, porque K es una extensión puramente inseparable de $\pi_0^k(K)$. Luego, $\mathrm{Aut}_{k-alg}(K) = \mathrm{Aut}_{k-alg}(\pi_0^k(K))$. Luego, $k = \pi_0^k(K)^G = \pi_0^k(K) \cap K^G = \pi_0^k(K^G)$ y K^G es puramente inseparable. K es una K^G-extensión de grado $|G|$, luego $\dim_k K^G = \dim_k K/|G|$. $\pi_0^k(K)$ es un k-extensión de grado $|G|$. Entonces el compuesto $\pi_0^k(K) \otimes_k K^G$ es de grado $\dim_k K$ y ha de coincidir con K.

Para la última afirmación, observemos que $\pi_0^k(K) = \pi_0^k(K_1) \otimes_k \pi_0^k(K_2) = K_1$. Además, hemos probado que $\mathrm{Aut}_{k-alg}(K) = \mathrm{Aut}_{k-alg}(\pi_0^k(K)) = \mathrm{Aut}_{k-alg}(K_1)$, luego todo automorfismo de $K = K_1 \otimes_k K_2$ opera en K_2 por la identidad y $K^G = K_1^G \otimes_k K_2 = K_2$.

□

16. Teorema de los irracionales naturales de Lagrange: *Sea $k \hookrightarrow K$ una extensión de Galois y $k \hookrightarrow L$ una extensión de cuerpos y consideremos un compuesto $L \cdot K$, que es una L-extensión de Galois. Entonces,* $\mathrm{Aut}_{L-alg}(L \cdot K) = \mathrm{Aut}_{L \cap K-alg}(K)$.

Demostración. K es el cuerpo de descomposición de un cierto polinomio separable $p(x) \in k[x]$, luego $L \cdot K$ es el cuerpo de descomposición del polinomio $p(x) \in L[x]$ y es una L-extensión de Galois.

Consideremos la inclusión $G' := \mathrm{Aut}_{L-alg}(L \cdot K) \hookrightarrow \mathrm{Aut}_{k-alg} K$, $g' \mapsto g'_{|K}$. Observemos que $K^{G'} = (K \cdot L)^{G'} \cap K = L \cap K$. Luego, G' se identifica con $\mathrm{Aut}_{L \cap K-alg}(K)$. □

2.6. Resolubilidad de las ecuaciones polinómicas por radicales

Sea $p(x) \in k[x]$ un polinomio. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$, en el cierre algebraico de k y sea $k(\alpha_1, \ldots, \alpha_n)$ el cuerpo de descomposición de $p(x)$. El morfismo

$k[x_1,\dots,x_n] \to k(\alpha_1,\dots,\alpha_n)$, $x_i \mapsto \alpha_i$ es epiyectivo, luego $k(\alpha_1,\dots,\alpha_n) = k[x_1,\dots,x_n]/I$, donde I es el ideal (maximal) formado por los polinomios $p(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$ tales que $p(\alpha_1,\dots,\alpha_n) = 0$. Sea $G = \mathrm{Aut}_{k-alg}\, k(\alpha_1,\dots,\alpha_n)$ *el grupo asociado* a $p(x)$. Todo $\tau \in G$ aplica cada raíz $p(x)$ en otra raíz de $p(x)$ y τ queda determinado por como opera sobre los raíces de $p(x)$. En conclusión, si consideramos la acción natural de S_n en $k[x_1,\dots,x_n]$, $\sigma(q(x_1,\dots,x_n)) = q(x_{\sigma(1)},\dots,x_{\sigma(n)})$, tenemos que

$$\mathrm{Aut}_{k-alg}\, k(\alpha_1,\dots,\alpha_n) = \{\sigma \in S_n : \sigma(I) = I\}$$

Es decir, el grupo asociado a $p(x)$ es el conjunto de permutaciones σ de las raíces de $p(x)$, tales que si $q(\alpha_1,\dots,\alpha_n) = 0$ entonces $q(\alpha_{\sigma(1)},\dots,\alpha_{\sigma(n)}) = 0$.

Si $p(x)$ es irreducible el grupo de $p(x)$, G, opera transitivamente sobre las raíces, es decir, G es un subgrupo transitivo de S_n.

El objetivo de esta sección es probar que las raíces de $p(x)$ se pueden obtener como combinaciones algebraicas y toma de radicales sucesivas de elementos de k si y solo si G es resoluble.

2.6.1. Extensiones cíclicas

1. Definición: Diremos que una extensión de cuerpos $k \to K$ es *cíclica* si es de Galois de grupo cíclico.

2. Teorema de independencia lineal de Artin: *Sea $k \to K$ una extensión de Galois de grupo $G = \{g_1,\dots,g_n\}$. Se cumple que $g_1,\dots,g_n$ son K-linealmente independientes.*

Demostración. Consideremos el diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Aut}_{k-alg} K & = & \mathrm{Hom}_{K-alg}(K \otimes_k K, K) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_k(K,K) & = & \mathrm{Hom}_K(K \otimes_k K, K) \end{array}$$

$K \underset{k}{\otimes} K = K \times \overset{n}{\dots} \times K$ y los automorfismos de k-álgebras de K se corresponden con las proyecciones de $K \times \overset{n}{\dots} \times K$ en cada uno de los factores, que son claramente K-linealmente independientes. □

A. Caso primo con la característica.

3. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos de grado n y supongamos que $(\operatorname{car} k, n) = (1)$ y que k contiene todas las raíces n-ésimas de la unidad. Entonces, $k \to K$ es una extensión cíclica si y solo existe $a \in k$ de modo que $K = k(\sqrt[n]{a})$.*

Demostración. Si $K = k(\sqrt[n]{a})$, K es una extensión de Galois porque es el cuerpo de descomposición del polinomio $x^n - a$. El grupo de Galois, G, de K es un subgrupo de $\mathbb{Z}/n\mathbb{Z}$: Dado $g \in \operatorname{Aut}_{k-alg}(k(\sqrt[n]{a})) = G$, tenemos que $g(\sqrt[n]{a}) = \epsilon^i \sqrt[n]{a}$, para cierto $0 \leq i < n$ y la aplicación $G \to \mathbb{Z}/n\mathbb{Z}$, $g \mapsto \bar{i}$ es un morfismo inyectivo de grupos. G es cíclico porque es un subgrupo de un grupo cíclico.

Supongamos que $k \hookrightarrow K$ sea una extensión de Galois de grupo cíclico $G = \langle\sigma\rangle$. Sea $\epsilon \in k$ una raíz n-ésima primitiva de la unidad. Si existe $0 \neq R \in K$ tal que $\sigma(R) = \epsilon R$, entonces

1. $R^n \in k$, porque $\sigma(R^n) = \sigma(R)^n = R^n$, luego $R^n \in K^{\langle\sigma\rangle} = k$.
2. $K = k(R)$, porque $k(R) = K^H$, donde $H = \{h \in G : h(R) = R\} = \{\mathrm{Id}\}$, luego $k(R) = K$.
3. Si denotamos $a = R^n \in k$, $K = k(\sqrt[n]{a})$.

Existe R: Tenemos que demostrar que ϵ es un valor propio de σ. Obviamente $x^n - 1$ anula a σ y por el teorema de independencia lineal de Artin, $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ son linealmente independientes, luego $x^n - 1$ es el polinomio mínimo anulador de σ y ϵ es un valor propio de σ. □

4. Observación: Sea $k \hookrightarrow K$ una extensión de Galois de grupo $G = \langle\sigma\rangle$ y $R \in K$. En la demostración del corolario anterior se ha visto que $R = \sqrt[n]{a}$, para algún $a \in k$, si y solo si $\sigma(R) = \epsilon R$, siendo ϵ una raíz n-ésima de la unidad.

Veamos ahora cómo expresar, de modo explícito, un elemento α de una k-extensión cíclica K de grado n (con $(n, \operatorname{car} k) = (1)$) en función de radicales de elementos de k (obtenidos a partir de α y el grupo de Galois $G = \langle\sigma\rangle$ de K).

El polinomio anulador de σ es $x^n - 1$, por el teorema de independencia lineal de Artin. Entonces, $K = \oplus_{i=1}^{n} \operatorname{Ker}(\sigma - \epsilon^i)$ y por dimensiones $\dim_k \operatorname{Ker}(\sigma - \epsilon^i) = 1$. Escribamos, $\operatorname{Ker}(\sigma - \epsilon^i) = k \cdot R_i$. Observemos que $\operatorname{Im} \frac{\sigma^n - 1}{\sigma - \epsilon^i} = k \cdot R_i$, pues $\frac{\sigma^n - 1}{\sigma - \epsilon^i}(R_j) = 0$, para $j \neq i$ y $\frac{\sigma^n - 1}{\sigma - \epsilon^i}(R_i) = (\sigma^{n-1} + \epsilon^i \sigma^{n-2} + \cdots + \epsilon^{i \cdot (n-1)})(R_1) = n \cdot (\epsilon^i)^{n-1} \cdot R_i = n \cdot \epsilon^{-i} \cdot R_i$. Luego, $\frac{\epsilon^i}{n} \cdot \frac{\sigma^n - 1}{\sigma - \epsilon^i}(R_i) = R_i$. Además,

$$\frac{\epsilon^i}{n} \cdot \frac{\sigma^n - 1}{\sigma - \epsilon^i} = \frac{1}{n} \cdot (\mathrm{Id} + \epsilon^{-i}\sigma + \cdots + \epsilon^{-(n-1)\cdot i}\sigma^{n-1})$$

Dado $\alpha \in K$ tendremos que

$$\alpha = \sum_i \lambda_i R_i = \sum_i \frac{1}{n}(\mathrm{Id} + \epsilon^{-i}\sigma + \cdots + \epsilon^{-(n-1)\cdot i}\sigma^{n-1})(\alpha) = \frac{1}{n}\sum_i (\alpha + \epsilon^{-i}\sigma(\alpha) + \cdots + \epsilon^{-i(n-1)}\sigma^{n-1}(\alpha)).$$

5. Definición: Dado $\alpha \in K$, llamaremos resolvente de Lagrange de α por ϵ^i, que denotaremos $R(\alpha, \epsilon^i)$, a

$$R(\alpha, \epsilon^i) := \sum_{j=0}^{n-1} (\epsilon^i)^j \sigma^j(\alpha)$$

Se cumple que $\sigma(R(\alpha, \epsilon^i)) = \epsilon^{-i} \cdot R(\alpha, \epsilon^i)$ (luego, $R(\alpha, \epsilon^i)^n \in k$) y para todo $\alpha \in K$

$$\boxed{\alpha = \frac{1}{n}\sum_{i=0}^{n-1} R(\alpha, \epsilon^i)}$$

que se conoce como *fórmula de Lagrange*.

B. Caso cíclico de orden igual a la característica.

Sea k un cuerpo de característica $p > 0$. Consideremos la ecuación $x^p - x - a$, con $a \in k$.

6. Definición: Llamaremos *radical p-ésimo modificado de a*, y lo denotaremos $\sqrt[p]{\underline{a}}$, a una raíz de $x^p - x - a$. Diremos además que $\sqrt[p]{\underline{a}}$ es un radical modificado *propio* si $x^p - x - a$ es irreducible.

Si $\sqrt[p]{\underline{a}}$ es una raíz de $x^p - x - a$, las demás raíces son $\sqrt[p]{\underline{a}} + 1$, $\sqrt[p]{\underline{a}} + 2$, ..., $\sqrt[p]{\underline{a}} + p - 1$. Basta ver que si α es raíz de $x^p - x - a$, entonces $\alpha + 1$ también. Efectivamente,

$$(\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = 0$$

luego se concluye. Por tanto el cuerpo de descomposición del polinomio $x^p - x - a$ es $k(\sqrt[p]{\underline{a}})$.

7. Ejercicio: Prueba que $x^p - x - a$ es o bien irreducible (sobre k), o bien tiene todas sus raíces en k.

Si $x^p - x - a$ es irreducible, entonces $k \to k(\sqrt[p]{\underline{a}})$ es una extensión de Galois de grado p, y por tanto el grupo es $\mathbb{Z}/p\mathbb{Z}$. Explícitamente, dado $i \in \mathbb{Z}/p\mathbb{Z}$, el automorfismo de $k(\sqrt[p]{\underline{a}})$ que define es

$$\begin{aligned} \tau_i : k(\sqrt[p]{\underline{a}}) &\longrightarrow k(\sqrt[p]{\underline{a}}) \\ \sqrt[p]{\underline{a}} &\longmapsto \sqrt[p]{\underline{a}} + i \end{aligned}$$

Vamos a ver ahora que todas las extensiones cíclicas de grado p son de este tipo, es decir, extender por un radical modificado.

8. Proposición: *Sea $k \to K$ una extensión de grado p = característica de k. Entonces, $k \to K$ es una extensión cíclica si y solo si existe $a \in k$ de modo que $K = k(\sqrt[p]{a})$.*

Demostración. Supongamos $k \to K$ es una extensión cíclica de grupo $G = \langle\sigma\rangle$. Existe $\beta \in K$, tal que $\sigma(\beta) = \beta + 1$, o equivalentemente, tal que $(\sigma - \mathrm{Id})(\beta) = 1$: En efecto, el polinomio anulador de σ es igual a $x^p - 1 = (x-1)^p$. Por tanto, K con el endomorfismo σ es un $k[x]$-módulo isomorfo a $k[x]/(x-1)^p$. Obviamente, $\mathrm{Im}(x-1)^{p-1} = \mathrm{Ker}(x-1) = k$, por el teorema de Artin. Por tanto, existe $\alpha \in K$ tal que $(\sigma - \mathrm{Id})^{p-1}(\alpha) = 1$. Luego, podemos definir $\beta := (\sigma - \mathrm{Id})^{p-2}(\alpha)$.

Veamos que β es un radical p-ésimo modificado. Basta ver que $\beta^p - \beta$ es invariante por σ. Pero

$$\sigma(\beta^p - \beta) = \sigma(\beta)^p - \sigma(\beta) = (\beta + 1)^p - (\beta + 1) = \beta^p - \beta$$

Para concluir, veamos que $k(\beta) = K$. Se tiene $k \hookrightarrow k(\beta) \hookrightarrow K$, y como $k \to K$ es de grado p, primo, debe ser $k = k(\beta)$ ó $k(\beta) = K$. Pero $k \neq k(\beta)$, ya que $\beta \notin k$, pues no es invariante por σ. Se concluye.

Supongamos ahora que $K = k(\sqrt[p]{a})$. Entonces, K es una extensión de Galois de grupo un grupo de orden primo, luego cíclico.

□

Denotemos por σ un generador del grupo de automorfismos de K. Sea $\beta \in K$ tal que $\sigma(\beta) = \beta + 1$, entonces $a := \beta^p - \beta \in k$, $\beta = \sqrt[p]{a}$ y $K = k(\beta) = k[x]/(x^p - x - a)$.

Veamos cómo hallar un radical modificado β. Según la demostración de la proposición anterior $\beta = (\sigma - \mathrm{Id})^{p-2}(\alpha)$, donde $(\sigma - \mathrm{Id})^{p-1}(\alpha) = 1$. Ahora bien,

$$\mathrm{Tr} = \sigma^{p-1} + \sigma^{p-2} + \cdots + \sigma + 1 = \frac{\sigma^p - 1}{\sigma - 1} = (\sigma - 1)^{p-1}.$$

Entonces, si $\gamma \in K$ es un elemento de traza no nula, entonces $\alpha = \frac{\gamma}{\mathrm{Tr}(\gamma)}$ es de traza 1 y $\beta := \frac{(\sigma-1)^{p-2}(\gamma)}{\mathrm{Tr}(\gamma)}$ es un radical modificado.

Dado $\alpha \in K$, existen $c_i \in k$ de modo que $\alpha = \sum_{i=0}^{p-1} c_i \beta^i$. Queremos calcular los c_i.

Si E es un k-espacio vectorial, T_2 una métrica no singular en E y sabemos calcular $T_2(e, e')$, para todo $e, e' \in E$, entonces dada una base $\{e_i\}$ y un vector $e \in E$ sabremos expresar e como combinación lineal de los e_i. Por tanto, si en una k-álgebra separable A sabemos calcular trazas, sabremos expresar todo elemento de A como combinación lineal de elementos de una base.

El lector puede comprobar que $\mathrm{Tr}(\overline{x^i}) = 0$, para todo $0 \leq i < 2p-2$ y $i \neq p-1$; y $\mathrm{Tr}(\overline{x^{p-1}}) = \mathrm{Tr}(\overline{x^{2p-2}}) = -1$. Entonces, $c_i = -\mathrm{Tr}(\alpha \cdot \overline{x^{p-1-i}})$, para $i \neq 0$ y $c_0 = -a \cdot Tr(\alpha/\bar{x})$.

9. Por tanto,

$$\boxed{\alpha = -a \cdot Tr(\alpha/\beta) - \sum_{i=1}^{p-1} Tr(\alpha \cdot \beta^{p-1-i}) \cdot \beta^i}$$

10. Resolución de la ecuación de segundo grado

Sea $x^2 + ax + b$ la ecuación general de segundo grado, de raíces α_1, α_2. Como ya sabemos, el grupo de la ecuación es $S_2 = \mathbb{Z}/2\mathbb{Z}$, generado por la permutación $\sigma = (1,2)$, $\sigma(\alpha_1) = \alpha_2$.

Característica distinta de 2: Calculamos las resolventes de Lagrange. Tenemos

$$R(\alpha_1, 1) = \alpha_1 + \alpha_2 = -a$$
$$R(\alpha_1, -1) = \alpha_1 - \alpha_2$$

y $R(\alpha_1,-1)^2 = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = a^2 - 4b$. Por tanto,

$$\alpha_1, \alpha_2 = \frac{1}{2}(R(\alpha_1,1) + R(\alpha_1,-1)) = \frac{-a \pm \sqrt{a^2-4b}}{2}$$

Característica 2: En primer lugar, encontremos un elemento de traza no nula. Es fácil: $Tr(\alpha_1) = \alpha_1 + \alpha_2 = a \neq 0$. Entonces, $\frac{\alpha_1}{a}$ es un radical modificado: $(\frac{\alpha_1}{a})^2 + \frac{\alpha_1}{a} = \frac{\alpha_1^2 + a\alpha_1}{a^2} = \frac{b}{a^2}$. Luego, $\frac{\alpha_1}{a} = \overset{\wedge}{{}_2\backslash}\underline{b/a^2}$. Por tanto,

$$\alpha_1 = a \cdot \overset{\wedge}{{}_2\backslash}\underline{b/a^2}, \quad \alpha_2 = a \cdot (1 + \overset{\wedge}{{}_2\backslash}\underline{b/a^2})$$

Apéndice: Teorema 90 de Hilbert.

11. Teorema (90 de Hilbert multiplicativo): *Sea $k \to K$ una extensión cíclica de grado n y grupo $G = <\sigma>$, y sea $\alpha \in K$. Entonces,*

$$N(\alpha) = 1 \Leftrightarrow \alpha = \frac{\beta}{\sigma(\beta)}, \text{ para cierto } \beta \in K$$

Demostración. Si $\alpha = \frac{\beta}{\sigma(\beta)}$, entonces

$$N(\alpha) = N\left(\frac{\beta}{\sigma(\beta)}\right) = \frac{N(\beta)}{N(\sigma(\beta))} = 1$$

Recíprocamente, supongamos que $N(\alpha) = 1$. Tenemos que probar que $T := \alpha\sigma$ tiene algún vector propio β de valor propio 1, es decir, existe $\beta \in K$ tal que $T(\beta) = \beta$, que

equivale a $\alpha = \frac{\beta}{\sigma(\beta)}$. $T^2 = \alpha\sigma(\alpha)\sigma^2$, y así sucesivamente, $T^n = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n = N(\alpha) = 1$. Por tanto, $x^n - 1$ anula a T. Es más, por el teorema de independencia lineal de Artin, $1, T, \ldots, T^{n-1}$ son linealmente independientes, luego $x^n - 1$ es el anulador de T. Como tiene la raíz 1, existe algún vector propio no nulo de valor propio 1. □

En particular, observemos que si $\epsilon \in K$ es una raíz n-ésima primitiva de la unidad entonces $N(\epsilon) = 1$, luego existe β tal que $\epsilon = \frac{\beta}{\sigma(\beta}$. Es decir, $\sigma(\beta) = \epsilon \cdot \beta$ y es fácil deducir, de nuevo, que $a = \beta^n \in k$ y $K = k[\beta] = k[x]/(x^n - a)$.

12. Teorema (90 de Hilbert aditivo): *Sea $k \to K$ una extensión cíclica de grado n y grupo $G = \langle\sigma\rangle$, y sea $\alpha \in K$. Entonces,*

$$Tr(\alpha) = 0 \Leftrightarrow \alpha = \sigma(\beta) - \beta, \text{ para cierto } \beta \in K$$

Demostración. Hay que probar que el núcleo de la traza coincide con la imagen de $\sigma - 1$. Se verifica que $\sigma^n = 1$, y por el teorema de independencia lineal de Artin se concluye que $x^n - 1$ es el anulador de σ. K con el endomorfismo lineal σ, tiene estructura de $k[x]$-módulo y es isomorfo a $k[x]/(x^n - 1)$. Tenemos que $x^n - 1 = (x-1)\cdot T(x)$, donde $T(x) = 1 + x + \cdot + x^{n-1}$. Es fácil ver que $T(x)\cdot\overline{q(x)} = 0 \in k[x]/(x^n - 1)$ si y solo si $q(x)$ es múltiplo de $(x-1)$. Por tanto, $\operatorname{Ker} Tr = \operatorname{Im}(\sigma - \mathrm{Id})$.

□

En particular, observemos que $Tr(1) = 0$, luego existe β tal que $1 = \sigma(\beta) - \beta$. Es decir, $\sigma(\beta) = \beta + 1$ y es fácil deducir, de nuevo, que si $car k = p = n$ entonces $a = \beta^p - \beta \in k$ $K = k[\beta] = k[x]/(x^p - x - a)$.

2.6.2. Extensiones por radicales

13. Definición: Diremos que una extensión finita $k \to K$ es *radical* si $K \simeq k(\sqrt[n]{a})$ ó $K \simeq k(\sqrt[p]{\underline{a}})$.

14. Definición: Diremos que una extensión $k \to K$ es *una extensión por radicales* si admite una cadena de subextensiones

$$k \to K_1 \to K_2 \to \cdots \to K_r = K$$

tal que $K_i \to K_{i+1}$ es radical. Análogamente, diremos que una ecuación, $p(x) = 0$, es resoluble por radicales si el cuerpo de descomposición de $p(x)$ es extensión por radicales.

Observemos que si $\operatorname{car} k = p$ y $k \hookrightarrow K$ es puramente inseparable, entonces es una extensión por radicales, porque $K^{p^n} = k$, para $n >> 0$.

Si $\operatorname{car} k = p$, $n = p^r \cdot m$, $(m,p) = 1$ y $k \hookrightarrow k(\sqrt[n]{a})$ es separable, entonces $k(\sqrt[n]{a}) = k(\sqrt[m]{a})$, porque la extensión $k(\sqrt[m]{a}) \to k(\sqrt[n]{a})$ es separable y puramente inseparable.

15. Teorema: *Sea $k \to K$ una extensión normal, de grupo $G = \mathrm{Aut}_{k-alg} K$ de orden n. Supongamos que k contiene todas las raíces n-ésimas de la unidad. Entonces, $k \to K$ es una extensión por radicales si y solo si el grupo G es resoluble.*

Demostración. $K = K_1 \otimes_k K_2$ con K_1 de Galois, K_2 puramente inseparable y $\mathrm{Aut}_{k-alg} K = \mathrm{Aut}_{k-alg} K_1$. Además, K es una extensión por radicales si y solo si lo es K_1 (observemos que $k \cdot K^{p^m} = K_1$, con $p = \mathrm{car}\, k$ y $m >> 0$).

En conclusión, podemos suponer que K es de Galois.

Observemos que si $H_1 \subset H_2 \subseteq G$ son dos subgrupos, entonces H_1 es normal en H_2 si y solo si $K^{H_2} \hookrightarrow K^{H_1}$ es una extensión de Galois (de grupo H_2/H_1): En efecto, $K^{H_2} \hookrightarrow K$ es una extensión de Galois de grupo H_2. Por la proposición 2.5.14, $K^{H_2} \hookrightarrow K^{H_1}$ es una extensión de Galois (de grupo H_2/H_1) si y solo si H_1 es normal en H_2.

Si existe $\{1\} = G_1 \subset G_2 \subset \cdots \subset G_r = G$ una cadena de subgrupos de G, con G_i normal en G_{i+1} y G_{i+1}/G_i cíclico (podemos suponer añadiendo más eslabones que $|G_{i+1}/G_i| k$ es primo)para todo i, entonces, $k = K^{G_r} \subset K^{G_{r-1}} \subset \cdots \subset K^{G_2} \subset K^{G_1} = K$ es una cadena de extensiones radicales. Recíprocamente, si existe una cadena $k = K_1 \subset \cdots \subset K_n = K$ de subextensiones, tal que $K_i \hookrightarrow K_{i+1}$ es radical (podemos suponer añadiendo eslabones que $\dim_{K_i} K_{i+1}$ es primo), entonces la cadena de subgrupos $G = G_1 \supset \cdots \supset G_n = \{1\}$, donde $G_i := \mathrm{Aut}_{K_i-alg}(K)$, cumplen que G_{i+1} es normal en G_i y G_i/G_{i+1} es cíclico. □

16. Teorema: *Sea $k \to K$ una extensión finita de cuerpos. Entonces, K está incluida en una extensión de k por radicales si y solo si el grupo de automorfismos de k-álgebras de la envolvente normal de K es resoluble.*

Demostración. Sea Σ la envolvente de normal de K. Recordemos que si $\bar{k}$ es el cierre algebraico de k y $\{\phi_1, \ldots, \phi_n\} = \mathrm{Hom}_{k-alg}(K, \bar{k})$, entonces $\Sigma = \phi_1(K) \cdots \phi_n(K)$. Además los morfismos ϕ_i prolongan a automorfismos de $\bar{k}$. Por tanto, si K está incluida en una extensión por radicales Σ' entonces Σ está incluida en una extensión por radicales: $\phi_1(\Sigma') \cdots \phi_n(\Sigma')$.

En conclusión, podemos suponer que K es normal.

Sea ϵ una raíz n-ésima de la unidad. Es obvio que K está incluida en una extensión de k por radicales si y solo si $K(\epsilon)$ está incluida en una extensión de $k(\epsilon)$ por radicales.

$K \cap k(\epsilon)$ es una k-extensión de Galois de grupo cíclico (pues es una subextensión de $k(\epsilon)$). Por 2.5.16, la sucesión obvia,

$$1 \to \mathrm{Aut}_{k(\epsilon)-alg}(K(\epsilon)) \to Aut_{k-alg}(K) \to \mathrm{Aut}_{k-alg}(K \cap k(\epsilon)) \to 1$$

es exacta. Por tanto, $\mathrm{Aut}_{k-alg}(K)$ es un grupo resoluble si y solo si $\mathrm{Aut}_{k(\epsilon)-alg}(K(\epsilon))$ es resoluble.

En conclusión, podemos suponer que $\epsilon \in k$.

Si el grupo de Galois de K es resoluble, por el teorema anterior K es una extensión por radicales (luego está incluida en una extensión por radicales).

Si K está incluida en una extensión K', que sea una extensión por radicales, entonces está incluida en una extensión K'' normal que es una extensión por radicales. Luego el grupo de automorfismos de K'' es resoluble, por el teorema anterior. Luego el grupo de de automorfismos de K es resoluble, porque es un cociente del de K''.

□

17. Definición: Diremos que un polinomio $p(x) \in k[x]$ es resoluble por radicales si todas sus raíces están incluidas en una extensión de k por radicales.

18. Definición: Sea $p(x) \in k[x]$, llamaremos grupo asociado a $p(x)$ al grupo de automorfismos del cuerpo de descomposición de $p(x)$.

19. Corolario: *Un polinomio $p(x) \in k[x]$ es resoluble por radicales si y solo si el grupo asociado al polinomio es resoluble.*

20. Sea k un cuerpo y $a_1, \ldots, a_n$ variables libres. Consideremos el cuerpo $k(a_1, \ldots, a_n)$, y el polinomio con coeficientes en este cuerpo:

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

que se denomina *ecuación general de grado n sobre k*. Denotemos $\alpha_1, \ldots, \alpha_n$ a las raíces de este polinomio (que también son variables libres sobre k). El grupo simétrico de n letras, S_n, opera en $k(\alpha_1, \ldots, \alpha_n)$ de modo natural (por automorfismos de k-álgebras), permutando las α_i. Obviamente

$$k(a_1, \ldots, a_n) \subseteq k(\alpha_1, \ldots, \alpha_n)^{S_n}$$

y $k(a_1, \ldots, a_n) \hookrightarrow k(\alpha_1, \ldots, \alpha_n)$ es una extensión de Galois, cuyo grupo está incluido en S_n, luego es igual a S_n. Por el teorema de Artin se concluye que

$$k(a_1, \ldots, a_n) \to k(\alpha_1, \ldots, \alpha_n)$$

es una extensión de Galois de grupo S_n. Es decir, *el grupo de la ecuación general de grado n es S_n.*

21. Teorema: *La ecuación general de grado n es resoluble por radicales para $n \leq 4$ y no es resoluble por radicales para $n > 4$.*

Demostración. Se deduce de que el grupo simétrico S_n es resoluble si y solo si $n \leq 4$. □

22. Proposición: *La condición necesaria y suficiente para que un polinomio irreducible y separable de grado primo sea resoluble por radicales es que el cuerpo de descomposición esté generado por dos de sus raíces. En este caso el cuerpo de descomposición está generado por dos de sus raíces cualesquiera.*

Demostración. Si el polinomio es resoluble entonces el grupo G asociado es resoluble. Por el teorema 2.8.26, G está incluido en el metacíclico $N \subset S_p = \mathrm{Biy}(\mathbb{Z}/p\mathbb{Z})$, donde $N = \{\sigma_{i,j}$, con $(i,j) \in \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^*\}$, siendo $\sigma_{i,j}$ la permutación definida por $\sigma_{i,j}(x) = jx + i$. Dados $x \neq x' \in \mathbb{Z}/p\mathbb{Z}$, entonces $\sigma_{i,j} = \mathrm{Id}$ si y solo si $\sigma_{i,j}(x) = x$ y $\sigma_{i,j}(x') = x'$. Por tanto, la extensión generada por dos raíces cualesquiera solo es invariante por Id, es decir, coincide con el cuerpo de descomposición de $p(x)$.

Recíprocamente, si el cuerpo de descomposición de $p(x)$ está generado por dos raíces α_1, α_2, entonces el orden de su grupo de Galois, G, es $\dim_k k(\alpha_1,\alpha_2) = \dim_k k(\alpha_1) \cdot \dim_{k(\alpha_1)} k(\alpha_1,\alpha_2) = p \cdot q$, con $q < p$. Entonces el número de p-subgrupo de Sylow de G, que divide a q y es congruente con 1 módulo p, es 1. Es decir, el p-subgrupo de Sylow de G, H_p, es normal. Luego, G está incluido en $N(H_p) \subset S_p$ que es un subgrupo metacíclico. Por tanto, G es resoluble y $p(x)$ es resoluble por radicales.

□

23. Corolario: *Si un polinomio irreducible de grado primo $p(x) \in \mathbb{R}[x]$, tiene dos raíces reales y es resoluble, entonces todas sus raíces son reales.*

24. Resolución de la ecuación cúbica (general), $x^3 + a_1x^2 + a_2x + a_3 = 0$.

Se verifica que S_3 es un grupo resoluble: el alternado $A_3 = <(1,2,3)> \approx \mathbb{Z}/3\mathbb{Z}$ es un subgrupo normal y $S_3/A_3 = <\overline{(1,2)}> \approx \mathbb{Z}/2\mathbb{Z}$.

Notación: En lo que sigue, denotaremos $\sigma = (1,2,3)$ y $\tau = (1,2)$; x_1, x_2, x_3 son las raíces la cúbica y $K = k(x_1,x_2,x_3)$.

La extensión $k \subset K^{A_3}$ es de Galois de grado 2 de grupo $S_3/A_3 = <\overline{(1,2)}> \approx \mathbb{Z}/2\mathbb{Z}$, es decir, generado por la permutación τ y la extensión $K^{A_3} \subset K$ es de Galois de grado 3 y grupo $A_3 = <\sigma> \approx \mathbb{Z}/3\mathbb{Z}$.

Característica de k distinta de 2 y de 3.

Por la fórmula de Lagrange, las raíces $x_1, x_2, x_3 \in K$ se expresan en función de radicales cúbicos de elementos de K^{A_3} de la siguiente forma:

$$x_i = \frac{1}{3}(R(x_i,1) + R(x_i,\varepsilon) + R(x_i,\varepsilon^2))$$

donde

$$R(x_i,1) = x_i + \sigma(x_i) + \sigma^2(x_i) = x_1 + x_2 + x_3 = -a_1$$
$$R(x_i,\varepsilon) = x_i + \sigma(x_i)\varepsilon + \sigma^2(x_i)\varepsilon^2 = \sigma^{i-1}(R(x_1,\varepsilon)) = \varepsilon^{2(i-1)}R(x_1,\varepsilon)$$
$$R(x_i,\varepsilon^2) = x_i + \sigma(x_i)\varepsilon^2 + \sigma^2(x_i)\varepsilon = \sigma^{i-1}(R(x_1,\varepsilon^2)) = \varepsilon^{i-1}R(x_1,\varepsilon^2)$$

Luego basta calcular los radicales cúbicos $R_1 = R(x_1, \varepsilon)$ y $R_2 = R(x_1, \varepsilon^2)$. Se cumple que $\sigma(R_1) = \varepsilon^2 \cdot R_1$, $\sigma(R_2) = \varepsilon \cdot R_2$, $\tau(R_1) = \varepsilon R_2$ y $\tau(R_2) = \varepsilon^2 R_1$ luego $R_1 \cdot R_2$ es invariante por S_3, es decir, $R_1 \cdot R_2 \in K^{S_3} = k$. Un cálculo sencillo prueba que

$$R_1 \cdot R_2 = a_1^2 - 3a_2.$$

$R_1^3 \in K^{A_3}$ y K^{A_3} es una k-extensión de Galois de grupo $\langle \tau \rangle$. Aplicando la resolvente de Lagrange,

$$R_1^3 = \frac{1}{2}(R_1^3 + \tau(R_1^3)) + \frac{1}{2}(R_1^3 - \tau(R_1^3))$$

Calculando resulta:

$$\frac{1}{2}(R_1^3 + \tau(R_1^3)) = \frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2}$$
$$\frac{1}{2}(R_1^3 - \tau(R_1^3)) = \frac{3}{2}\sqrt{-3\Delta}$$

Observación: Como se puede comprobar es $\tau(R_1) = \varepsilon R_2$, luego $\tau(R_1^3) = R_2^3$. Por lo tanto, $R_2^3 = \frac{1}{2}(R_1^3 + \tau(R_1^3)) - \frac{1}{2}(R_1^3 - \tau(R_1^3))$.

En conclusión, resulta:

$$x_i = \frac{1}{3}\Big(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\Big)$$

donde los dos radicales cúbicos no son independientes, ya que, como dijimos, el primero determina el segundo pues el producto de estos dos es $R_1 \cdot R_2 = a_1^2 - 3a_2$.

Característica de k igual a 2.

En característica 2 hay que sustituir el cálculo hecho de R_1^3 por el de la resolución de la ecuación $x^2 + ax + b$ (en característica 2) cuyas raíces son R_1^3 y $\tau(R_1^3) = R_2^3$, luego $a = R_1^3 + R_2^3 = -2a_1^3 + 9a_1a_2 - 27a_3 = a_1a_2 + a_3$ (que es distinto de cero ya que $\Delta = (a_1a_2 + a_3)^2 \neq 0$) y $b = R_1^3 \cdot R_2^3 = (a_1^2 - 3a_2)^3 = (a_1^2 + a_2)^3$. Resolviendo queda:

$$x_i = a_1 + \sqrt[3]{(a_1a_2 + a_3) \cdot \Big(\sqrt[2]{(a_1^2 + a_2)^3/(a_1a_2 + a_3)^2}\Big)} + \sqrt[3]{(a_1a_2 + a_3) \cdot \Big(\sqrt[2]{(a_1^2 + a_2)^3/(a_1a_2 + a_3)^2} + 1\Big)} \qquad \text{(car. } k = 2\text{)}$$

Característica de k igual a 3.

Supongamos que $a_1 \neq 0$.

La traza de x_1 (por el grupo A_3) es igual a $-a_1$, que es no nulo. Por tanto, tenemos que $\beta = \frac{(\sigma-\mathrm{Id})(x_1)}{Tr(x_1)} = \frac{x_1-x_2}{a_1}$ es un radical modificado. En efecto, $a := \beta^3 - \beta = \frac{(x_1-x_2)^3-a_1^2(x_1-x_2)}{a_1^3} = \frac{-(x_1-x_2)(x_1-x_3)(x_2-x_3)}{a_1^3} = \frac{\sqrt{\Delta}}{a_1^3} = \frac{\sqrt{a_1^2a_2^2-a_1^3a_3-a_2^3}}{a_1^3}$ y $\beta = \sqrt[3]{a}$.

Por 2.6.9,

$$x_1 = -a \cdot Tr(x_1/\beta) - Tr(x_1 \cdot \beta) \cdot \beta - Tr(x_1) \cdot \beta^2$$

$Tr(x_1) = -a_1$. $Tr(x_1\beta) = x_1\beta + x_2(\beta+1) + x_3(\beta+2) = -a_1\beta + x_2 + 2x_3 = -x_1 + 2x_2 + 2x_3 = a_1$. $Tr(x_1/\beta) = a_1 \cdot Tr(\frac{x_1}{x_1-x_2}) = a_1 \cdot \frac{x_1(x_2-x_3)(x_3-x_1)+x_2(x_1-x_2)(x_3-x_1)+x_3(x_1-x_2)(x_2-x_3)}{(x_1-x_2)(x_2-x_3)(x_3-x_1)} = \frac{-a_1^2a_2}{\sqrt{\Delta}}$. Luego, $x_1 = \frac{a_2}{a_1} - a_1\beta + a_1\beta^2$ y

$$\boxed{x_1 = \frac{a_2}{a_1} - a_1\sqrt[3]{\sqrt{a_1^2a_2^2-a_1^3a_3-a_2^3}\,/a_1^3} + a_1\left(\sqrt[3]{\sqrt{a_1^2a_2^2-a_1^3a_3-a_2^3}\,/a_1^3}\right)^2} \quad \left(\begin{array}{l}\mathrm{car}\, k = 3\\ a_1 \neq 0\end{array}\right)$$

Supongamos ahora que $a_1 = 0$.

Hagamos el cambio de variable $x = \sqrt{-a_2}y$, entonces tenemos que $x^3 + a_2x + a_3 = (-a_2)^{3/2} \cdot (y^3 - y + (a_3/(-a_2)^{3/2}))$, cuyas raíces son $y_i = \sqrt[3]{-a_3/(-a_2)^{3/2}} + i$ y

$$\boxed{x_i = \sqrt{-a_2} \cdot \left(\sqrt[3]{-a_3/(-a_2)^{3/2}} + i\right)} \qquad (\text{car. } k = 3, a_1 = 0).$$

25. Teorema: *Sea K una extensión de Galois de grupo $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ ($n = n_1 \cdots n_r$ primo con la característica). Sea $\{\sigma_1, \ldots \sigma_r\}$ un sistema de generadores de G de órdenes $n_1, \ldots, n_r$, respectivamente, y ε_i raíces n_i-ésimas primitivas de la unidad, para $1 \leq i \leq r$. Dado $\alpha \in K$, denotemos*

$$R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r}) = \sum_{i_1 < n_1, \ldots, i_r < n_r} \varepsilon_1^{i_1 j_1} \cdots \varepsilon_r^{i_r j_r} (\sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r})(\alpha).$$

$R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r})$ son radicales d-ésimos (d el mínimo común múltiplo de $n_1, \ldots, n_r$) y se cumple la fórmula:

$$\alpha = \frac{1}{n} \sum_{j_1 < n_1, \ldots, j_r < n_r} R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r}).$$

Demostración. Se cumple que $R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r}) \overset{*}{=} R(R(\alpha, \varepsilon_1^{j_1}), \varepsilon_2^{j_2} \ldots, \varepsilon_r^{j_r})$. Procedamos por

inducción sobre r. Sea $n' = n_2 \cdots n_r$. Entonces,

$$\alpha = \frac{1}{n_1} \sum_{j_1<n_1} R(\alpha, \varepsilon_1^{j_1}) = \frac{1}{n_1} \sum_{j_1<n_1} (\frac{1}{n'} \sum_{j_2<n_2,\ldots,j_r<n_r} R(R(\alpha, \varepsilon_1^{j_1}), \varepsilon_2^{j_2}, \ldots, \varepsilon_r^{j_r}))$$
$$= \frac{1}{n} \sum_{j_1<n_1,\ldots,j_r<n_r} R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r}).$$

Denotemos $G_i = \langle \sigma_i \rangle$. Denotemos $R = R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r})$. Por la igualdad $\stackrel{*}{=}$, $R^{n_1} \in K^{G_1}$. Como la definición de la resolvente R no depende del orden con el que se tomen los σ_i, tenemos que $R^{n_i} \in K^{G_i}$. Por tanto, $R^d \in \cap_i K^{G_i} = K^{\langle G_1,\ldots,G_r \rangle} = K^G = k$.

□

26. Resolución de la ecuación cuártica (general), $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$.

S_4 es un grupo resoluble: se tiene la cadena normal $K_4 \subset A_4 \subset S_4$ donde

$$K_4 = < (1,2)(3,4), (1,3)(2,4) > \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

es el grupo de Klein y los factores son $A_4/K_4 = < \overline{(1,2,3)} > \approx \mathbb{Z}/3\mathbb{Z}$ y $S_4/A_4 = < \overline{(1,2)} > \approx \mathbb{Z}/2\mathbb{Z}$.

Notación: Denotaremos $s_1 = (1,2)(3,4)$ y $s_2 = (1,3)(2,4)$; x_1, x_2, x_3, x_4 son las raíces la cuártica y $K = k(x_1, x_2, x_3, x_4)$.

La extensión $K^{K_4} \subset K$ es de Galois de grado 4 y de grupo $K_4 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generado por las permutaciones s_1, s_2.

Sean

$$\theta_1 = x_1x_2 + x_3x_4$$
$$\theta_2 = x_1x_3 + x_2x_4$$
$$\theta_3 = x_1x_4 + x_2x_3$$

Se verifica que una permutación τ deja fijos a estos 3 elementos si y solo si $\tau \in K_4$, luego $K^{K_4} = k(\theta_1, \theta_2, \theta_3)$. Además el grupo simétrico permuta estos elementos entre sí (dando una identificación de S_4/K_4 con S_3) y, por tanto, son las raíces de una cúbica con coeficientes en k, a saber:

$$(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 - a_2x^2 + (a_1a_3 - 4a_4)x - (a_1^2a_4 - 4a_2a_4 + a_3^2).$$

Esta cúbica es a la que se denomina *cúbica resolvente*.

Característica de k distinta de 2

Por ser la característica distinta de 2 se puede aplicar la fórmula de Lagrange generalizada al caso no cíclico (como es K_4).

Las resolventes de x_1 respecto de $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ son:

$$\begin{aligned} R(x_1,1,1) &= x_1+x_2+x_3+x_4 = -a_1 \\ R(x_1,1,-1) &= x_1+x_2-x_3-x_4 = \xi_1 \\ R(x_1,-1,1) &= x_1-x_2+x_3-x_4 = \xi_2 \\ R(x_1,-1,-1) &= x_1-x_2-x_3+x_4 = \xi_3 \end{aligned}$$

donde ξ_1,ξ_2,ξ_3 son radicales cuadráticos sobre $K^{K_4} = k(\theta_1,\theta_2,\theta_3)$, es decir, $\xi_1^2,\xi_2^2,\xi_3^2 \in K^{K_4}$ y verifican la relación $\xi_1\xi_2\xi_3 = -a_1^3+4a_1a_2-8a_3$. Como se puede comprobar es: $\xi_i^2 = a_1^2-4a_2+4\theta_i$, luego cuando la característica es distinta de 2 es $K^{K_4} = k(\xi_1^2,\xi_2^2,\xi_3^2)$.

Resolviendo la cúbica resolvente se concluye, por ser:

$$\boxed{x_i = \frac{1}{4}(-a_1 + \sqrt{a_1^2-4a_2+4\theta_1} + \sqrt{a_1^2-4a_2+4\theta_2} + \sqrt{a_1^2-4a_2+4\theta_3})} \text{ (car } k \neq 2)$$

donde el producto de cada dos de estos radicales cuadráticos determinan el tercero, pues el producto de los tres es $-a_1^3+4a_1a_2-8a_3$.

Característica de k igual a 2.

$K = K^{\mathbb{Z}/2\mathbb{Z}\times 0} \otimes_{K^{K_4}} K^{0\times\mathbb{Z}/2\mathbb{Z}} = K^{K_4}(\beta_1) \otimes_{K^{K_4}} K^{K_4}(\beta_2) = K^{K_4}(\beta_1,\beta_2)$. Donde β_1 y β_2 son radicales modificados, β_1 invariante por s_1 y β_2 invariante por s_2.

$\underline{a_1 \neq 0}$:

La traza de x_1 por K_4 es $-a_1 = a_1 \neq 0$. Entonces, $x_1 + s_1(x_1) = x_1+x_2$ es invariante por s_1 y su traza por $0\times\mathbb{Z}/2\mathbb{Z} = \langle s_2\rangle$ es $a_1 \neq 0$ y podemos tomar $\beta_1 = \frac{x_1+x_2}{a_1}$. Además, $\beta_1^2-\beta_1 = \frac{(x_1+x_2)^2}{a_1^2} + \frac{x_1+x_2}{a_1} = \frac{(x_1+x_2)(x_3+x_4)}{a_1^2} = \frac{a_2+\theta_1}{a_1^2} =: b_1$, luego $\beta_1 = \wp_2\backslash\underline{b_1}$. Equivalentemente, $\beta_2 = \frac{x_1+x_3}{a_1}$ y $\beta_2 = \wp_2\backslash\underline{b_2}$, con $b_2 := (a_2+\theta_2)/a_1^2$.

Por tanto,

$$\begin{aligned} x_1 &= Tr_{\langle s_2\rangle}(x_1b_1/\beta_1) + Tr_{\langle s_2\rangle}(x_1)\cdot\beta_1 \\ &= Tr_{K_4}(x_1b_1b_2/\beta_1\beta_2) + Tr_{K_4}(x_1b_2/\beta_2)\cdot\beta_1 + Tr_{K_4}(x_1b_1/\beta_1)\cdot\beta_2 + Tr_{K_4}(x_1)\cdot\beta_1\cdot\beta_2 \\ &= \theta_3/a_1 + 0 + 0 + a_1\beta_1\beta_2 \end{aligned}$$

Luego,

$$\boxed{x_1 = \theta_3/a_1 + a_1\cdot\wp_2\backslash\underline{(a_2+\theta_1)/a_1^2}\cdot\wp_2\backslash\underline{(a_2+\theta_2)/a_1^2}} \quad (\text{car } k=2, a_1\neq 0)$$

$\underline{a_1 = 0}$ (luego, $x_4 = x_1 + x_2 + x_3$)

Si $a_3 = 0$, $x^4 + a_2x^2 + a_4 = y^2 + a_2y + a_4$, y $\boxed{x_1 = \sqrt[2]{a_2 \bigwedge_2 a_4/a_2^2}}$, (car $k = 2, a_1 = a_3 = 0$).

Podemos suponer $a_3 \neq 0$. La traza de $x_1x_2x_3$ por K_4, es $-a_3 = a_3 \neq 0$. Entonces, $x_1x_2x_3 + s_1(x_1x_2x_3) = x_1x_2x_3 + x_1x_2x_4$ es invariante por s_1 y su traza por $\langle s_2 \rangle$ es $a_3 \neq 0$ y podemos tomar $\beta_1 = \frac{x_1x_2x_3 + x_1x_2x_4}{a_3}$. Además, $b_1 := \beta_1^2 - \beta_1 = a_4/\theta_1^2$ y $\beta_1 = \bigwedge_2 \underline{b_1}$. Igualmente, $\beta_2 = x_1x_2x_3 + x_1x_3x_4$ y $\beta_2 = \bigwedge_2 \underline{b_2}$, con $b_2 = a_4/\theta_2^2$.

Por tanto,

$$\begin{aligned} x_1 &= Tr_{\langle s_2 \rangle}(x_1b_1/\beta_1) + Tr_{\langle s_2 \rangle}(x_1) \cdot \beta_1 \\ &= Tr_{K_4}(x_1b_1b_2/\beta_1\beta_2) + Tr_{K_4}(x_1b_2/\beta_2) \cdot \beta_1 + Tr_{K_4}(x_1b_1/\beta_1) \cdot \beta_2 + Tr_{K_4}(x_1) \cdot \beta_1 \cdot \beta_2 \\ &= a_4/a_3 + (x_1 + x_3)\beta_1 + (x_1 + x_2)\beta_2 + 0 \end{aligned}$$

Además, $a_3 = \theta_2 \cdot (x_1 + x_3)$ y $a_3 = \theta_1 \cdot (x_1 + x_2)$. Entonces,

$$\boxed{x_1 = a_4/a_3 + (a_3/\theta_2) \cdot \bigwedge_2 \underline{a_4/\theta_1^2} + (a_3/\theta_1) \cdot \bigwedge_2 \underline{a_4/\theta_2^2}} \quad (\text{car } k = 2, a_1 = 0, a_3 \neq 0)$$

2.6.3. Grupo de Galois de las cúbicas y las cuárticas

Los cálculos anteriores se han realizado para los polinomios genéricos, pero obviamente son válidos para cualquier polinomio.

Si un polinomio de grado 2, $x^2 + a_1x + a_2$, es irreducible, su grupo de Galois es S_2 y, en caso contrario es trivial. Es reducible si y solo si tiene raíces en k y esto sucede cuando $\sqrt{a_1^2 - 4a_2} \in k$.

27. Proposición : *Sea $p(x) \in k[x]$ un polinomio separable de grado n. El grupo de Galois $G \subseteq S_n$ de $p(x)$ está incluido en el grupo alternado A_n si y solo si el discriminante Δ de $p(x)$ es un cuadrado en k. Es decir,*

$$G \subseteq A_n \iff \sqrt{\Delta} \in k$$

Demostración. Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$, $\sqrt{\Delta} = \prod_{i<j}(\alpha_i - \alpha_j) \in k(\alpha_1, \ldots, \alpha_n)$. Además, dado $\sigma \in G \subseteq S_n$, $\sigma(\sqrt{\Delta}) = \text{sign}(\sigma) \cdot \sqrt{\Delta}$. Entonces, $\sqrt{\Delta} \in k = k(\alpha_1, \ldots, \alpha_n)^G$ $\iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$, para todo $\sigma \in G \iff \text{sign}(\sigma) = 1$, para todo $\sigma \in G \iff G \subseteq A_n$. □

Consideremos un polinomio irreducible de grado 3, $x^3 + a_1x^2 + a_2x + a_3$. Como el grupo de Galois, G es transitivo, su orden es múltiplo de 3, luego G es igual a A_3 ó S_3. Tenemos que $\Delta = a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2$. Si $\sqrt{\Delta} \in k$ entonces $G = A_3$. Si $\sqrt{\Delta} \notin k$ entonces $G = S_3$.

Consideremos un polinomio irreducible de grado 4, $x^4+a_1x^3+a_2x^2+a_3x+a_4$. Como las cuatro raíces son distintas, es fácil comprobar que las tres raíces de su cúbica resolvente también son distintas entre sí. $G\cap K_4$ son los automorfismos que dejan fijas las tres raíces, $\theta_1,\theta_2,\theta_3$ de la cúbica resolvente, luego $k(\alpha_1,\ldots,\alpha_4)^{G\cap K_4} = k(\theta_1,\theta_2,\theta_3) = K'$. Observemos que $G/(G\cap K_4) \subseteq S_4/K_4 = S_3$. Denotemos $d = \#(G/(G\cap K_4))$, que el grado de la extensión $k \hookrightarrow K'$. Tenemos que $d = 6,3,2,1$.

Como la cuártica se supone irreducible, el orden de su grupo de Galois, G, es múltiplo de 4.

Si $d = 6$, entonces el orden de G es 12 o 24. Si es 12 entonces $A_4 = G$ y $K_4 \subseteq G$. Por tanto, $G\cap K_4 = K_4$, luego el orden de G es 24. En conclusión, si $d = 6$, $G = S_4$.

Si $d = 3$, entonces el orden de G es 12 y $G = A_4$.

Si $d = 2$, entonces el orden de G es 4 (cuando $G\cap K_4$ es de orden 2, que no actúa transitivamente sobre las raíces de la cuártica, luego ésta es reducible sobre K') y $G = \mathbb{Z}/4\mathbb{Z}$, ó el orden de G es 8 y contiene a K_4 (que actúa transitivamente sobre las raíces de la cuártica, luego ésta es irreducible sobre K'), luego $G = D_4$ (el grupo diédrico).

Si $d = 1$, entonces $G = K_4$.

2.7. Extensiones por radicales cuadráticos

Sea k un cuerpo, de característica distinta de dos.

Dado $a \in k$, la extensión $k \hookrightarrow k(\sqrt{a})$ tiene grado 1 o 2 según que $\sqrt{a}$ pertenezca a k o no. Recíprocamente, si $k \hookrightarrow K$ es una extensión de grado 2, entonces $K = k(\alpha)$, donde α es una raíz de un polinomio con coeficientes en k, irreducible de grado 2. La bien conocida fórmula de las raíces de los polinomios de grado 2, prueba que $K = k(\sqrt{a})$, para cierto $a \in k$.

1. Definición: Diremos que una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si $K = k(\alpha_1,\ldots,\alpha_n)$, donde $\alpha_i^2 \in k(\alpha_1,\ldots,\alpha_{i-1})$, para todo $1 \le i \le n$.

De la discusión anterior se sigue que el grado de extensión por radicales cuadráticos es una potencia de 2. Además, es obvio que el compuesto de un número finito de extensiones por radicales cuadráticos de k es una extensión por radicales cuadráticos de k.

2. Teorema: *Sea $k \hookrightarrow K$ una extensión de Galois. K es una extensión por radicales cuadráticos de k si y solo si es de grado una potencia de 2.*

Demostración. Solo tenemos que probar el recíproco. Como $\#G = 2^n$, entonces G es resoluble y existe una serie normal $\{1\} \subset G_1 \subset \cdots \subset G_n = G$ de factores isomorfos a $\mathbb{Z}/2\mathbb{Z}$.

Esta sucesión de grupos por toma de invariantes se corresponde con una sucesión de subcuerpos $K \supset K^{G_1} \supset \cdots \supset K^{G_n} = k$, cada uno de grado 2 sobre el anterior. Por tanto, $K^{G_i} = K^{G_{i-1}}(\alpha_i)$, donde $\alpha_i^2 \in K^{G_i}$. Luego, $K = k(\alpha_1, \ldots, \alpha_n)$ es una extensión por radicales cuadráticos. □

3. Ejercicio: Sea $K = k(x_1, \ldots, x_4)$ el cuerpo descomposición de la ecuación general de grado 4. Sea $H = \langle (1,2,3) \rangle \subset S_4$. Prueba que el grado de la k-extensión K^H es 2^3 y que la envolvente de Galois de K^H es K que es de grado 24. Prueba que K^H no es una extensión por radicales cuadráticos.

4. Proposición: *Una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si y solo si está incluida en una extensión por radicales cuadráticos.*

Demostración. Supongamos que K está incluida en una extensión $k \hookrightarrow \Sigma$ por radicales cuadráticos. Σ es separable y su envolvente de Galois es una extensión por radicales cuadráticos. Luego podemos suponer que Σ es de Galois. Su grupo de Galois G es un 2-grupo. Sea $H \subset G$ tal que $\Sigma^H = K$. Existe una cadena de grupos $H \subset H_1 \subset H_2 \subset \cdots \subset H_n = G$ de modo que $|H_{i+1}/H_i| = 2$, para todo i (ver demostración del primer teorema de Sylow 0.1.76). Tenemos la cadena $k \hookrightarrow K^{H_{n-1}} \hookrightarrow \cdots \hookrightarrow K^{H_1} \hookrightarrow K$ que muestra que $k \hookrightarrow K$ es una extensión de cuerpos por radicales cuadráticos. □

5. Corolario: *Una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si y solo si su envolvente de Galois es de grado 2^n.*

Demostración. Si K es una extensión por radicales cuadráticos, su envolvente de Galois es una extensión por radicales cuadráticos, luego es de grado 2^n. Si la envolvente de Galois de K es de grado 2^n, entonces es una extensión por radicales cuadráticos y K también.

□

6. Definición: Diremos que un elemento $\alpha \in K$ de una extensión de cuerpos de k es un irracional cuadrático de k, si existe una extensión por radicales cuadráticos de k que contiene a α. Diremos que un polinomio con coeficientes en k es resoluble por radicales cuadráticos si todas sus raíces son irracionales cuadráticos.

7. Ejercicio: Si α es un irracional cuadrático sobre k, pruébese que $k(\alpha)$ es una extensión de k por radicales cuadráticos.

Si un polinomio es irreducible y una raíz es un irracional cuadrático entonces todas las raíces son irracionales cuadráticos, ya que si α y β son raíces de $p(x)$, entonces $k(\alpha) = k[x]/(p(x)) = k(\beta)$.

8. Teorema: *Un polinomio irreducible con coeficientes en k es resoluble por irracionales cuadráticos si y solo si es separable y su grupo de Galois es un grupo de orden una potencia de* 2.

Demostración. Si el polinomio es resoluble por irracionales cuadráticos entonces su cuerpo de descomposición puede incluirse en una extensión por radicales cuadráticos de k, luego es separable, de Galois y es una extensión por radicales cuadráticos de k. Por tanto, el cuerpo de descomposición de $p(x)$ es de grado una potencia de 2, luego su grupo de Galois es un grupo de orden una potencia de 2.

Si el polinomio es separable y su grupo de Galois es un grupo de orden una potencia de 2, entonces su cuerpo de descomposición es una extensión por radicales cuadráticos de k y las raíces del polinomio son irracionales cuadráticos.

□

2.7.1. Construcciones con regla y compás

Consideremos en el plano euclídeo un conjunto de puntos $\mathbb{P}$, de cardinal mayor o igual que dos. El conjunto $\mathscr{C}(\mathbb{P})$ de los puntos del plano euclídeo constructibles con regla y compás a partir de $\mathbb{P}$ se define inductivamente mediante la aplicación reiterada de un número finito de las construcciones 2., 3. y 4.:

1. Diremos que los puntos de $\mathbb{P}$ son constructibles.

2. Diremos que las rectas que pasan por un par de puntos constructibles son constructibles.

3. Diremos que las circunferencias de centro un punto constructible y radio la distancia entre dos puntos constructibles son constructibles.

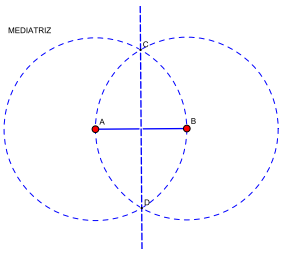
4. Diremos que los puntos de corte entre dos líneas constructibles (rectas o circunferencias) son constructibles.

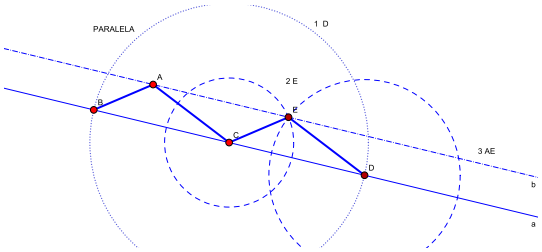
5. $\mathscr{C}(\mathbb{P})$ es el conjunto de todos los puntos constructibles (con regla y compás a partir de $\mathbb{P}$).

Es bien conocido que las siguiente construcciones pueden realizarse con regla y compás:

- Trazar la perpendicular por su punto medio a un segmento dado.

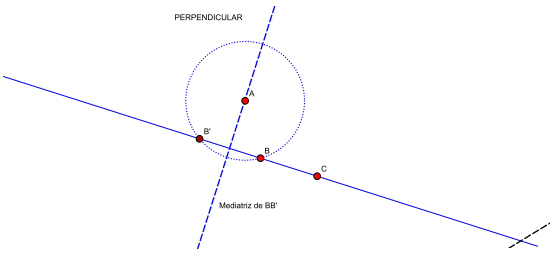
- Dados tres puntos no alineados A,B,C, trazar la paralela a la recta BC que pasa por A.

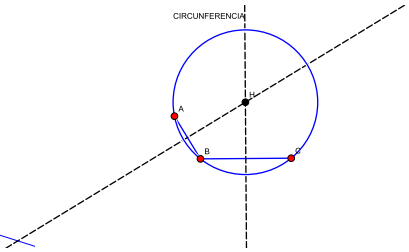




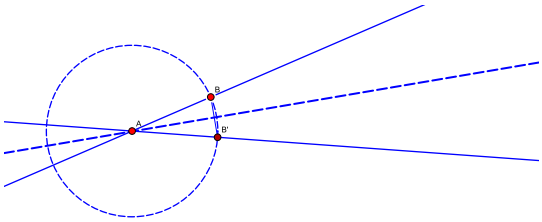
- Dados tres puntos no alineados A, B, C, trazar la perpendicular a la recta BC que pasa por A.

- Trazar la circunferencia que pasa por tres puntos no alineados A, B y C





- Trazar la bisectriz de un ángulo dado.



Escojamos dos puntos de $\mathbb{P}$ como sistema de referencia, uno el origen de coordenadas $(0,0)$ y el otro el $(0,1)$. Identifiquemos el plano euclídeo con $\mathbb{C}$. Los puntos escogidos se corresponden con el 0 y 1 de $\mathbb{C}$. Los puntos de $\mathbb{C}(\mathbb{P})$ se corresponden con ciertos números complejos. A partir de ahora identificamos los puntos del plano euclídeo con los correspondientes números complejos.

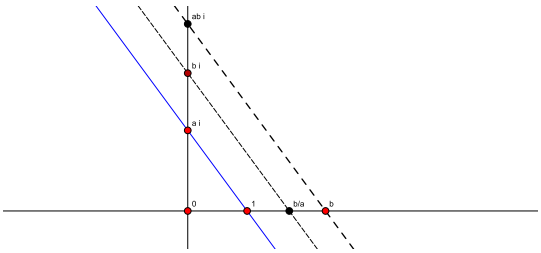
9. Lema: *La condición necesaria y suficiente para que un número complejo $a+bi$ sea constructible es que lo sean su parte real a y su parte imaginaria b.*

Demostración. Es consecuencia directa de la posibilidad de trazar paralelas y perpendiculares con regla y compás. □

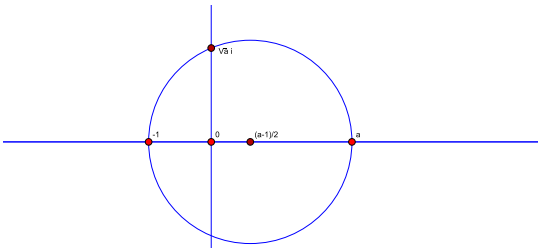
10. Lema: *Los números complejos constructibles $\mathscr{C}(\mathbb{P})$, forman un subcuerpo de $\mathbb{C}$, estable por toma de raíces cuadradas.*

Demostración. La suma y diferencia de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales y este caso es trivial.

El producto y cociente de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales. En la siguiente figura construimos el producto y cociente de a y b.



Para concluir hay que demostrar que la raíz cuadrada de cualquier número complejo constructible también lo es. Si el número es real, basta considerar la siguiente figura:



En el caso de un número complejo arbitrario, se construye la bisectriz del ángulo que determina con el 1 y se traza en ella el segmento de longitud igual a la raíz cuadrada del módulo del número complejo dado.

□

11. Teorema: *Sea k el mínimo subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{P}$. La condición necesaria y suficiente para que un número complejo sea constructible a partir de $\mathbb{P}$ es que sea un irracional cuadrático de k.*

Demostración. Si α es un irracional cuadrático, entonces $k(\alpha)$ es una extensión de k por radicales cuadráticos. Por el lema anterior, α es constructible.

Para demostrar el recíproco, obsérvese que los coeficientes de las ecuaciones de las rectas y circunferencias son funciones racionales de las coordenadas de los puntos que las determinan, según las construcciones 2 y 3. Además, las coordenadas de la intersección de dos líneas (círculos o rectas), se expresan en función de los coeficientes de las ecuaciones como irracionales cuadráticos. Procediendo inductivamente concluimos que las coordenadas de cualquier punto constructible son irracionales cuadráticos sobre k. Es decir, si $a+bi$ es constructible, es un irracional cuadrático sobre k.

□

12. Definición: Se dice que un número primo $p \in \mathbb{Z}$ es un primo de Fermat si $p = 2^n + 1$, para cierto $n \in \mathbb{N}$.

13. Proposición: *Si 2^n+1 es primo, entonces n es igual a una potencia de 2.*

Demostración. Escribamos $n = 2^m \cdot m'$, con m' impar y sea $a = 2^{2^m}$. Entonces, $2^n + 1 = 2^{2^m \cdot m'} + 1 = a^{m'} + 1$ que es divisible por $a+1$. Entonces, si 2^n+1 es primo, $m' = 1$. □

Los únicos primos de Fermat conocidos son $3 = 2+1, 5 = 2^2+1, 17 = 2^4+1, 257 = 2^8+1, 65537 = 2^{16}+1$.

14. Proposición: *El polígono de n lados es constructible con regla y compás a partir de $\mathbb{P} = \{0,1\}$, si y solo si $n = 2^{n_0} \cdot p_1 \cdots p_r$, con $n_0 \geq 0$, $r \geq 0$ y $p_1, \ldots, p_r$ números primos de Fermat distintos.*

Demostración. El polígono de n lados es constructible con regla y compás si y solo si $e^{2\pi i/n}$ es constructible con regla y compás. Por los teoremas 2.7.8, 2.7.11, el polígono de n lados es constructible con regla y compás si y solo si $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/n})$ es una potencia de 2. Ahora bien, si $n = 2^m \cdot p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de n en producto de potencias de primos distintos, entonces,

$$\begin{aligned}\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/n}) &= |(\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/2^m\mathbb{Z})^*| \cdot |(\mathbb{Z}/p_1^{n_1}\mathbb{Z})^*| \cdots |(\mathbb{Z}/p_r^{n_r}\mathbb{Z})^*| \\ &= 2^{m-1} \cdot p_1^{n_1-1}(p_1-1) \cdots p_r^{n_r-1}(p_r-1),\end{aligned}$$

que es una potencia de dos si y solo si n es producto de una potencia de 2 y de números primos de Fermat distintos. □

Construyamos el pentágono regular. Tenemos que construir $\xi = e^{2\pi i/5}$, que es raíz de

$$\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$$

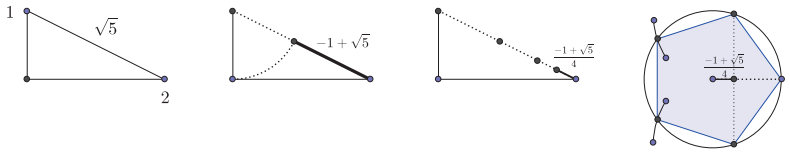
$\mathbb{Q}(\xi)$ es una $\mathbb{Q}$-extensión de Galois de grado 4, de grupo cíclico $G = \langle\sigma\rangle$, $\sigma(\xi) = \xi^2$. Consideremos las dos extensiones por un radical cuadrático

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\xi)^{\langle\sigma^2\rangle} = \mathbb{Q}(\xi + \xi^4) \hookrightarrow \mathbb{Q}(\xi)$$

El polinomio mínimo anulador de $\xi + \xi^4$ es

$$(x - (\xi + \xi^4)) \cdot (x - \sigma(\xi + \xi^4)) = (x - (\xi + \xi^4)) \cdot (x - (\xi^2 + \xi^3)) = x^2 + x - 1$$

Luego, $\xi + \xi^4 = (-1 + \sqrt{5})/2$. Observemos que si $\xi = a + bi$, entonces $2a = \xi + \xi^4 = (-1 + \sqrt{5})/2$ y $a = (-1 + \sqrt{5})/4$. Dibujemos el pentágono regular



Comentemos tres problemas irresolubles famosos de la Grecia clásica.

15. Duplicación del cubo: En el año 429 a. C., Pericles, gobernador de Atenas por esa época, muere víctima de la peste que atacaba muy severamente la ciudad. A raíz de este suceso algunos de los habitantes deciden ir a la ciudad de Delfos para hacer consultas al Oráculo de Apolo y saber como poder detener la epidemia. La respuesta a la consulta del Oráculo fue que debían elaborar un nuevo altar en forma de cubo cuyo volumen duplicara el del altar entonces existente.

Si el altar existente es un cubo de lado de longitud $a \in \mathbb{Q}$, su volumen es a^3. Para construir un altar de volumen $2a^3$, hay que construir un cubo de lado de longitud $\sqrt[3]{2} \cdot a$. Este problema se resuelve con regla y compás si y solo si $\sqrt[3]{2}$ es un irracional cuadrático sobre $\mathbb{Q}$, que no lo es, pues $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$.

16. Cuadratura del círculo: ¿Es posible, dado un círculo, construir con regla y compás un cuadrado del mismo área (y por tanto ser capaces de "conocer" el área del círculo)? Si el círculo es de radio $a \in \mathbb{Q}$, su área es $a^2 \cdot \pi$. El cuadrado de área $a^2 \cdot \pi$, es el cuadrado de lado de longitud $a \cdot \sqrt{\pi}$. Este problema se resuelve con regla y compás si y solo si $\sqrt{\pi}$ es un irracional cuadrático sobre $\mathbb{Q}$, que no lo es, pues como demostró Lindemann, π es trascendente, es decir, $\dim_{\mathbb{Q}} \mathbb{Q}(\pi) = \infty$ (luego $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{\pi}) = \infty$).

17. Trisección de un ángulo: ¿Es posible, dado un ángulo cualquiera, dividirlo en tres ángulos iguales, con regla y compás? Dar un ángulo de α radianes es dar el número complejo $e^{\alpha \cdot i}$ y trisecarlo con regla y compás es construir el número complejo $e^{\alpha \cdot i/3}$. Por ejemplo, si consideramos el ángulo $\pi/3$, es decir, el número complejo $e^{\pi/3 \cdot i}$, entonces $e^{\pi/9 \cdot i}$ no es un irracional cuadrático sobre $\mathbb{Q}(e^{\pi/3 \cdot i})$, porque $\dim_{\mathbb{Q}(e^{\pi/3 \cdot i})} \mathbb{Q}(e^{\pi/9 \cdot i}) = 3$.

2.8. Apéndice: Grupos resolubles

Series de composición.

1. Definición: Se dice que un grupo G es simple cuando no contiene subgrupos normales no triviales (es decir, distintos de $\{1\}$ y G).

2. Ejemplo: Un grupo abeliano, G, es simple si y solo si su orden es un número primo.

3. Definición: Se llama *serie normal* en G a cada cadena de subgrupos $1 \subset H_1 \subset \cdots \subset H_r = G$ tal que cada H_i es normal en el siguiente, H_{i+1}. Se llama *longitud* de una serie normal al número de términos distintos que aparecen. Se llaman *factores* de la serie normal a los grupos H_{i+1}/H_i.

4. Definición: Un grupo G se dice de *longitud infinita* si admite series normales de longitud arbitrariamente grande. En caso contrario, se define la *longitud de* G como el máximo de las longitudes de sus cadenas normales. Denotaremos a este número $long(G)$.

5. Definición: Una serie normal $1 \subset H_1 \subset \cdots \subset H_r = G$ se dice que es una *serie de composición* cuando sus términos son distintos y sus factores H_i/H_{i+1} son grupos simples.

Dicho de otro modo las cadenas de composición son las series normales de términos distintos tales que no se pueden refinar, es decir, añadir términos intermedios $H_i \subset H \subset H_{i+1}$ (obsérvese que tales subgrupos H se corresponden con subgrupos de H_{i+1}/H_i y, por tanto, la simplicidad de éste impide la existencia de tales subgrupos).

6. Ejemplo: Los grupos finitos abelianos tienen series de composición.

7. Definición: Se dice que un grupo es resoluble si contiene una serie normal de factores grupos abelianos.

8. Proposición: *Sea G un grupo finito y $|G| = p_1^{n_1} \cdots p_r^{n_r}$ la descomposición en factores primos. Entonces,*

1. *G es de longitud finita y*
$$long(G) \leq n_1 + \cdots + n_r$$
2. *Un grupo finito G es resoluble si y solo si*
$$long(G) = n_1 + \cdots + n_r$$

Demostración. Si $1 \subset H_1 \subset \cdots H_r = G$ es una serie normal, entonces por el teorema de Lagrange es
$$|G| = \prod_i |H_{i+1}/H_i|$$
Por tanto $|G|$ es el producto de r factores, luego r es menor o igual que el número de primos en los que descompone n, es decir, que $n_1 + \cdots + n_r$. Por tanto:
$$long(G) \leq n_1 + \cdots + n_r$$

Si G admite una cadena cuya longitud es de orden $n_1 + \cdots + n_r$, entonces, por lo dicho anteriormente, los factores tienen que tener orden primo, luego son abelianos y, por tanto, es resoluble. Recíprocamente, si G es resoluble, entonces admite una cadena de factores abelianos simples, luego de orden primo, es decir, de longitud $n_1 + \cdots + n_r$ (por la fórmula anterior) y por la acotación ésta es la longitud de G. □

9. Lema : *Sea $N \subset G$ es un subgrupo normal y $\pi : G \to G/N$ el paso al cociente. Se verifica:*

1. *Si se tiene una cadena $N \subseteq H_1 \subset H_2 \subseteq G$ con H_1 normal en H_2, entonces $\pi(H_1)$ es normal en $\pi(H_2)$ y*
$$H_2/H_1 \approx \pi(H_2)/\pi(H_1).$$
2. *Si G es de longitud finita, entonces también lo son N y G/N y*
$$long(N) + long(G/N) \leq long(G).$$
En particular, si $N \subset G$ es propio (es decir, distinto de $\{1\}$ y G), entonces $long(N)$ y $long(G/N)$ son menores estrictos que $long(G)$.

Demostración. (1) Si $h_2 \in H_2$, entonces $h_2 H_1 h_2^{-1} = H_1$, y por tanto $\pi(h_2)\pi(H_1)\pi(h_2)^{-1} = \pi(h_2 H_1 h_2^{-1}) = \pi(H_1)$. Es decir, $\pi(H_1)$ es normal en $\pi(H_2)$.

Consideremos el epimorfismo composición $H_2 \xrightarrow{\pi} \pi(H_2) \to \pi(H_2)/\pi(H_1)$. Es claro que el núcleo es $\pi^{-1}(\pi(H_1)) = H_1$ (ya que $N \subseteq H_1$) y, por el teorema de factorización tenemos que $H_2/H_1 \approx \pi(H_2)/\pi(H_1)$.

(2) Cada serie normal en H, $1 \underset{\neq}{\subset} H_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} H_r = N$, y cada serie normal en G/N, $1 \underset{\neq}{\subset} \overline{N}_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \overline{N}_s = G/N$, da una serie normal en G:

$$1 \underset{\neq}{\subset} H_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} H_r \underset{\neq}{\subset} N_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} N_s = G$$

(siendo $N_i = \pi^{-1}(\overline{N}_i)$) y de términos distintos (pues $\pi(N_i) = \overline{N}_i$), luego de longitud $r+s \leq long(G)$. En particular, $r \leq long(G)$ y $s \leq long(G)$. Por tanto, N y G/N son de longitud finita. Eligiendo las cadenas manera que sean de longitud máxima, se obtiene $long(N) + long(G/N) = r+s \leq long(G)$. □

10. Teorema de Jordan-Hölder: *Todo par de series de composición de un grupo tienen la misma longitud y los factores isomorfos (salvo permutación de éstos).*

Demostración. Por inducción sobre $long(G)$. Se observa que $long(G) = 1$ si y solo G es simple y por tanto su única cadena de composición es $\{1\} \subset G$ y no hay nada que demostrar.

Sean $1 \subset H_1 \subset \cdots \subset H_r = G$ y $1 \subset N_1 \subset \cdots \subset N_s = G$ dos series de composición.

• Si ambas tienen un término en común (distinto de los extremos) tal que es normal en G, digamos $H_i = N_j$, entonces se concluye. En efecto:

Por el lema anterior se tiene $long(H_i), long(G/H_i) < long(G)$. Por inducción se obtiene que las correspondientes cadenas definidas en H_i y G/H_i son de la misma longitud ($i = j$ y $r - i = s - j$ y, por tanto, $r = s$) y factores isomorfos (salvo una permutación), luego se concluye.

• Supongamos que no tienen ningún término en común: sea $M = H_{r-1} \cap N_{s-1}$ y una serie de composición $1 \subset M_1 \subset \cdots \subset M_l = M$. M es normal en G por ser intersección de dos subgrupos normales. Se tienen las cadenas:

$$\begin{aligned}
&1 \subset H_1 \subset \cdots \subset H_{r-1} \subset G \\
&1 \subset M_1 \subset \cdots \subset M_{l-1} \subset M \subset H_{r-1} \subset G \\
&1 \subset M_1 \subset \cdots \subset M_{l-1} \subset M \subset N_{s-1} \subset G \\
&1 \subset N_1 \subset \cdots \subset N_{s-1} \subset G
\end{aligned}$$

Si probamos que estas series son de composición se concluye, pues cada una tiene con la anterior un término en común normal en G y se acabaría por el apartado anterior. Es decir, basta ver que H_{r-1}/M y N_{s-1}/M son simples. Basta observar que $H_{r-1}/M = H_{r-1}/(H_{r-1} \cap N_{s-1}) \hookrightarrow G/N_{s-1}$, es una inclusión normal (por serlo $H_{r-1} \subset G$) y este último es simple, luego $H_{r-1}/M = G/N_{s-1}$ y, por tanto, el primero es simple. Del mismo modo se prueba que N_{s-1}/M es simple.

□

11. Corolario: *Si $N \subset G$ es un subgrupo normal y G es de longitud finita, entonces:*

$$long(G) = long(N) + long(G/N).$$

12. Ejercicios: 1. Sean p y q son números primos distintos, entonces:

   a) Ningún grupo G de orden pq es simple, y si además $p < q$ y q no es congruente con 1 módulo p, entonces G es cíclico.

   b) Ningún grupo G de orden p^2q es simple.

   c) Ningún grupo G de orden p^3q es simple.

2. Los únicos grupos simples de orden menor que 60 son los de orden primo.

3. Todo grupo de orden menor que 60 es resoluble.

4. Si p y q son números primos distintos, entonces todos los grupos de orden pq, p^2q y p^3q son resolubles.

5. Si un grupo finito G tiene un único p-subgrupo de Sylow para cada número primo p que divide a su orden, entonces G es resoluble.

Resolubilidad de los grupos S_2, S_3 y S_4

13. Teorema: *S_2 es un grupo abeliano simple y A_2 es trivial.*

Demostración. Inmediato, por ser $|S_2| = 2! = 2$. □

14. Teorema: *S_3 es resoluble y admite una única cadena de composición:*

$$\{Id\} \subset A_3 \subset S_3$$

Es decir, A_3 es el único subgrupo normal de S_3 y es simple (abeliano).

Demostración. En efecto, $|A_3| = 3$, luego A_3 es cíclico de orden 3 y la cadena anterior es de composición. Por tanto, S_3 es resoluble. La unicidad de la cadena se obtiene de que los únicos subgrupos de orden 2 son los generados por las transposiciones y, por tanto, ninguno es normal y además los elementos de orden 3 son los 3 ciclos y cada uno de ellos genera A_3. □

15. Notación: Denotaremos $N_r = \{1, 2, \ldots, r\}$.

Sea $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si identificamos como conjuntos $K_4 = N_4$, entonces por el teorema de Cayley se tiene $K_4 \hookrightarrow S_4$, operando K_4 en K_4 por traslación por la izquierda. Se puede observar que K_4 se identifica con el subconjunto de los pares de ciclos disjuntos

$$K_4 = \{Id, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$$

que es un subgrupo (trivialmente normal) de S_4, es decir, el subgrupo resultante es independiente de la identificación de K_4 con N_4.

A este subgrupo $K_4 \subset A_4$ (normal en S_4) es al que denominaremos *grupo de Klein*.

16. Proposición: *Se verifica un isomorfismo canónico $S_4/K_4 \approx S_3$. Además, cada subgrupo $S_3 \subset S_4$ es un suplementario de K_4, es decir, $S_4 \approx K_4 \rtimes S_3$.*

Demostración. En efecto, K_4 es normal, S_3 tiene orden complementario que K_4 en S_4 y $S_3 \cap K_4 = \{Id\}$. □

17. Corolario: *S_4 es un grupo resoluble. Es más, la siguiente cadena es de composición,*

$$\{Id\} \subset \mathbb{Z}/2\mathbb{Z} \subset K_4 \subset A_4 \subset S_4$$

Simplicidad del grupo alternado.

18. Lema: *El grupo alternado, A_n, está generado por los tres ciclos ($n > 2$).*

Demostración. Si $\sigma = (i,j,k) \in S_n$ es un tres ciclo, entonces $\text{sign}(\sigma) = (-1)^2 = 1$ y $\sigma \in A_n$. Por la proposición 0.1.37, toda permutación par es producto de un número par de transposiciones. Tenemos que probar que todo producto de dos transposiciones es producto de tres ciclos. Basta observar que $(1,2)(2,3) = (1,2,3)$ (cuando las transposiciones no sean disjuntas) y $(1,2)(3,4) = (1,2,3)(2,3,4)$ (cuando las transposiciones sean disjuntas). □

19. Teorema: *Si $n \neq 4$, el único subgrupo normal propio de S_n es A_n. Los únicos subgrupos normales propios de S_4 son el alternado A_4 y el grupo de Klein K_4.*

Demostración. Por lo visto anteriormente, el teorema es claro para $n = 2,3$, luego podemos suponer $n \geq 4$.

Sea $H \subset S_n$ un subgrupo normal. Por el teorema 0.1.35, si $\sigma \in H$, entonces todas las permutaciones con la misma forma que σ pertenecen también a H.

Sea $Id \neq \sigma \in H$ y sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_h$ su descomposición en producto de ciclos disjuntos de órdenes respectivos $n_1 \geq \cdots \geq n_h$.

• Si $n_1 \geq 3$, digamos $\sigma_1 = (a_1, a_2, a_3, \ldots, a_{n_1})$, sea $\overline{\sigma}_1 = (a_{n_1}, a_{n_1-1} \ldots, a_3, a_1, a_2)$. Se verifica que $\overline{\sigma} = \overline{\sigma}_1 \circ \sigma_2^{-1} \circ \cdots \circ \sigma_h^{-1} \in H$, pues tiene la misma forma que σ. Luego, $\overline{\sigma} \circ \sigma =$

$(a_1, a_{n_1}, a_2) \in H$ y por el lema 2.8.18, se concluye que H contiene a A_n. Por tanto, $H = A_n$ ó S_n.

• Si $n_1 = 2$ y $h = 1$, entonces σ es una transposición y H las contiene a todas, luego $H = S_n$ (proposición 0.1.37).

• Por último, si $n_1 = 2$ y $h \geq 2$, entonces $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ \sigma_3 \circ \cdots \circ \sigma_h$. Eligiendo la permutación con la misma forma $\overline{\sigma} = (a_1, a_4) \circ (a_2, a_1) \circ \sigma_3^{-1} \circ \cdots \circ \sigma_h^{-1}$, se obtiene que

$$\tau := (a_1, a_4) \circ (a_2, a_3) = \overline{\sigma} \circ \sigma \in H$$

y, por tanto H contiene a todos los pares de trasposiciones disjuntas. Si $n > 4$, sea $\tau' = (a_2, a_3) \circ (a_1, a_5)$, entonces $(a_1, a_5, a_4) = \tau \circ \tau' \in H$. Luego, H contiene a todos los tres ciclos y $A_n \subseteq H$. Entonces, $H = S_n$ ó $H = A_n$. Si $n = 4$, entonces H contiene al grupo de Klein y $H/K_4 \subset S_4/K_4 \approx S_3$ es un subgrupo normal, es decir, es trivial o A_3 y, por tanto, $H = K_4$ o A_4. □

20. Teorema: *A_n es simple para $n \neq 4$.*

Demostración. Sea $H \subset A_n$ normal no trivial. Se verifica que $N_{S_n}(H) = A_n$ (por el teorema anterior). Es decir, que H tiene exactamente dos conjugados (por S_n) uno es H y el otro es $H' = \sigma \circ H \circ \sigma^{-1}$ para cualquier permutación impar σ. En particular, $H \cap H' = \{id\}$ y $H \cdot H' = A_n$, pues ambos son subgrupos normales en S_n, es decir, $A_n \approx H \times H'$. De aquí que H tiene orden par (por tenerlo A_n) y, por tanto, contiene un elemento μ de orden 2 (teorema de Cauchy). De aquí que μ descompone en producto de trasposiciones disjuntas $\mu = \sigma_1 \circ \cdots \circ \sigma_h$. Por tanto, $\mu = \sigma_1 \circ \mu \circ \sigma_1^{-1} \in H'$, es decir, $\mu \in H \cap H' = \{Id\}$ y se obtiene una contradicción.

□

21. Corolario: *La única serie de composición de S_n, para $n > 4$, es*

$$\{Id\} \subset A_n \subset S_n$$

Demostración. $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$ y A_n es simple, luego la serie es de composición. La unicidad es consecuencia de los dos teoremas anteriores. □

22. Ejercicio: Halla resoluciones de los grupos cíclicos $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$ y $\mathbb{Z}/30\mathbb{Z}$; de los grupos abelianos $(\mathbb{Z}/15\mathbb{Z})^*$ y $(\mathbb{Z}/32\mathbb{Z})^*$; de los grupos simétricos S_2, S_3 y S_4; y de los grupos diédricos D_3, D_4 y D_5.

Grupo metacíclico.

Como hemos visto los grupos S_n son resolubles exactamente para $n \leq 4$. El primero no resoluble es para $n = 5$, que es un número primo. Queremos determinar los

subgrupos transitivos resolubles maximales de este grupo, por su interés en la teoría de ecuaciones.

23. Lema : *Si X es una G-órbita de orden primo p y $N \subset G$ un subgrupo normal operando de modo no trivial en X, entonces X es una N-órbita.*

Demostración. Los subgrupos de isotropía G_x de los puntos de $x \in X$ son subgrupos conjugados, $G_{x'} = gG_xg^{-1}$ (por ser X una órbita). Como N es invariante por conjugación, los grupos de isotropía operando N son $N_{x'} = N \cap G_{x'} = N \cap (gG_xg^{-1}) = g(N \cap G_x)g^{-1}$. Es decir, son conjugados en G y, por tanto, del mismo orden. Luego las órbitas en X por N son todas del mismo orden, luego divisor de p y mayor que 1 (porque N opera de modo no trivial). En conclusión X es una órbita operando N. □

24. Proposición: *Sea $\sigma = (1,\dots,n) \in S_n$ un n-ciclo. Se cumple que*

$$N_{S_n}(<\sigma>) \approx \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

Con la identificación obvia $\{1,\dots,n\} = \mathbb{Z}/n\mathbb{Z}$ se cumple que

$$N_{S_n}(<\sigma>) = \{\sigma_{(i,k)} \,:\, (i,k) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*\},$$

siendo $\sigma_{(i,k)}$ la permutación de los elementos de $\mathbb{Z}/n\mathbb{Z}$ definida por $\sigma_{(i,k)}(x) = kx + i$ (obsérvese que $\sigma = \sigma_{(\bar{1},\bar{1})}$).

Demostración. Identifiquemos $\{1,\dots,n\} = \mathbb{Z}/n\mathbb{Z}$. Si $\sigma' \in S_n$ conmuta con σ, entonces $(\bar{1},\dots,\bar{n}) = \sigma'\sigma\sigma'^{-1} = (\sigma'(\bar{1}),\dots,\sigma'(\bar{n}))$. Por tanto, $\sigma'(\overline{i+1}) = \sigma'(\bar{i}) + \bar{1}$. Luego, σ' está determinado por $\sigma'(\bar{1})$ y el subgrupo de S_n de las permutaciones que conmutan con σ, $C_{S_n}(\sigma)$, es de orden menor o igual que n, luego es $\langle\sigma\rangle$. $C_{S_n}(\sigma)$ es igual al núcleo del morfismo natural, $N_{S_n}(\langle\sigma\rangle) \to \mathrm{Aut}_{grp}(\langle\sigma\rangle)$, $\sigma' \mapsto \tau_\sigma$ (donde $\tau_{\sigma'}$ es el morfismo conjugar por σ'). Luego, $|N_{S_n}(\langle\sigma\rangle)|/|C_{S_n}(\sigma)|$ divide a $|\mathrm{Aut}_{grp}(\langle\sigma\rangle)| = |(\mathbb{Z}/n\mathbb{Z})^*|$. Luego, $|N_{S_n}(\langle\sigma\rangle)|$ divide a $|\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*|$. Como $\{\sigma_{(i,k)} \,:\, (i,k) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*\} \subseteq N_{S_n}(\langle\sigma\rangle)$, por órdenes son iguales. □

25. Definición: Se dice que $N_{S_n}(<\sigma>) = \{\sigma_{(i,k)} \,:\, (i,k) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*\}$ es un subgrupo metacíclico de S_n.

26. Teorema : *$G \subseteq S_p$ (p primo) es un subgrupo transitivo y resoluble si y solo si contiene un p-ciclo, σ, y G es un subgrupo intermedio $<\sigma> \subseteq G \subseteq N_{S_p}(<\sigma>)$.*

Demostración. Basta ver el enunciado directo. Como G es resoluble, admite una cadena de subgrupos, cada uno normal en el siguiente y de factores de orden primo: $0 \subset H_1 \subset \cdots \subset H_r = G$. Ahora por el lema anterior H_{r-1} es transitivo, por tanto H_{r-2} lo es, y recurrentemente H_1 es transitivo. Como H_1 es de orden primo y $\{1,\ldots,p\}$ es de orden p, se concluye que H_1 es de orden p y está generado por un p-ciclo, $H_1 =< \sigma_p >$.

Como $|S_p| = p! = p(p-1)\cdots 1$, los subgrupos de orden p son los p-subgrupos de Sylow. Luego esto mismo le pasa a cada subgrupo $G \subset S_p$. Como H_i es normal en H_{i+1} y los p-subgrupos de Sylow de H_{i+1} son conjugados (en H_{i+1}), si H_i contiene a uno de ellos, los contiene a todos. Como este es el caso (pues $H_i \supset H_1$), se obtiene por recurrencia, que H_1 contiene a todos los p-subgrupos de Sylow de G. En particular, estamos diciendo que H_1 es el único p-subgrupo de Sylow en G, luego H_1 es normal en G, es decir, $< \sigma > \subseteq G \subseteq N_{S_p}(< \sigma >)$.

□

2.9. Problemas

1. Sea A una k-álgebra finita reducida. Prueba que todo ideal es idempotente.

2. Sea k-algebraicamente cerrado y A una k-álgebra finita. Prueba que

$$(A \otimes_k A)_{\text{red}} = A_{\text{red}} \otimes_k A_{\text{red}}$$

3. Sea $k \to K$ una extensión finita. Prueba que $K \otimes_k K$ es cuerpo si y solo si $K = k$.

4. Sea A una k-álgebra finita e I un ideal. Prueba:

   a) Si A es local, A/I es un A-módulo plano $\Leftrightarrow I = 0$.

   b) Si A es cualquiera, A/I es un A-módulo plano $\Leftrightarrow I = I^2$.

5. Prueba que la localización de una k-álgebra finita es una k-álgebra finita.

6. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcula $\text{Hom}_{k-\text{alg.}}(A,K)$.

7. Sea $k \to K$ una extensión trivializante de la k-álgebra finita A. Prueba que el polinomio característico de todo elemento de A (considerando como homotecia de A) tiene sus raíces en K.

8. Sea $A = \mathbb{R}[x,y](y^2 - x^3 + 1)$. Para cada $\lambda \in \mathbb{R}$ se considera $A_\lambda = A/(x - \lambda)$. Calcula

$$\text{Spec} A_\lambda,\ \text{Hom}_{\mathbb{R}-\text{alg.}}(A_\lambda, \mathbb{R}),\ \text{Hom}_{\mathbb{R}-\text{alg.}}(A_\lambda, \mathbb{C}).$$

9. Sea ω una raíz primitiva cúbica de la unidad. Halla los siguientes grupos:

$$\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\omega), \quad \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[4]{2}), \quad \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(i, \sqrt[2]{2}), \quad \mathrm{Aut}_{\mathbb{Q}(\omega)}\,\mathbb{Q}(\omega, \sqrt[3]{2}).$$

10. Sea $A = k[x]/(p(x))$. Prueba que A es puramente inseparable si y solo si $\mathrm{car}\, k = p > 0$ y $p(x) = x^{p^n} - a$.

11. Sea A una k-álgebra finita. Se llama grado de separabilidad de A a $[A:k]_s = \dim_k \pi_0^k(A)$. Sea K una extensión finita de cuerpos de k y B una K-álgebra finita. Prueba:

    a) $[A_K : K]_s = [A:k]_s$.

    b) $[A:k]_s =$ orden de $\mathrm{Hom}_{k-alg}(A, \overline{k})$, con $\overline{k} =$ cierre algebraico de k.

    c) $[B:K]_s \cdot [K:k]_s = [B:k]_s$.

    d) $\dim_k K = p^n \cdot [K:k]_s$.

12. Una extensión finita de cuerpos $k \hookrightarrow K$ se dice simple cuando $K = k(\alpha)$. Prueba que una extensión finita de cuerpos $k \hookrightarrow K$ es simple $\Leftrightarrow$ solo hay un número finito de cuerpos F tales que $k \subset F \subset K$.

13. Sea k un cuerpo de característica p y sean t, u algebraicamente independientes sobre k. Prueba:

    a) $k(t,u)$ es de grado p^2 sobre $k(t^p, u^p)$.

    b) $k(t,u)$ no es simple sobre $k(t^p, u^p)$.

14. Sea $k \to K = k(u,v)$ una extensión finita y sea u separable. Prueba que K es una extensión simple de k.

15. Sea K una extensión finita de k, $K_0 = \pi_0^k(K)$ y F un cuerpo intermedio entre k y K. Prueba:

    a) K es puramente inseparable sobre $F \Leftrightarrow K_0 \subseteq F$.

    b) Si K es separable sobre F, entonces F contiene la máxima subextensión puramente inseparable de K.

16. Si u es separable sobre k y v es puramente inseparable sobre k, prueba que $k(u,v) = k(u \cdot v) = k(u+v)$.

17. Sea A una k-álgebra finita, siendo k un cuerpo de característica cero. Prueba que $A = \pi_0^k(A) \oplus \mathrm{Rad}$ (traza). ¿Es cierto este resultado si car $k \neq 0$?

18. Sea K una extensión finita de k tal que $K \otimes_k K$ es racional sobre K. Prueba que $\pi_0^k(K)$ se trivializa a sí mismo.

19. Sea $k \to K$ una extensión finita de cuerpos. Prueba que k es perfecto $\Leftrightarrow$ K es perfecto.

20. Determina el grupo de Galois de $x^4 - 3x^2 + 4$ sobre $\mathbb{Q}$ y el de $x^3 - 10$ sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$.

21. Determina el grupo de Galois de $x^4 + ax^3 + bx^2 + ax + 1$ sobre $\mathbb{Q}(a,b)$.

22. Sea $p(x)$ un polinomio de grado n, separable sobre k. Prueba que su cuerpo de descomposición es una extensión de k de grado menor o igual a $n!$.

23. Sea $\overline{k}$ un cierre algebraico de k, y σ un automorfismo de $\overline{k}$ sobre k. Si K es el cuerpo fijo de σ, prueba que toda extensión finita de K es cíclica.

24. Si $k \hookrightarrow K$ es una extensión de Galois de grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, y car $k \neq 2$, entonces $K = k(\alpha, \beta)$, con $\alpha^2, \beta^2 \in k$.

25. Se dice que dos extensiones K y F de k son linealmente disjuntas sobre k cuando $K \otimes_k F$ es cuerpo. Prueba que si K y F son de Galois y linealmente disjuntos, entonces
$$G(K \cdot F/k) = G(K/k) \times G(F/k)$$
Como aplicación, determínese el grupo de Galois de $\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2}, \omega)$ sobre $\mathbb{Q}$, siendo ω una raíz primitiva tercera de la unidad.

26. Sea $k \to K$ una extensión de Galois y $k \to L$ una extensión. Prueba que $K \otimes_k L$ es un producto de cuerpos todos isomorfos.
Si $f(x) \in k[x]$ es irreducible y $g(x)$, $h(x)$ son factores irreducibles mónicos de $f(x)$ en $K[x]$, prueba que existe un automorfismo σ de K sobre k tal que $\sigma(g) = h$.

27. Prueba que todo compuesto de dos extensiones de Galois es una extensión de Galois.

28. Prueba que todo grupo finito es el grupo de Galois de alguna extensión de cuerpos.

29. Sea k un cuerpo finito con q elementos. Si $f(x) \in k[x]$ es irreducible, demuestra que $f(x)$ divide a $x^{q^n} - x$ si y solo si el grado de $f(x)$ divide a n.

30. Sean p, q primos diferentes. Prueba que $\frac{x^p-1}{x-1}$ es irreducible sobre $\mathbb{F}_q \Leftrightarrow q^d - 1$ no es divisible por p, para $d < p - 1$.

31. Prueba que en un cuerpo finito todo elemento es suma de dos cuadrados.

32. Sea $p(x)$ un polinomio irreducible y separable de grado 3 sobre k. Prueba que su grupo de Galois es A_3 si y solo si su discriminante es un cuadrado en k (car $k \neq 2$).

33. Grupo de las bicuadradas. Sea $p(x) = x^4 + ax^2 + b$ irreducible y separable sobre un cuerpo k (car $k \neq 2$) y G su grupo de Galois. Prueba:

    a) Si b es un cuadrado en k, entonces $G = K_4$.

    b) Si b no es un cuadrado en k pero $b(a^2 - 4b)$ sí lo es, entonces $G = \mathbb{Z}/4\mathbb{Z}$.

    c) Si ni b ni $b(a^2 - 4b)$ son cuadrados en k, entonces $G = D_4$.

34. Grupo de las recíprocas. Sea $p(x) = x^4 + ax^3 + bx^2 + ax + 1$ irreducible y separable sobre k (car $k \neq 2$) y G su grupo de Galois. Prueba:

    a) Si $b^2 + 4b + 4 - 4a^2$ es un cuadrado en k, entonces $G = K_4$.

    b) Si $b^2 + 4b + 4 - 4a^2$ no es un cuadrado, pero $(b^2 + 4b + 4 - 4a^2)(a^2 - 4b + 8)$ sí lo es, entonces $G = \mathbb{Z}/4\mathbb{Z}$.

    c) Si ninguno de los dos es un cuadrado, entonces $G = D_4$.

35. Si n, m son primos entre sí, prueba:

$$\mathbb{Q}(\epsilon_n) \cap \mathbb{Q}(\epsilon_m) = \mathbb{Q}, \quad \mathbb{Q}(\epsilon_n, \epsilon_m) = \mathbb{Q}(\epsilon_n \cdot \epsilon_m) = \mathbb{Q}(\epsilon_{n \cdot m}).$$

36. Pruébese que toda quíntica, en característica cero, puede transformarse en una del tipo $x^5 + px + q$ mediante una transformación que utiliza, eventualmente, raíces cuadradas y cúbicas.

37. Si el polinomio $x^5 + px + q$ es irreducible sobre k, probar que entonces es resoluble por radicales si y solo si $(Y^3 - 5pY^2 + 15p^2Y + 5p^3)^2 - \Delta Y$ tiene una raíz en k, siendo $\Delta = 2^8 p^5 + 5^5 q^4$ el discriminante de la quíntica.

38. (Extensiones abelianas). Sea $k \to K$ una extensión abeliana finita de grupo G y exponente (=anulador de G) n (n primo con car k). Si k contiene las raíces n-ésimas de la unidad μ_n, y A es el subgrupo de los elementos de k^* cuya raíz n-ésima pertenece a K, entonces:

$$G \simeq \mathrm{Hom}(A/k^{*n}, \mu_n)$$

    Prueba que hay una correspondencia biunívoca entre las extensiones abelianas de exponente n y los subgrupos de k^*/k^{*n}. Las extensiones cíclicas se corresponden con los subgrupos cíclicos.

39. Si k contiene las raíces n-ésimas de la unidad y n es primo con car k, prueba:

$$k(\sqrt[n]{a}) = k(\sqrt[n]{b}) \Leftrightarrow a = \lambda^n \cdot b^m, \quad \text{con } (n,m) = 1 \text{ y } \lambda \in k.$$

40. Sea $k \to K$ una extensión, posiblemente infinita, tal que $K = \varinjlim K_i$. Si cada K_i es una extensión de Galois de grupo G_i, prueba que el grupo de automorfismos de K es $G = \varprojlim G_i$. Determina el grupo de automorfismos del cierre algebraico de un cuerpo finito.

Parte II

Álgebra Conmutativa II

Capítulo 3

Variedades algebraicas

3.1. Introducción

Una definición de Matemáticas podría ser: "La Matemática estudia el concepto de espacio, es Geometría". Desde este punto de vista, la Topología es el estudio de los espacios topológicos, de las variedades topológicas, la Geometría Diferencial es el estudio de las variedades diferenciales, la asignatura de Variable Compleja el estudio de las variedades analíticas y el Álgebra el estudio de las variedades algebraicas. El análisis del espacio se funda en las funciones del espacio considerado. Así el fundamento de la Topología es el anillo de funciones continuas, de la Geometría Diferencial el anillo de las funciones infinito diferenciables, el de la Variable Compleja el anillo de funciones analíticas o conformes y el del Álgebra el anillo de funciones algebraicas.

Una definición del Álgebra podría ser: "El estudio de los espacios definidos por sistemas de ecuaciones algebraicas". Así el primer problema que nos planteamos es: ¿qué es un sistema de ecuaciones algebraicas? Podríamos responder que es dar r polinomios $p_1(x_1,\dots,x_n),\cdots,p_r(x_1,\dots,x_n)\in\mathbb{C}[x_1,\dots,x_n]$ y escribimos el sistema

$$\begin{aligned} &p_1(x_1,\dots,x_n)=0\\ &\cdots\\ &p_r(x_1,\dots,x_n)=0 \end{aligned}$$

De modo inconsciente identificamos el sistema de ecuaciones algebraicas con el conjunto de soluciones del sistema de ecuaciones algebraicas, con "la variedad de soluciones". Por ello decimos que si al sistema de ecuaciones algebraicas anterior añadimos la ecuación $a_1\cdot p_1(x_1,\dots,x_n)+\cdots+a_r p_r(x_1,\dots,x_n)=0$ obtenemos el mismo sistema de ecuaciones algebraicas. En definitiva una definición mejor adaptada a nuestros propósitos inconscientes debería ser: "Un sistema de ecuaciones algebraicas es un ideal $(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))\subseteq\mathbb{C}[x_1,\dots,x_n]$"

Surgen, ahora, varias preguntas: ¿Todo ideal de $\mathbb{C}[x_1,\ldots,x_n]$ está generado por un número finito de elementos? ¿Están los ideales de $\mathbb{C}[x_1,\ldots,x_n]$ determinados por su variedades de soluciones?

La respuesta a la primera pregunta es afirmativa. Los anillos cuyos ideales son finito generados se denominan anillos noetherianos y, como sabemos por el teorema de la base de Hilbert, los anillos de polinomios son anillos noetherianos.

La respuesta a la segunda pregunta es: "no, pero casi sí". Observemos que las soluciones (sobre $\mathbb{C}$) del sistema $x_1 = 0$ son las mismas que $x_1^2 = 0$. Obviamente, dado un ideal $I \subseteq \mathbb{C}[x_1,\ldots,x_n]$ si consideramos el ideal $r(I) := \{q \in \mathbb{C}[x_1,\ldots,x_n]$, tales que $q^m \in I$, para algún $m\}$, entonces la variedad de soluciones de I es la misma que la de $r(I)$. El teorema de los ceros de Hilbert afirma que I e I' tienen la misma variedad de soluciones si y solo si $r(I) = r(I')$, es decir, salvo "nilpotencias" los ideales están determinados por sus variedades de soluciones.

Llamemos variedad algebraica a la variedad de soluciones de un ideal. Un primer resultado inmediato de la teoría de variedades algebraicas es que una variedad V es irreducible, es decir, no es unión propia de dos variedades algebraicas, si y solo si el ideal de todas las funciones que se anulan en V es un ideal primo. En general, toda variedad algebraica V es unión de un número finito de variedades algebraicas irreducibles. En términos de ideales: todo ideal radical es intersección de un número finito de ideales primos.

Puede parecernos que dado un ideal I es siempre mejor considerar $r(I)$ en vez de I. Pongamos un ejemplo sencillo en el que nos interese el ideal I: Consideremos el ideal $(x, y^2 - x)$ o el sistema

$$\begin{aligned} x &= 0 \\ y^2 - x &= 0 \end{aligned}$$

la variedad de soluciones de este sistema es el punto $x = 0, y = 0$. Tenemos que $I = (x, y^2 - x) = (x, y^2)$ y $r(I) = (x, y)$. Podemos pensar la variedad de soluciones dada, como el conjunto de puntos de corte de la recta $x = 0$ con la parábola $y^2 - x = 0$, y como esta recta es tangente a la parábola nos gustaría afirmar que la variedad de soluciones es "el origen contado dos veces". De esta afirmación "queda rastro" en el ideal I pero no en $r(I)$. En conclusión, cuando estudiamos el sistema de ecuaciones definido por I, si consideramos solo el conjunto de soluciones del sistema de ecuaciones (o equivalentemente, consideramos solo $r(I)$) perdemos información que puede ser esencial, sobre todo en una teoría fina de intersección de variedades.

El ideal $(x, y^2 - x)$ es el ideal de polinomios $p(x, y)$ tales que $p(0,0) = 0$ y $\frac{\partial p}{\partial y}(0,0) = 0$, que hemos expresado de modo más impreciso como ideal de funciones que se anulan dos veces en el origen. En general, demostraremos que los ideales I son los ideales de polinomios que se anulan en ciertas variedades irreducibles y cumplen ciertas condiciones infinitesimales (no preciso este concepto) a lo largo de estas variedades irredu-

cibles. Si llamamos ideal primario al ideal de funciones que se anula en una variedad irreducible y cumple ciertas condiciones infinitesimales a lo largo de ella, el resultado fundamental de la teoría de descomposiciones primarias afirma que todo ideal es intersección de un número finito de ideales primarios. En conclusión, dar un sistema de ecuaciones algebraicas equivale a dar un número finito de variedades algebraicas irreducibles y condiciones infinitesimales a lo largo de ellas. Euclides se habría sorprendido si hubiese sabido que su Teorema de Euclides era la punta del iceberg de un teorema geométrico.

Una vez que hemos profundizado en el concepto de variedad algebraica nos preguntamos: ¿cuántas variedades algebraicas hay?, ¿cómo distinguir dos variedades algebraicas? Nos planteamos la clasificación de las variedades algebraicas.

Un invariante obvio de las variedades algebraicas es la dimensión. Se dice que una variedad algebraica es de dimensión n si existe una cadena (de inclusiones estrictas) de subvariedades irreducibles $\emptyset = C_0 \subset C_1 \subset \cdots \subset C_n$ de longitud n y no existe ninguna otra de longitud mayor. Probaremos que la dimensión de una variedad algebraica es m si existe una proyección de fibras finitas y no vacías de la variedad en un espacio afín $\mathbb{A}^m(\mathbb{C})$. Veremos que el concepto de dimensión en variedades algebraicas irreducibles es local, y aún más, que todas las cadenas irrefinables de subvariedades irreducibles tienen la misma longitud. Por último, veremos que las hipersuperficies $f = 0$ de una variedad algebraica irreducible de dimensión m son de dimensión $m-1$ y que todo punto de la variedad es (localmente) la solución de un sistema de m ecuaciones algebraicas y no menos. Todos estos resultados serán expresados en términos de los anillos de funciones algebraicas de la variedad y sus ideales primos.

Puede decirse que la Geometría Algebraica Local se mueve dentro del marco afín y que la Geometría Algebraica Global dentro del marco proyectivo. Por ejemplo, el Teorema de Bézout que afirma que dos curvas planas proyectivas de grados n y m se cortan en $n \cdot m$ puntos (contando multiplicidades), es obviamente un enunciado no local y pertenece a la Geometría Algebraica Proyectiva. En este capítulo, definiremos las variedades proyectivas, veremos que todos los conceptos afines (esencialmente locales), como descomposición en componentes irreducibles, dimensión, etc, se extienden a las variedades proyectivas.

El teorema central, que usaremos para la demostración del teorema de los ceros de Hilbert y el desarrollo de la teoría de la dimensión, será el lema de normalización de Noether.

3.2. Descomposición primaria

Queremos demostrar que todo ideal de un anillo noetheriano viene definido por condiciones infinitesimales en un número finito de puntos del espectro. Desde el punto de vista aritmético, esto puede entenderse como el teorema de Euclides para anillos noetherianos. Comencemos con los ideales primarios que serán los definidos por condiciones infinitesimales en un punto.

1. Definición: Sea A un anillo. Un ideal $\mathfrak{q} \subsetneq A$ es *primario* si todo divisor de cero de $A/\mathfrak{q}$ es nilpotente; es decir:

$$ab \in \mathfrak{q},\ a \notin \mathfrak{q} \ \Rightarrow\ b^n \in \mathfrak{q} \text{ para algún } n \geq 1.$$

2. Ejemplos: 1. Los ideales primos son primarios.

2. Si $p \in \mathbb{Z}$ es un número primo entonces (p^n) es un ideal primario de $\mathbb{Z}$. Igualmente si $p(x) \in k[x]$ es un polinomio irreducible entonces $(p(x)^n)$ es un ideal primario de $k[x]$

3. Proposición: *El radical de un ideal primario es un ideal primo.*

Demostración. En efecto, sea $\mathfrak{p}$ el radical de un ideal primario $\mathfrak{q}$. Si $ab \in \mathfrak{p}$ y $a \notin \mathfrak{p}$, entonces $(ab)^n \in \mathfrak{q}$ para algún $n \geq 1$ y $a^r \notin \mathfrak{q}$ para ningún r. Como $\mathfrak{q}$ es primario, alguna potencia de b^n ha de estar en $\mathfrak{q}$, luego $b \in \mathfrak{p}$. □

4. Definición: Sea $\mathfrak{q}$ un ideal primario y $\mathfrak{p} = r(\mathfrak{q})$ el radical de $\mathfrak{q}$. Diremos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario ó que $\mathfrak{p}$ es el *ideal primo asociado* a $\mathfrak{q}$.

En tal caso, si $A' \to A$ es un morfismo de anillos, es sencillo comprobar que $A' \cap \mathfrak{q}$ es un ideal $(A' \cap \mathfrak{p})$-primario de A'.

5. Proposición: *Sea $\mathfrak{m} \subset A$ un ideal maximal. Entonces, un ideal $I \subset A$ es $\mathfrak{m}$-primario si y solo si $r(I) = \mathfrak{m}$.*

En particular, todas las potencias $\mathfrak{m}^n$, con $n > 0$, son ideales $\mathfrak{m}$-primarios.

Demostración. Si I es un ideal de radical $\mathfrak{m}$, entonces $\mathfrak{m}$ es el único ideal primo que contiene a I. Por tanto, A/I tiene un único ideal primo, luego todo elemento de A/I es invertible o nilpotente; en particular, todo divisor de cero es nilpotente. □

Si el anillo A es noetheriano, cada ideal contiene una potencia de su radical, así que todo ideal $\mathfrak{m}$-primario es de la forma $\pi^{-1}(\bar{\mathfrak{q}})$ para algún ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}^r$ (donde $\pi\colon A \to A/\mathfrak{m}^r$ es el morfismo de paso al cociente). En el caso del anillo $A = \mathbb{C}[x_1, \ldots, x_n]$,

si consideramos el ideal maximal $\mathfrak{m}_\alpha = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ y escribimos $t_i = x_i - \alpha_i$, entonces $\mathfrak{m}_\alpha = (t_1, \ldots, t_n)$,

$$A/\mathfrak{m}_\alpha^r = \mathbb{C}[t_1, \ldots, t_n]/(t_1, \ldots, t_n)^r = \begin{bmatrix} \text{Polinomios de grado} \\ < r \text{ en } t_1, \ldots, t_n \end{bmatrix}$$

y la reducción módulo $\mathfrak{m}_\alpha^r$ de cualquier polinomio coincide con el clásico desarrollo de Taylor hasta el orden $r-1$ en el punto $(\alpha_1, \ldots, \alpha_n)$. Por tanto, el ideal $\mathfrak{m}_\alpha$-primario $\mathfrak{q}$ está formado por todas las funciones $f \in A$ cuyo desarrollo de Taylor $\bar{f} \in A/\mathfrak{m}_\alpha^r$ hasta el orden $r-1$ en el punto α, pertenece al subespacio vectorial $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}_\alpha^r$.

Una base del $\mathbb{C}$-espacio vectorial dual de $A/\mathfrak{m}^r$, la constituyen las formas lineales

$$\omega_\beta = \left(\frac{\partial^{|\beta|}}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_n} x_n}\right)_{|\alpha}$$

con $\beta = (\beta_1, \ldots, \beta_n)$ y $|\beta| = \beta_1 + \cdots + \beta_n < r$, definidas por $\omega_\beta(\bar{f}) = \frac{\partial^{|\beta|} f}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_n} x_n}(\alpha_1, \ldots, \alpha_n)$. Por tanto, todo ideal de $A/\mathfrak{m}_\alpha^r$ está definido por un sistema de s-ecuaciones

$$\sum_{|\beta|<r} \lambda_{i,\beta} \omega_\beta(\bar{f}) = 0, \quad 1 \le i \le s.$$

Añadamos la ecuación redundante $f(\alpha_1, \ldots, \alpha_n) = 0$. Los ideales $\mathfrak{m}$-primarios son ideales generados por las funciones f que verifican un sistema de s-ecuaciones

$$\begin{aligned} &\sum_{0<|\beta|<r} \lambda_{i,\beta} \frac{\partial^{|\beta|} f}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_n} x_n}(\alpha_1, \ldots, \alpha_n) = 0, \quad 1 \le i \le s \\ &f(\alpha_1, \ldots, \alpha_n) = 0 \end{aligned}$$

(variando $r, s, \lambda_{i,\beta}$ se obtienen todos los ideales $\mathfrak{m}_\alpha$-primarios).

Por tanto, cada ideal $\mathfrak{m}$-primario viene definido por ciertas relaciones entre las derivadas parciales iteradas en el punto $(\alpha_1, \ldots, \alpha_n)$.

Por ello, en general, diremos: "Los ideales primarios de radical maximal $\mathfrak{m}_x$ son los ideales definidos por condiciones infinitesimales en el punto cerrado x".

6. Ejemplo: El ideal primario $(x^2, y) \subset \mathbb{C}[x, y]$ es igual al ideal

$$I = \{f \in \mathbb{C}[x, y] \colon f(0,0) = 0, \frac{\partial f}{\partial x}(0,0) = 0\}.$$

7. Proposición: *Sea S un sistema multiplicativo de un anillo A y sea $\mathfrak{q}$ un ideal $\mathfrak{p}_x$-primario.*

1. *Si* $\mathfrak{p}_x$ *corta a* S*, entonces* $\mathfrak{q}A_S = A_S$.

2. *Si* $\mathfrak{p}_x$ *no corta a* S*, entonces* $\mathfrak{q}A_S$ *es un ideal* $\mathfrak{p}_xA_S$*-primario y* $\mathfrak{q} = A \cap (\mathfrak{q}A_S)$ *. En particular:*

$$\mathfrak{q} = A \cap (\mathfrak{q}A_x).$$

Por tanto, dos ideales $\mathfrak{p}_x$*-primarios coinciden si coinciden al localizar en* x*.*

Demostración. 1. Si $s \in S \cap \mathfrak{p}_x$, entonces $\mathfrak{q}$ contiene alguna s^n, que es invertible en A_S; luego $\mathfrak{q}A_S = A_S$.

2. Si $S \cap \mathfrak{p}_x = \emptyset$, entonces $\mathfrak{p}_xA_S$ es un ideal primo de A_S y es fácil comprobar que $\mathfrak{q}A_S$ es un ideal $\mathfrak{p}_xA_S$-primario. Por último, veamos que $\mathfrak{q} = A \cap (\mathfrak{q}A_S)$. Si $f \in A \cap (\mathfrak{q}A_S)$, entonces $sf \in \mathfrak{q}$ para algún $s \in S$. Ninguna potencia de s está en $\mathfrak{q}$, luego $f \in \mathfrak{q}$. Por tanto, $A \cap (\mathfrak{q}A_S) \subseteq \mathfrak{q}$. La inclusión contraria es evidente. □

8. Ejercicio: Prueba la igualdad

$$\{\text{Ideales primarios de } A_S\} = \{\text{Ideales primarios } \mathfrak{q} \subset A \text{ tales que } \mathfrak{q} \cap S = \emptyset\}.$$

Sea $\mathfrak{p}_x \subset A$ un ideal primo, que también denotamos $x \in \operatorname{Spec} A$. Denotemos $\mathfrak{m} = \mathfrak{p}_xA_x$. Los ideales de A_x de radical $\mathfrak{m}$ son precisamente los ideales $\mathfrak{m}$-primarios, porque $\mathfrak{m}$ es maximal. Por tanto, si $\mathfrak{q}$ es un ideal $\mathfrak{p}_x$-primario, el radical de $\mathfrak{q} \cdot A_x$ es $\mathfrak{m}$ y, si A es noetheriano, existe un r tal que $\mathfrak{m}^r \subseteq \mathfrak{q} \cdot A_x$, luego existe un ideal $\bar{\mathfrak{q}}$ de $A_x/\mathfrak{p}_x^r A_x$ tal que

$$\mathfrak{q} = \pi^{-1}(\bar{\mathfrak{q}})$$

siendo $\pi\colon A \to A_x/\mathfrak{p}_x^r A_x$ el morfismo natural. Recíprocamente, si $\mathfrak{q} = \pi^{-1}(\bar{\mathfrak{q}})$, entonces $\mathfrak{q}$ es un ideal $\mathfrak{p}_x$-primario. Por tanto, "los ideales $\mathfrak{p}_x$-primarios deberían llamarse ideales determinados por condiciones infinitesimales a lo largo de x".

9. Ejemplos: Si un ideal primo $\mathfrak{p}$ no es maximal, pueden existir ideales de radical $\mathfrak{p}$ que no son primarios. Fijemos en un plano afín un punto racional p y una recta r que pase por él. Sea $\mathfrak{m}_p$ el ideal de funciones del plano que se anulen en p y $\mathfrak{p}_r$ el ideal de funciones del plano que se anulen en r. Consideremos ahora el ideal $I = {\mathfrak{m}_p}^2 \cap \mathfrak{p}_r$, que son los polinomios que se anulan en la recta r y sus derivadas parciales se anulan en el punto fijado p. El radical de I es

$$r(I) = r({\mathfrak{m}_p}^2) \cap r(\mathfrak{p}_r) = \mathfrak{m}_p \cap \mathfrak{p}_r = \mathfrak{p}_r$$

pero el ideal I no es primario: si fuese primario sería $\mathfrak{p}_r$-primario. Al localizarlo en r, coincide con la localización de $\mathfrak{p}_r$ en r, por tanto I coincidiría con $\mathfrak{p}_r$, lo cual es falso.

Puede incluso darse el caso de que una potencia de un ideal primo no sea un ideal primario. Por ejemplo, sea $A = k[x,y,z]/(x^2+y^2-z^2)$ el anillo de las funciones algebraicas de un cono de $\mathbb{A}^3$ y sea $\mathfrak{p}_{gt} = (x, y-z)$ el ideal primo de A definido por una generatriz. El ideal ${\mathfrak{p}_{gt}}^2$ no viene definido por condiciones infinitesimales en el punto genérico de tal generatriz; es decir, ${\mathfrak{p}_{gt}}^2$ no coincide con $A \cap {\mathfrak{p}_{gt}}^2 A_{gt}$ sino que involucra además condiciones en el vértice del cono, pues las funciones de ${\mathfrak{p}_{gt}}^2$ deben cumplir además la condición de estar en $\mathfrak{m}^2$, donde $\mathfrak{m} = (x,y,z)$ denota el ideal maximal del vértice del cono. En efecto, $y-z \in A \cap {\mathfrak{p}_{gt}}^2 A_{gt}$ (porque $(y-z)\cdot(y+z) \in {\mathfrak{p}_{gt}}^2 A_{gt}$) pero $y-z \notin {\mathfrak{p}_{gt}}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal ${\mathfrak{p}_{gt}}^2$ no es primario.

10. Definición: Diremos que un ideal $\mathfrak{q}$ de un anillo A es *irreducible* si no es intersección de dos ideales estrictamente mayores; equivalentemente, si el ideal 0 de $A/\mathfrak{q}$ no es intersección de dos ideales no nulos.

11. Lema fundamental: *Sea A un anillo noetheriano. Todo ideal irreducible $\mathfrak{q} \neq A$ es primario.*

Demostración. Sea $\mathfrak{q}$ irreducible y sea $b \in A/\mathfrak{q}$ un divisor de cero. Sea $b\colon A/\mathfrak{q} \to A/\mathfrak{q}$ la homotecia de razón b. Se tiene que

$$0 \neq \operatorname{Ker} b \subseteq \operatorname{Ker} b^2 \subseteq \cdots \subseteq \operatorname{Ker} b^n \subseteq \cdots$$

Como $A/\mathfrak{q}$ es un anillo noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún n. Por lo tanto, $(\operatorname{Ker} b) \cap (\operatorname{Im} b^n) = 0$. Como $\mathfrak{q}$ es irreducible, debe ser $\operatorname{Ker} b = 0$ ó $\operatorname{Im} b^n = 0$. Por hipótesis $\operatorname{Ker} b \neq 0$, luego $\operatorname{Im} b^n = 0$ y por tanto b es nilpotente. En conclusión, los divisores de cero de $A/\mathfrak{q}$ son nilpotentes y $\mathfrak{q}$ es primario. □

12. Teorema de existencia: *Sea A un anillo noetheriano. Todo ideal $I \subsetneq A$ es intersección finita de ideales irreducibles de A. Por tanto, todo ideal $I \subsetneq A$ es intersección finita de ideales primarios de A.*

Demostración. Basta ver que si I no es irreducible entonces $I = I_1 \cap I'$ con I_1 irreducible e $I \subsetneq I'$ (pues con I' se repite el argumento y así sucesivamente y se concluye por noetherianidad). Si I no es irreducible, entonces es intersección de ideales estrictamente mayores: $I = I_1 \cap J_1$. Si I_1 es irreducible hemos terminado; si no, $I_1 = I_{11} \cap I_{12}$, luego $I = I_{11} \cap I_{12} \cap J_1$. Si la inclusión $I \subset I_{12} \cap J_1$ es estricta, tomamos $I_2 = I_{11}, J_2 = I_{12} \cap J_1$; si no, tomamos $I_2 = I_{12}$, $J_2 = J_1$. En ambos casos obtenemos de nuevo que $I = I_2 \cap J_2$, con $I \subsetneq J_2$, además $I_1 \subsetneq I_2$. Así sucesivamente, el proceso es finito por noetherianidad, luego para cierto n, $I = I_n \cap J_n$ con I_n irreducible e $I \subsetneq J_n$ por construcción. □

13. Definición: Sea I un ideal de un anillo A. Diremos que una descomposición $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ como intersección de ideales primarios de A es una *descomposición primaria reducida* de I cuando no tenga componentes redundantes (i.e., no puede eliminarse ninguno de los $\mathfrak{q}_i$ en la igualdad) ni componentes asociadas a un mismo ideal primo ($r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ cuando $i \neq j$).

14. Proposición: *Si $\mathfrak{q}$ y $\mathfrak{q}'$ son dos ideales $\mathfrak{p}_x$-primarios entonces $\mathfrak{q} \cap \mathfrak{q}'$ es $\mathfrak{p}_x$-primario.*

Demostración. Al lector. □

Si un ideal de un anillo puede descomponerse como intersección finita de ideales primarios, agrupando los términos de igual radical obtenemos una descomposición primaria en que todos los términos tienen radicales diferentes. Eliminando entonces términos redundantes, si los hubiera, se obtiene una descomposición primaria reducida. En conclusión, *si un ideal admite una descomposición primaria, entonces admite una descomposición primaria reducida.*

15. Teorema de unicidad de las componentes no sumergidas: *Sea I un ideal de un anillo A y sea $\mathfrak{p}_x$ el ideal primo de las funciones que se anulan en una componente irreducible de $(I)_0$. Si $I = \bigcap\limits_i \mathfrak{q}_i$ es una descomposición primaria reducida, entonces $\mathfrak{p}_x$ es el radical de una componente $\mathfrak{q}_i$ y*

$$\mathfrak{q}_i = A \cap (IA_x)$$

Por tanto, las componentes $\mathfrak{q}_i$ cuyos radicales son mínimos (entre los primos que contienen a I), son únicas.

Demostración. $(I)_0 = \cup_i (\mathfrak{q}_i)_0$ y alguna de las componentes irreducibles de $(I)_0$ es $(\mathfrak{q}_i)_0$, luego $\mathfrak{p}_x = r(\mathfrak{q}_i)$ (y $\mathfrak{p}_x \not\supset \mathfrak{q}_j$, para $j \neq i$). Ahora, si $j \neq i$, entonces $\mathfrak{q}_j A_x = A_x$, porque $r(\mathfrak{q}_j)$ corta al sistema multiplicativo $A \setminus \mathfrak{p}_x$. Por tanto,

$$IA_x = \bigcap_{j=1}^{n} \mathfrak{q}_j A_x = \mathfrak{q}_i A_x$$

y, por 3.2.7, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_x) = A \cap (IA_x)$. □

16. Definición: Si $I = \cap_i \mathfrak{q}_i$ es una descomposición primaria reducida, las componentes $\mathfrak{q}_i$ cuyos radicales son mínimos se denominan componentes *no sumergidas*. Una componente $\mathfrak{q}_j$ está *sumergida* cuando sus ceros están contenidos estrictamente en los ceros de alguna otra componente: $(\mathfrak{q}_j)_0 \subset (\mathfrak{q}_i)_0$.

Las componentes no sumergidas corresponden a los puntos genéricos de las componentes irreducibles de $(I)_0$.

17. Corolario: *Si los ceros de un ideal I de un anillo noetheriano son puntos aislados, la descomposición primaria reducida de I es única salvo el orden.*

Las componentes sumergidas no son únicas pero sí lo son sus radicales, como vamos a demostrar.

Sea $a \in A$ e $I \subset A$ un ideal. Denotaremos

$$(I : a) = \{b \in A : a \cdot b \in I\}.$$

18. Proposición: *Sea $\mathfrak{q} \subset A$ un ideal $\mathfrak{p}$-primario. Se verifica*

$$(\mathfrak{q} : a) = \begin{cases} A & \text{si } a \in \mathfrak{q}. \\ \mathfrak{q}' & \text{si } a \notin \mathfrak{q}, \text{ siendo } \mathfrak{q}' \text{ un ideal } \mathfrak{p}\text{-primario que contiene a } \mathfrak{q}. \end{cases}$$

Demostración. Es una sencilla comprobación. □

19. Teorema: *Sea A un anillo noetheriano. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida de I. Un ideal primo $\mathfrak{p} \subset A$ es un ideal primo asociado a un primario de la descomposición primaria de I si y solo si existe $a \in A$ de modo que $(I : a) = \mathfrak{p}$.*

En particular, los primos asociados a una descomposición primaria reducida de un ideal son independientes de la descomposición.

Demostración. Observemos que $(I : a) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : a) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a)$. Denotemos $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Si $(I : a) = \mathfrak{p}$, tomando radicales tenemos que $\mathfrak{p}$ es intersección de unos cuantos $\mathfrak{p}_i$, por la proposición anterior. Luego, $\mathfrak{p}$ ha de coincidir con alguno de los $\mathfrak{p}_i$ (observemos que el cerrado irreducible $(\mathfrak{p})_0$ es unión de unos cuantos cerrados irreducibles $(\mathfrak{p}_i)_0$).

Recíprocamente, supongamos $\mathfrak{p} = r(\mathfrak{q}_1)$. Sea $a \in \bigcap_{i=2}^{n} \mathfrak{q}_i$ y $a \notin \mathfrak{q}_1$; por la proposición anterior $(I : a) = (\mathfrak{q}_1 : a)$ y es un ideal $\mathfrak{p}$-primario. Si $(\mathfrak{q}_1 : a) \neq \mathfrak{p}$, sea $\mathfrak{p}^r$ la primera potencia contenida en $(\mathfrak{q}_1 : a)$. Sea $b \in \mathfrak{p}^{r-1}$ tal que $b \notin (\mathfrak{q}_1 : a)$. Entonces $(I : ab) = (\mathfrak{q}_1 : ab) = \mathfrak{p}$. □

20. Definición: Sea A un anillo noetheriano. Llamaremos *ideales primos asociados* a un ideal I a los radicales de las componentes de cualquier descomposición primaria reducida de I.

Veamos ahora que los A-módulos $A/\mathfrak{p}_x$, $x \in \operatorname{Spec} A$, son los "ladrillos" de la categoría de los A-módulos noetherianos. El significado preciso viene dado por el siguiente teorema.

21. Teorema: *Sea M un A-módulo noetheriano. Existe una cadena de submódulos*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

tal que $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, con $\mathfrak{p}_i$ primo.

Demostración. Sea m un elemento no nulo de M. Entonces, $A/I \simeq \langle m\rangle \subset M$. Existe $\bar{a} \in A/I$ cuyo anulador es $\bar{\mathfrak{p}}_1$, siendo $\bar{\mathfrak{p}}_1$ un primo de A/I asociado al ideal 0. Sea $\pi\colon A \to A/I$ el morfismo de paso al cociente y $\mathfrak{p}_1 = \pi^{-1}(\bar{\mathfrak{p}}_1)$. Luego $A/\mathfrak{p}_1 = (A/I)/\bar{\mathfrak{p}}_1 = \langle \bar{a}\rangle \subset \langle m\rangle \subset M$. Tomando $M_1 = A/\mathfrak{p}_1$ y repitiendo el argumento para M/M_1 se obtiene $A/\mathfrak{p}_2 \subset M/M_1$. Sea $M_2 = \phi^{-1}(A/\mathfrak{p}_2)$, siendo $\phi\colon M \to M/M_1$ el morfismo de paso al cociente; así sucesivamente se concluye por noetherianidad.

□

Hasta ahora, hemos desarrollado la descomposición primaria de los ideales de un anillo noetheriano. De modo totalmente análogo podemos desarrollar la descomposición primaria en módulos noetherianos. Indiquemos la línea argumental y dejemos al lector las demostraciones.

22. Definición: Un submódulo $M' \subset M$ diremos que es primario, si los elementos del anillo que son divisores de cero en M/M' (es decir, la homotecia definida por el elemento tiene núcleo no trivial) son nilpotentes en M/M' (es decir, la homotecia definida es nilpotente).

23. Definición: Un submódulo $M' \subseteq M$ diremos que es irreducible si no es intersección de dos submódulos estrictamente mayores de M.

24. Proposición: *Los submódulos irreducibles de un módulo noetheriano son primarios.*

25. Teorema: *Todo submódulo de un módulo noetheriano es intersección de un número finito de submódulos primarios.*

26. Proposición: *Si $M' \subset M$ es un submódulo primario, entonces el anulador de M/M' es un ideal primario.*

Si M' es un submódulo primario y $\mathfrak{p}$ es el radical del anulador de M/M', entonces diremos que M' es un submódulo $\mathfrak{p}$-primario y que $\mathfrak{p}$ es el ideal primo asociado a M'.

27. Proposición : *Si M_1,M_2 son submódulos $\mathfrak{p}$-primarios entonces $M_1 \cap M_2$ es $\mathfrak{p}$-primario.*

Por tanto, existen descomposiciones primarias reducidas de los submódulos de un módulo noetheriano.

Dados $m \in M$ y $M' \subset M$, denotaremos $(M'\colon m) = \{a \in A : am \in M'\}$.

28. Proposición: *Sea $M' \subset M$ un submódulo primario. Sea $\mathfrak{q}$ el anulador de M/M' y $\mathfrak{p}$ el radical de $\mathfrak{q}$. Se verifica*

$$(M'\colon m) = \begin{cases} A & \text{si } m \in M'. \\ \mathfrak{q}' & \text{si } m \notin M', \text{ siendo } \mathfrak{q}' \text{ un ideal } \mathfrak{p}\text{-primario, que contiene a } \mathfrak{q}. \end{cases}$$

29. Proposición: *Sea M' un submódulo de un módulo noetheriano M y consideremos una descomposición primaria reducida $M' = M_1 \cap \cdots \cap M_n$ de M'. Un ideal primo $\mathfrak{p}$ es un ideal primo asociado a alguno de los M_i si y solo si existe $m \in M$ tal que $(M' : m) = \mathfrak{p}$.*

30. Teorema de unicidad de las componentes no sumergidas: *Sea M' un submódulo de un módulo noetheriano M y $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida. Sea $\mathfrak{p}_x$ el ideal primo asociado a M_i y supongamos que es minimal entre los ideales primos asociados a los M_j. Entonces,*

$$M_i = M \cap M'_x$$

31. Ejercicio: Prueba que los ideales primos minimales asociados a un submódulo M' de un módulo noetheriano M, coinciden con los ideales primos minimales asociados al ideal anulador de M/M'.

3.2.1. Una descomposición primaria canónica

32. Proposición: *Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida y $\mathfrak{p}_x$ un ideal primo. Denotemos $J := \cap_{\mathfrak{q}_i \subseteq \mathfrak{p}_x} \mathfrak{q}_i$. Entonces*

$$J = A \cap I_x.$$

Por tanto, el ideal J no depende de la descomposición primaria de I escogida.

Demostración. Se deduce de la Proposición 3.2.7 □

33. Corolario: *Sean $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$ dos descomposiciones primarias reducidas de primos asociados $r(\mathfrak{q}'_i) = r(\mathfrak{q}_i) = \mathfrak{p}_{x_i}$. Se cumple que*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j \cap \mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$$

para todo j. En consecuencia, si $\mathfrak{q}''_i$ son ideales $\mathfrak{p}_{x_i}$-primarios, y cada uno de ellos aparece en alguna descomposición primaria reducida de I, entonces

$$I = \mathfrak{q}''_1 \cap \cdots \cap \mathfrak{q}''_n.$$

Demostración. Reordenando, podemos suponer que $\mathfrak{q}_i, \mathfrak{q}'_i \subseteq \mathfrak{p}_{x_j} \Leftrightarrow i \leq j$. Por la proposición anterior, $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_j$. Denotemos $J_i = A \cap I_{x_i}$. Por la proposición anterior, $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} = \cap_{i<j} J_i = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1}$. Por tanto,

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1} \cap \mathfrak{q}'_j \overset{3.2.32}{=} \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

Cortando con $\mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$ concluimos. □

Procedamos a ver que entre las descomposiciones primarias de I hay una canónica.

34. Proposición: *Sea I un ideal de un anillo noetheriano, de ideales primos asociados $x_1,\dots,x_r$. Sea n_i el número natural más pequeño posible tal que $\mathfrak{p}_{x_i}^{n_i}$ está incluido en algún ideal $\mathfrak{p}_{x_i}$-primario que aparezca en alguna descomposición primaria reducida de I y $\alpha_i = A \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i}$. Entonces,*

$$I = \alpha_1 \cap \cdots \cap \alpha_r$$

es una descomposición primaria reducida de I (y diremos que es la descomposición primaria canónica de I).

Demostración. $(I+\mathfrak{p}_{x_i}^{n_i})_{x_i}$ es un ideal $\mathfrak{p}_{x_i}\cdot A_{x_i}$-primario, luego α_i en un ideal $\mathfrak{p}_{x_i}$-primario. Consideremos una descomposición primaria reducida $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, tal que $\mathfrak{p}_{x_i}^{(n_i)} \subset \mathfrak{q}_i$, para todo i. Entonces, $\alpha_i \subseteq \mathfrak{q}_i$ y por tanto

$$I \subseteq \bigcap_{i=1}^{r} \alpha_i \subseteq \bigcap_{i=1}^{r} \mathfrak{q}_i = I$$

luego todas las inclusiones son igualdades.

□

Tenemos pues unos números $n_1,\dots,n_r$ canónicamente asociados al ideal I. Determinemos de un modo algo más algorítmico los números n_i. Sea $I_i = \cap_{\mathfrak{p}_{x_j} \subsetneq \mathfrak{p}_{x_i}} \alpha_j$. Entonces, n_i es el mínimo número tal que $I_{i,x_i} \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i} = I_{x_i}$. Como

$$I_{i,x_i} \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i} = (I_i \cap (I + \mathfrak{p}_{x_i}^{n_i}))_{x_i} = (I + (I_i \cap \mathfrak{p}_{x_i}^{n_i}))_{x_i},$$

n_i es el mínimo numero tal que $(I_i \cap \mathfrak{p}_{x_i}^{n_i})_{x_i} \subseteq I_{x_i}$, es decir, $(I : I_i \cap \mathfrak{p}_{x_i}^{n_i})_{x_i} = A_{x_i}$. Por tanto, n_i es el mínimo número tal que $(I : I_i \cap \mathfrak{p}_{x_i}^{n_i}) \not\subseteq \mathfrak{p}_{x_i}$.

Del mismo modo obtenemos descomposiciones primarias canónicas para los submódulos de un módulo noetheriano. Las demostraciones de las siguientes proposiciones se pueden copiar de sus equivalentes en el caso de ideales.

35. Proposición: *Sea M' un submódulo del módulo noetheriano M, $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida, y $\mathfrak{p}_x$ un ideal primo. Sea M'' la intersección de los M_i cuyos primos asociados están contenidos en $\mathfrak{p}_x$. Entonces*

$$M'' = M \cap M'_x.$$

Por tanto, M'' no depende de la descomposición primaria escogida.

36. Corolario: *Sean $M' = M_1 \cap \cdots \cap M_n = N_1 \cap \cdots \cap N_n$ dos descomposiciones primarias reducidas, de primos asociados $\mathfrak{p}_{x_i}$. Se verifica que*

$$M' = M_1 \cap \cdots \cap M_{j-1} \cap N_j \cap M_{j+1} \cap \cdots \cap M_n$$

para todo j. En consecuencia, si $\{L_i\}_{1 \leq i \leq n}$ son submódulos $\mathfrak{p}_{x_i}$-primarios y cada uno de ellos aparece en alguna descomposición primaria de M', entonces

$$M' = L_1 \cap \cdots \cap L_n.$$

37. Proposición: *Sea M' un submódulo de un A-módulo noetheriano M. Sea $M' = M_1 \cap \cdots \cap M_m$ una descomposición primaria reducida de primos asociados $\mathfrak{p}_{x_i}$. Sea $n_i \in \mathbb{N}$ tal que $\mathfrak{p}_{x_i}^{n_i}$ está contenido en el anulador de M/M_i. Denotemos por N_i el submódulo $\mathfrak{p}_{x_i}$-primario antimagen de ${M'}_{x_i} + \mathfrak{p}_{x_i}^{n_i} M_{x_i}$ por el morfismo de localización $M \to M_{x_i}$. Entonces,*

$$M' = M_1 \cap \cdots \cap N_i \cap \cdots \cap M_m.$$

Ahora, argumentando como en el caso de los ideales, obtendremos una descomposición primaria canónica de M'.

3.3. Morfismos finitos

1. Definición: Un morfismo de anillos $f : A \to B$ se dice que es finito si B es un A-módulo finito generado, con la estructura natural de A-módulo que define el morfismo f en B ($a \cdot b := f(a) \cdot b$). En este caso, también se dice que B es una A-álgebra finita. Si $A \to B$ es un morfismo finito, diremos que el morfismo inducido $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ es finito.

2. Proposición: *La composición de morfismos finitos es finito.*

Demostración. Sean $A \overset{\text{finito}}{\longrightarrow} B \overset{\text{finito}}{\longrightarrow} C$. Es decir, $B = Ab_1 + \cdots + Ab_n$ y $C = Bc_1 + \cdots + Bc_m$. Luego,

$$C = (Ab_1 + \cdots + Ab_n)c_1 + \cdots + (Ab_1 + \cdots + Ab_n)c_m = \sum_{i=1,j=1}^{n,m} Ab_i c_j$$

En conclusión, $A \to C$ es un morfismo finito.

□

3. Proposición : *Si $A \to B$ es un morfismo finito y $A \to C$ un morfismo de anillos, entonces $C = A \otimes_A C \to B \otimes_A C$ es un morfismo finito.*

"Los morfismos finitos son estables por cambio de base".

Demostración. Es inmediata. □

4. Corolario : *Si $A \to B$ es un morfismo finito, entonces $A_S \to B_S$ y $A/I \to B/I \cdot B$ son morfismos finitos*

5. Definición : Sea $A \to B$ un morfismo de anillos. Se dice que $b \in B$ es entero sobre A si verifica una relación del tipo

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0, \qquad \text{con} a_i \in A.$$

Hemos demostrado el teorema de Hamilton-Cayley para los endomorfismos de espacios vectoriales, pero también es cierto para los endomorfismos de módulos. Con precisión, sea $M = \langle m_1, \ldots, m_r \rangle$, $f : M \to M$, $f(m_i) = \sum_j a_{ij} m_j$ un endomorfismo de A-módulos y sea $p_c(x)$ el polinomio característico de la matriz (a_{ij}). Entonces $p_c(f) = 0$. En efecto, consideremos la matriz $B = (x_{ij})$ de coeficientes variables y el polinomio característico $P_c(X)$ de esta matriz. $P_c(X)$ es un polinomio con coeficientes en $\mathbb{Z}[x_{ij}] \subset \mathbb{Q}(x_{ij})$. Por el teorema de Hamilton-Cayley $P_c(B) = 0$. Por tanto, especializando a $x_{ij} = a_{ij}$, tendremos que $p_c(f) = 0$.

6. Proposición : *Sean $f : A \to B$ un morfismo de anillos y $b \in B$. Denotemos $A[b] = \{p(b) \in B, \text{para } p(x) \in A[x]\}$. El morfismo $A \to A[b]$ es finito $\Leftrightarrow$ b es entero sobre A.*

Demostración. $\Rightarrow$) Consideremos el endomorfismo de A-módulos

$$\begin{aligned} A[b] &\xrightarrow{\cdot b} A[b] \\ p(b) &\longmapsto p(b) \cdot b \end{aligned}$$

Si (a_{ij}) es una matriz asociada a $\cdot b$ en un sistema generador de $A[b]$, entonces el polinomio característico de (a_{ij}), $p_c(x)$ anula a $\cdot b$, luego $0 = p_c(b\cdot)(1) = p_c(b)$ y b es entero sobre A.

$\Leftarrow$) Sea $p(x)$ un polinomio mónico con coeficientes en A que anula a b. Entonces $A[b]$ es un cociente de $A[x]/(p(x))$. Como $A[x]/(p(x))$ es un A-módulo finito generado (se prueba igual que 0.6.69) se concluye. □

7. Observación : Para la demostración de $\Rightarrow$) solo es necesario suponer que $A[b]$ está incluido en una A-álgebra finita.

8. Ejemplo: Si α es una raíz n-ésima de la unidad, entonces $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ es un morfismo finito.

9. Ejemplo: El morfismo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3) \to \operatorname{Spec} k[x]$ definido por $(\alpha, \beta) \mapsto \alpha$ es un morfismo finito.

3.3.1. Cierre entero

10. Proposición: *Sea $f : A \to B$ un morfismo de anillos. El conjunto de elementos de B enteros sobre A forman una A-subálgebra de B.*

Demostración. Sean $b_1, b_2 \in B$ enteros sobre A. Tenemos que $A \to A[b_1]$ es un morfismo finito, y $A[b_1] \to A[b_1, b_2]$ es un morfismo finito porque si b_2 verifica una relación entera con coeficientes en A, en particular la verifica con coeficientes en $A[b_1]$. Por tanto, por la proposición 3.3.2, $A \to A[b_1, b_2]$ es un morfismo finito. Luego, por la observación anterior, todo elemento $p(b_1, b_2) \in A[b_1, b_2] \subseteq B$, con $p(x,y) \in A[x,y]$, es entero sobre A.

□

11. Definición: Diremos que un anillo íntegro A es íntegramente cerrado en su cuerpo de fracciones Σ, si todo elemento de Σ entero sobre A pertenece a A. También se dice que A es un anillo normal.

Se dice que un morfismo de anillos $A \to B$ es entero si todo elemento de B es entero sobre A, es decir, si B es unión de A-subálgebras finitas.

Sea $A \to B$ un morfismo inyectivo de anillos. Llamaremos cierre entero de A en B al subanillo de B formado por todos los elementos de B enteros sobre A.

12. Proposición: *La composición de dos morfismos enteros es entero.*

Demostración. Sean $A \to B$ y $B \to C$ dos morfismos enteros. Dado $c \in C$, existe un polinomio $p(x) = \sum_i b_i x^i \in B[x]$ tal que $p(c) = 0$. Consideremos la A-álgebra $B' := A[b_i]_i$. Los morfismos $A \to B'$ y $B' \to B'[c]$ son finitos. Por tanto, $A \to B'[c]$ es finito y c es entero sobre A. En conclusión, $A \to C$ es un morfismo entero. □

Dejamos que el lector pruebe que el cierre entero de un anillo íntegro en su cuerpo de fracciones es un anillo íntegramente cerrado.

13. Ejercicio: Demuestra que $\mathbb{Z}$ es un anillo íntegramente cerrado en $\mathbb{Q}$.

14. Lema : *El cierre entero conmuta con localizaciones: Sea $A \to B$ un morfismo de anillos y $S \subset A$ un sistema multiplicativo. Sea $\bar{A}$ el cierre entero de A en B y $\overline{A_S}$ el cierre entero de A_S en B_S. Entonces,*

$$\overline{A_S} = (\bar{A})_S.$$

En particular, si A es íntegramente cerrado, entonces A_S también.

Un anillo íntegro es íntegramente cerrado en su cuerpo de fracciones si y solo si es localmente íntegramente cerrado.

Demostración. $A_S \to (\bar{A})_S$ es un morfismo entero, luego $(\bar{A})_S \subseteq \overline{A_S}$. Sea $f \in \overline{A_S}$. Existe una relación entera

$$f^n + a_1/s_1 \cdot f^{n-1} + \cdots + a_n/s_n = 0 \qquad \text{con } a_i \in A \text{ y } s_i \in S \neq 0.$$

Sea $s = s_1 \cdots s_n$ (luego $s \in S$). Multiplicando la relación anterior por $t^n s^n$ (para cierto $t \in S$) obtenemos una relación entera de tsf con coeficientes en A, luego $tsf \in \bar{A}$ y $f \in (\bar{A})_S$. Luego, $(\bar{A})_S = \overline{A_S}$.

Por último, $A = \bar{A} \iff A_x = (\bar{A})_x = \overline{A_x}$ para todo $x \in \operatorname{Spec} A$.

□

15. Proposición : *Sea A un anillo noetheriano íntegro e íntegramente cerrado en su cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita separable de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces, el morfismo $A \hookrightarrow \bar{A}$, es finito y el cuerpo de fracciones de $\bar{A}$ es $\bar{\Sigma}$.*

Demostración. $\bar{\Sigma}$ es el cuerpo de fracciones de $\bar{A}$, porque el cierre entero conmuta con localizaciones por 3.3.14, luego $\bar{A}_{A-0} = \overline{A_{A-0}} = \bar{\Sigma}$.

Como A es noetheriano, basta probar que $\bar{A}$ es un submódulo de un A-módulo libre finito generado.

Sea T_2 la métrica de la traza en $\bar{\Sigma}$, $T_2(f,g) = \operatorname{tr}(f \cdot g)$, y sea $iT_2 \colon \bar{\Sigma} \to \bar{\Sigma}^*$ su polaridad asociada, que es un isomorfismo por ser $\bar{\Sigma}$ separable. Sea $\bar{a}_1, \ldots, \bar{a}_n \in \bar{A}$ una base de $\bar{\Sigma}$ como Σ-espacio vectorial y $w_1, \ldots, w_n \in \bar{\Sigma}^*$ su base dual. Si probamos que $iT_2(\bar{A}) \subseteq Aw_1 + \cdots + Aw_n$ concluimos.

Como ya sabemos, $\operatorname{tr}(a') = \sum_{g \in G} g(a')$, siendo $G = \operatorname{Hom}_{\Sigma - alg}(\bar{\Sigma}, \bar{\bar{\Sigma}})$ y $\bar{\bar{\Sigma}}$ la envolvente de Galois de la extensión $\Sigma \to \bar{\Sigma}$. Dado $a' \in \bar{A}$, escribamos $iT_2(a') = \lambda_1 w_1 + \cdots + \lambda_n w_n$, con $\lambda_i \in \Sigma$. Tenemos que ver que $\lambda_i \in A$. Se tiene que

$$\lambda_i = iT_2(a')(\bar{a}_i) = \operatorname{tr}(a' \cdot \bar{a}_i) = \sum_{g \in G} g(a' \cdot \bar{a}_i)$$

Ahora bien, $a' \cdot \bar{a}_i \in \bar{A}$, luego $g(a' \cdot \bar{a}_i)$ es entero sobre A y λ_i es entero sobre A. Como A es íntegramente cerrado en su cuerpo de fracciones entonces $\lambda_i \in A$.

□

16. Proposición: *Los dominios de factorización única son íntegramente cerrados en su cuerpo de fracciones.*

Demostración. Sea A un dominio de factorización única y Σ su cuerpo de fracciones. Sea $\frac{a}{b} \in \Sigma$ una fracción de modo que b no sea invertible y sea primo con a. Si $\frac{a}{b}$ es entero sobre A, verifica una relación

$$(\frac{a}{b})^n + a_1(\frac{a}{b})^{n-1} + \ldots + a_n = 0.$$

Multiplicando por b^n tendremos que a^n es múltiplo de b, lo que contradice que b es primo con a. En conclusión, los únicos elementos de Σ enteros sobre A son los de A.

□

17. Teorema: *Sea A una k-álgebra de tipo finito íntegra de cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces, $A \hookrightarrow \bar{A}$ es un morfismo finito, y $\bar{\Sigma}$ es el cuerpo de fracciones $\bar{A}$.*

Demostración. Por el lema de normalización de Noether existe un morfismo

$$k[x_1, \ldots, x_n] \hookrightarrow A$$

finito e inyectivo. El cierre entero de A en $\bar{\Sigma}$ coincide con el cierre entero de $k[x_1, \ldots, x_n]$ en $\bar{\Sigma}$, luego podemos suponer que $A = k[x_1, \ldots, x_n]$.

Sea Ω la envolvente normal de $\bar{\Sigma}$. El cierre entero de A en Ω contiene a $\bar{A}$, luego si demostramos que el cierre entero de A en Ω es un A-módulo finito generado tendremos que $\bar{A}$ también lo es. Así pues, podemos suponer que $\bar{\Sigma}$ es una extensión normal de Σ.

Sea G el grupo de Galois de $\bar{\Sigma}$. Sea $\bar{\Sigma}^G$ los elementos de $\bar{\Sigma}$ invariantes por G y denotemos A' al cierre entero de A en $\bar{\Sigma}^G$. A' es un A-módulo finito generado: Observemos que $\Sigma \hookrightarrow \bar{\Sigma}^G$ es una extensión puramente inseparable. Sea $\operatorname{car} k = p > 0$ y escribamos $\bar{\Sigma}^G = \Sigma[\xi_1, \ldots, \xi_r]$. Existe $m >> 0$ de modo que $\xi_i^{p^m} \in \Sigma = k(x_1, \ldots, x_n)$, para todo i. Escribamos $\xi_i^{p^m} = p_i/q_i$, con $p_i = \sum_j \lambda_{ij} x^j \in k[x_1, \ldots, x_n]$ y $q_i = \sum_j \mu_{ij} x^j \in k[x_1, \ldots, x_n]$. Sea $k' := k(\sqrt[p^m]{\lambda_{ij}}, \sqrt[p^m]{\mu_{ij}})_{ij}$ y $\Sigma' := k'(\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n})$. Se verifica que $\xi_i = \sqrt[p^m]{p_i/q_i} \in \Sigma'$, luego $\bar{\Sigma}^G \subseteq \Sigma'$. Podemos suponer que $\bar{\Sigma}^G = \Sigma'$. Ahora bien, el cierre entero $k[x_1, \ldots, x_n]$ en Σ' es $k'[\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n}]$, pues $k'[\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n}]$ es un $k[x_1, \ldots, x_n]$-módulo finito generado y es íntegramente cerrado (porque es un anillo de polinomios). Hemos concluido.

$\bar{A}$ coincide con el cierre entero de A' en $\bar{\Sigma}$, luego $\bar{A}$ es un A'-módulo finito generado por el lema anterior, pues $\bar{\Sigma}^G \hookrightarrow \bar{\Sigma}$ es una extensión separable (de Galois). Por tanto, $\bar{A}$ es un A-módulo finito generado.

□

18. Proposición: *Si $f : A \hookrightarrow B$ es un morfismo entero e inyectivo, entonces el morfismo inducido $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo*

Demostración. Supongamos que f es un morfismo finito. Dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to B_x$ es finito e inyectivo. Por Nakayama, $\mathfrak{p}_x B_x \neq B_x$, luego $\operatorname{Spec} B_x/\mathfrak{p}_x B_x \neq \emptyset$. Es decir, la fibra de x es no vacía, luego f^* es epiyectivo.

Ahora ya, si B es entero sobre A, entonces $B_x/\mathfrak{p}_x B_x \neq 0$ porque si $B_x/\mathfrak{p}_x B_x = 0$, es decir, $1 \in \mathfrak{p}_x B_x$, para alguna subálgebra finita B_i se verificará que $1 \in \mathfrak{p}_x B_i$, es decir, $(B_i)_x/\mathfrak{p}_x(B_i)_x = 0$ y llegaremos a contradicción con el párrafo anterior. De nuevo, tenemos que la fibra de x es no vacía y f^* es epiyectivo. □

19. Definición: Llamaremos dimensión de Krull de un anillo A, que denotaremos $\dim A$, al supremo de las longitudes de las cadena de ideales primos de A, o equivalentemente, al supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$. Llamaremos dimensión de $\operatorname{Spec} A$, que denotaremos $\dim \operatorname{Spec} A$, a la dimensión de Krull de A.

20. Ejercicio: Demuestra que la dimensión de Krull de $\mathbb{Z}$ y $k[x]$ es uno y la de $\mathbb{C}[x, y]$ dos.

21. Teorema: *Sea $f : A \to B$ es un morfismo entero. El morfismo inducido*

$$f^* : \operatorname{Spec} B \to \operatorname{Spec} A$$

es una aplicación cerrada de fibras de dimensión cero (y finitas si f es finito).

Demostración. Sea $C = (J)_0$ un cerrado de $\operatorname{Spec} B$. Debemos demostrar que $f^*(C)$ es un cerrado de $\operatorname{Spec} A$. Consideremos los diagramas

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A/(J \cap A) & \longrightarrow & B/J \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ (J \cap A)_0 = \operatorname{Spec} A/(J \cap A) & \xleftarrow[f^*{}_{|C}]{} & \operatorname{Spec} B/J = C \end{array}$$

Como $A/J \cap A \hookrightarrow B/J$ es un morfismo entero inyectivo, por 3.3.18 $f^*{}_{|C}$ es epiyectiva y $f^*(C) = (J \cap A)_0$.

La fibra de un punto $x \in \operatorname{Spec} A$ es $f^{*-1}(x) = \operatorname{Spec} B_x/\mathfrak{p}_x B_x$. Supongamos que f es un morfismo finito. Observemos que si $f^{*-1}(x) \neq \emptyset$ entonces $B_x/\mathfrak{p}_x B_x$ es una $A_x/\mathfrak{p}_x$-álgebra finita. Por la proposición 0.6.70, concluimos que f^* es de fibras de dimensión cero y finitas. Si f entero es sencillo deducir que las fibras son de dimensión cero una vez que se sabe esto para los morfismos finitos. □

22. Ejercicio: Prueba que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

3.3.2. Teorema de normalización de Noether

23. Definiciones: Sea $A = k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) = k[\xi_1,\ldots,\xi_n]$ una k-álgebra de tipo finito. Diremos que $\operatorname{Spec} A$ es una variedad algebraica afín sobre un cuerpo k. Los cerrados de las variedades algebraicas los llamaremos subvariedades algebraicas.

Si $V = \operatorname{Spec} k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ es una variedad algebraica, entonces V es un cerrado del espacio afín $\mathbb{A}^n := \operatorname{Spec} k[x_1,\ldots,x_n]$. En efecto, $V = (p_1,\ldots,p_r)_0$.

Si A y B son k-álgebras de tipo finito y $f: A \to B$ es un morfismo de k-álgebras, diremos que el morfismo inducido $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ es un morfismo de variedades algebraicas.

24. Lema de normalización de Noether: *Sea $A = k[\xi_1,\ldots,\xi_n]$ una k-álgebra de tipo finito. Supongamos que k tiene un número infinito de elementos*[1]*. Existe un morfismo finito e inyectivo*

$$k[x_1,\ldots,x_r] \hookrightarrow A$$

"Toda variedad algebraica afín se proyecta con fibras finitas en un espacio afín".

Demostración. Vamos a hacerlo por inducción sobre n. Para $n = 0$, no hay nada que decir. Supongamos que el teorema es cierto hasta $n-1$.

Si los $\{\xi_i\}$ son algebraicamente independientes entre sí, entonces $k[\xi_1,\ldots,\xi_n] = k[x_1,\ldots,x_n]$ y hemos concluido. Podemos suponer que existe $p(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$, no nulo, tal que $p(\xi_1,\ldots,\xi_n) = 0$.

Escribamos $p(x_1,\ldots,x_n) = p_s(x_1,\ldots,x_n) + p_{s-1}(x_1,\ldots,x_n) + \ldots + p_0(x_1,\ldots,x_n)$ como suma de polinomios homogéneos $p_r(x_1,\ldots,x_n)$ de grado r. Sean $x_i =: x_i' + \lambda_i x_n$, para $i < n$. Entonces,

$$p(x_1' + \lambda_1 x_n,\ldots,x_{n-1}' + \lambda_{n-1}x_n, x_n) = p_s(\lambda_1,\ldots,\lambda_{n-1},1)x_n^s + \text{polinomio en } x_1',\ldots,x_{n-1}', x_n \text{ de grado en } x_n \text{ menor que } s$$

[1] Esta hipótesis no es necesaria, solo la imponemos porque la demostración del lema es algo más sencilla.

Así pues, si elegimos $\lambda_1,\ldots,\lambda_{n-1}\in k$ de modo que $p_s(\lambda_1,\ldots,\lambda_{n-1},1)\neq 0$, tendremos que ξ_n es entero sobre $k[\xi'_1,\ldots,\xi'_{n-1}]$, con $\xi'_i=\xi_i-\lambda_i\xi_n$. Por tanto, la composición

$$k[x_1,\ldots,x_r]\underset{\text{Hip.ind.}}{\overset{\text{finito}}{\hookrightarrow}} k[\xi'_1,\ldots,\xi'_{n-1}]\overset{\text{finito}}{\hookrightarrow} k[\xi'_1,\ldots,\xi'_{n-1},\xi_n]=k[\xi_1,\ldots,\xi_{n-1},\xi_n]$$

es un morfismo finito. □

25. Observación: En la demostración del lema de Noether hemos probado que si $\xi_1,\ldots,\xi_n$ son algebraicamente dependientes entonces $r<n$.

Teorema de los ceros de Hilbert

26. Forma débil del teorema de los ceros de Hilbert: *Sea A una k-álgebra de tipo finito y $\mathfrak{m}$ un ideal maximal. Entonces $A/\mathfrak{m}$ es una extensión finita de k. En particular, si k es algebraicamente cerrado, entonces $k=A/\mathfrak{m}$: "Todo punto cerrado de una variedad algebraica afín sobre un cuerpo algebraicamente cerrado es racional".*

Demostración. Obviamente $A/\mathfrak{m}$ es una k-álgebra de tipo finito sobre k. Por el lema de normalización de Noether, existe un morfismo finito inyectivo

$$k[x_1,\ldots,x_r]\hookrightarrow A/\mathfrak{m}$$

Por tanto, $k[x_1,\ldots,x_r]$ ha de tener dimensión de Krull cero, luego $r=0$ y concluimos. □

27. Ejercicio: Sea k un cuerpo algebraicamente cerrado y

$$\begin{aligned} p_1(x_1,\ldots,x_n) &= 0\\ &\cdots\\ p_r(x_1,\ldots,x_n) &= 0 \end{aligned}$$

un sistema de ecuaciones k-algebraicas. Prueba que el sistema no tiene ninguna solución (en k) si y solo si $1\in(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$.

28. Ejercicio: Sean $X=\operatorname{Spec}A$ y $Y=\operatorname{Spec}B$ dos variedades algebraicas sobre un cuerpo algebraicamente cerrado k. Definamos $X\times_k Y:=\operatorname{Spec}A\otimes_k B$. Prueba que el conjunto de los puntos cerrados de $X\times_k Y$ es igual al producto cartesiano del conjunto de los puntos cerrados de X y del conjunto de los puntos cerrados de Y.

29. Corolario: *Sea $\bar{k}$ el cierre algebraico de k y $X = \operatorname{Spec} k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ una variedad k-algebraica. Dos soluciones $\alpha,\beta \in \bar{k}^n$ del sistema de ecuaciones $p_1 = \cdots = p_r = 0$ diremos que son equivalentes si existe un automorfismo $\tau\colon \bar{k} \to \bar{k}$ de k-álgebras tal que $\tau(\alpha) := (\tau(\alpha_1),\dots,\tau(\alpha_n)) = \beta$. Se cumple que*

$$\{\textit{Conjunto de puntos cerrados de } X\} = \left\{ \begin{array}{l} \textit{Conjunto de soluciones sobre } \bar{k} \\ \textit{del sistema } p_1 = \cdots = p_r = 0 \end{array} \right\} / \sim$$

Demostración. Escribamos $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$, $X_{\bar{k}} = \operatorname{Spec}(A \otimes_k \bar{k})$. El morfismo natural $A \hookrightarrow A \otimes_k \bar{k}$ es inyectivo y entero. Por tanto, el morfismo natural $\pi\colon X_{\bar{k}} \to X$ es epiyectivo, y aplica epiyectivamente los puntos cerrados de $X_{\bar{k}}$ en los puntos cerrados de X. El conjunto de puntos cerrados de $X_{\bar{k}}$ se identifica con el conjunto de las soluciones con valores en $\bar{k}$ del sistema $p_1 = \cdots = p_r = 0$, por el teorema de los ceros de Hilbert. Sólo nos falta probar que dos soluciones α, β cumplen que $\pi(\alpha) = \pi(\beta)$ si y solo si son equivalentes. Observemos que $\mathfrak{m}_{\pi(\alpha)} = \{\bar{p} \in k[x_1,\dots,x_n]/(p_1,\dots,p_r)\colon p(\alpha) = 0\}$. Como $\tau(p(\alpha)) = p(\tau(\alpha))$ tenemos que $\mathfrak{m}_{\pi(\alpha)} = \mathfrak{m}_{\pi(\tau(\alpha))}$. Supongamos que $\pi(\alpha) = \pi(\beta)$ y sea $K = A/\mathfrak{m}_{\pi(\alpha)} = A/\mathfrak{m}_{\pi(\beta)}$. Tenemos dos morfismos $f, g\colon K \to \bar{k}$, $\bar{p} \mapsto p(\alpha), p(\beta)$. Por el teorema de prolongación (la aplicación $\operatorname{Hom}_{k-alg}(\bar{k},\bar{k}) = \operatorname{Spec}(\bar{k} \otimes_k \bar{k}) \to \operatorname{Spec}(K \otimes_k \bar{k}) = \operatorname{Hom}_{k-alg}(K,\bar{k})$ es epiyectiva) existe un automorfismo $\tau\colon \bar{k} \to \bar{k}$ de modo que $\tau \circ f = g$, luego $\tau(x_i(\alpha)) = x_i(\beta)$ y $\tau(\alpha) = \beta$.

□

30. Proposición: *Si $f^*\colon X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ es un morfismo entre variedades algebraicas afines, entonces la imagen de un punto cerrado es un punto cerrado.*

Demostración. Si x es un punto cerrado de X e $y = f^*(x)$, entonces $A/\mathfrak{p}_y \to B/\mathfrak{m}_x$ es inyectivo. Por el teorema de los ceros de Hilbert, $B/\mathfrak{m}_x$ es una extensión finita de k, por tanto $A/\mathfrak{p}_y$ es una k-álgebra finita e íntegra, luego es un cuerpo; es decir, y es un punto cerrado. □

31. Corolario: *Sea $U \subset X$ un abierto de una variedad algebraica afín. Un punto $x \in U$ es cerrado en U si y solo si es cerrado en X. Es decir, los puntos cerrados de U son los puntos cerrados de X que yacen en U.*

Demostración. Todo abierto es unión de abiertos básicos, luego basta probar el enunciado para un abierto básico U_a. Ahora bien, como $A_a = A[\frac{1}{a}]$ es una k-álgebra de tipo finito, $U_a = \operatorname{Spec} A_a$ es una variedad algebraica. Se concluye por la proposición anterior aplicada a la inclusión $U_a \hookrightarrow X$. □

32. Definición: Diremos que $X = \mathrm{Spec}\, A$ es íntegra si A es un anillo íntegro. Diremos que $X = \mathrm{Spec}\, A$ es reducida si A es un anillo reducido.

33. Forma fuerte de los ceros de Hilbert: *Sea $X = \mathrm{Spec}\, A$ una variedad algebraica. Si $f \in A$ se anula en todo punto cerrado de X, entonces es nilpotente. En particular, si $X = \mathrm{Spec}\, A$ es una variedad algebraica reducida sobre un cuerpo algebraicamente cerrado, entonces una función es nula si y solo si se anula en todos los puntos racionales.*

Demostración. Por el corolario anterior, U_f no contiene puntos cerrados, luego $U_f = \emptyset$. Es decir, f se anula en todo punto de X, luego es nilpotente. □

34. Corolario: *Dos subconjuntos cerrados de una variedad algebraica afín son iguales si y solo si contienen los mismos puntos cerrados.*

Demostración. Una función se anula sobre todos los puntos de un cerrado de una variedad algebraica si y solo si se anula sobre todos los puntos cerrados del cerrado, por la forma fuerte del teorema de los ceros de Hilbert. Como todo cerrado coincide con los ceros del ideal de todas las funciones que se anulan sobre él, hemos terminado. □

3.3.3. Teoremas de ascenso y descenso de ideales

35. Definición: Se dice que un morfismo de anillos $A \to B$ cumple el teorema del ascenso de ideales si para cada par de ideales primos $\mathfrak{p}_y \subseteq \mathfrak{p}_{y'}$ de A, y un ideal primo $\mathfrak{p}_x \subseteq B$ tal que $\mathfrak{p}_x \cap A = \mathfrak{p}_y$, entonces existe un ideal primo $\mathfrak{p}_{x'} \supseteq \mathfrak{p}_x$ tal que $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$.

Se dice que un morfismo de anillos $A \to B$ cumple el teorema del descenso de ideales si para cada par de ideales primos $\mathfrak{p}_{y'} \subseteq \mathfrak{p}_y \subseteq A$, y un ideal primo $\mathfrak{p}_x \subseteq B$ tal que $\mathfrak{p}_x \cap A = \mathfrak{p}_y$, entonces existe un ideal primo $\mathfrak{p}_{x'} \subseteq \mathfrak{p}_x$ tal que $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$.

36. Teorema del ascenso: *Si $f\colon A \to B$ es un morfismo entero entonces cumple el teorema del ascenso de ideales.*

Demostración. Sea $f^*\colon \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ inducida por f. Como $f^*(x) = y$, entonces $f^*(\bar{y}) \subseteq \bar{x}$. Como $x \in f^*(\bar{y})$ y $f^*(\bar{y})$ es cerrado, entonces $f^*(\bar{y}) = \bar{x}$. Por lo tanto, existe $y' \in \bar{y}$ tal que $f^*(y') = x' \in \bar{x}$. Es decir, existe un ideal primo $\mathfrak{p}_{y'} \supset \mathfrak{p}_y$, tal que $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$. □

37. Corolario: *Si $f\colon A \hookrightarrow B$ es un morfismo entero inyectivo, entonces* $\dim A = \dim B$. *Geométricamente, si $\pi\colon \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ es un morfismo entero y $C \subseteq \mathrm{Spec}\, B$ es un cerrado entonces* $\dim C = \dim \pi(C)$.

Demostración. Dada una cadena estricta de ideales primos $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ de B, $f^{-1}(\mathfrak{p}_1) \subset f^{-1}(\mathfrak{p}_2) \subset \cdots \subset f^{-1}(\mathfrak{p}_n)$ es una cadena de ideales primos estricta de A, pues las fibras del morfismo inducido por f entre los espectros son de dimensión cero, por 3.3.21. Por tanto, $\dim B \leq \dim A$.

Sea ahora una cadena estricta de ideales primos $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_n$ de A. Sea $\mathfrak{p}_1$ un ideal primo de B, tal que $f^{-1}(\mathfrak{p}_1) = \mathfrak{q}_1$ (existe por 3.3.18). Por el teorema del ascenso, existe $\mathfrak{p}_2 \supset \mathfrak{p}_1$ tal que $f^{-1}(\mathfrak{p}_2) = \mathfrak{q}_2$. Así sucesivamente, obtendremos una cadena estricta de ideales primos $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ de B (de antimagen por f, la cadena de A). Por tanto, $\dim A \leq \dim B$, luego $\dim A = \dim B$.

En cuanto a la formulación geométrica del corolario, digamos que si I_C es el ideal de todas las funciones que se anulan en C e $I_{\pi(C)}$ es el ideal de todas las funciones que se anulan en $\pi(C)$, tenemos el morfismo entero inyectivo $A/I_{\pi(C)} \hookrightarrow B/I_C$, luego $\dim C = \dim \pi(C)$.

□

Si G es un grupo de automorfismos de un anillo A, de modo natural G es un grupo de homeomorfismos de $\operatorname{Spec} A$, definiendo $g \cdot x := g^{*-1}(x)$, es decir, $\mathfrak{p}_{g\cdot x} = g(\mathfrak{p}_x)$.

Sea G un grupo de homeomorfismos de un espacio topológico X. Llamaremos espacio topológico cociente de X por G, al conjunto $X/G := \{[x], x \in X$, de modo que $[x] = [x']$ si y solo si existe $g \in G$ tal que $x' = g(x')\}$, con la topología final del morfismo de paso a cociente, $\pi\colon X \to X/G$, $\pi(x) = [x]$, es decir, $U \subset X/G$ es un abierto si y solo si $\pi^{-1}(U)$ es un abierto de X. Se verifica que π es una aplicación abierta, porque si V es un abierto de X, $\pi^{-1}(\pi(V)) = \bigcup_{g\in G} g(V)$, que es un abierto, luego $\pi(V)$ es un abierto de X/G. Del mismo modo, si G es finito, π es un morfismo cerrado. En este caso, si $\pi(x) = y$ e $y \in \bar{y'}$ (cierre de y'), entonces existe x' de modo que $x \in \bar{x'}$ y $\pi(x') = y'$: Sea x'' tal que $\pi(x'') = y'$. Las fibras de π son las órbitas por la acción de G y $\pi(\overline{x''}) = \overline{y'}$, luego $\pi^{-1}(\bar{y'}) = \bigcup_{g\in G} \overline{gx''}$. Entonces, $x \in \overline{gx''}$ para algún $g \in G$. Luego, $x' := gx''$ verifica que $x \in \bar{x'}$ y $\pi(x') = \pi(x'') = y'$.

38. Proposición: *Sea G un grupo finito de automorfismos de un anillo B. Se verifica que*

$$\operatorname{Spec}(B^G) = (\operatorname{Spec} B)/G$$

donde $B^G = \{b \in B\colon g(b) = b$, para todo $g \in G\}$.

En consecuencia, el morfismo natural $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} B^G$ cumple el teorema del descenso de ideales.

Demostración. Empecemos observando que dada $f \in B$, el polinomio $\prod_{g\in G} (x - g(f))$ es un polinomio mónico con coeficientes en B^G que anula a f, luego f es entero sobre B^G.

Por tanto, $B^G \hookrightarrow B$ es un morfismo entero, luego en espectros epiyectivo, cerrado y de fibras de dimensión cero.

Sólo nos falta ver que las fibras del morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$ son órbitas por la acción de G.

G actúa transitivamente sobre las fibras del morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$: Dado un ideal primo $\mathfrak{p}_x \subset B$, $g(\mathfrak{p}_x)$ corta a B^G en el mismo ideal primo que $\mathfrak{p}_x$. Es decir, G actúa en las fibras. Sea $\mathfrak{p}_x$ es un ideal primo de B distinto de $g(\mathfrak{p}_{x'}) = \mathfrak{p}_{g(x')}$ para todo $g \in G$. Supongamos que x, x' tienen la misma imagen por el morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$, digamos y. Por ser el morfismo $B^G \hookrightarrow B$ entero sabemos que $g(x') \notin \bar{x}$ para todo $g \in G$, luego existe una $f \in B$ que se anula en x y no se anula en ninguno de los $g(x')$. Entonces $N(f) := \prod_{g \in G} g(f) \in B^G$ se anula en x y no se anula en ninguno de los $g(x')$. Llegamos a contradicción, porque por un lado $N(f)$ ha de anularse en y y por el otro no. □

39. Teorema del descenso de Cohen-Seidenberg: *Sea A un anillo íntegramente cerrado en su cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \Sigma'$ una extensión finita de cuerpos y A' una A-álgebra contenida en el cierre entero de A en Σ'. El morfismo $\operatorname{Spec} A' \to \operatorname{Spec} A$ es abierto y $A \hookrightarrow A'$ cumple el teorema del descenso de los ideales.*

Demostración. Sea Σ'' la envolvente normal de Σ' sobre Σ. Sea A'' el cierre entero de A en Σ''. Tenemos los morfismos

$$A \hookrightarrow A' \hookrightarrow A'', \quad \operatorname{Spec} A \leftarrow \operatorname{Spec} A' \leftarrow \operatorname{Spec} A''$$

Los morfismos inyectivos enteros, como los finitos, son epiyectivos en espectros. Por tanto, si $\operatorname{Spec} A'' \to \operatorname{Spec} A$ es abierto entonces $\operatorname{Spec} A' \to \operatorname{Spec} A$ es abierto. Igualmente, si $A \hookrightarrow A''$ cumple el teorema del descenso de ideales, entonces $A \hookrightarrow A'$ también. En conclusión, podemos suponer que $\Sigma \hookrightarrow \Sigma'$ es una extensión normal, digamos de grupo de automorfismos G, y que A' es al cierre entero de A en Σ'. Sea $\bar{A}$ el cierre entero de A en ${\Sigma'}^G$. Es fácil ver que $\bar{A} = {A'}^G$. Por la proposición 3.3.38, el teorema es cierto para el morfismo ${A'}^G \hookrightarrow A'$. Para concluir, basta demostrar el teorema para

$$\begin{array}{ccc} A & \longrightarrow & \bar{A} \\ \downarrow & & \downarrow \\ \Sigma & \longrightarrow & {\Sigma'}^G \end{array}$$

Basta probar que $\operatorname{Spec} \bar{A} \to \operatorname{Spec} A$ es biyectiva. Como $\Sigma \to {\Sigma'}^G$ es puramente inseparable, para todo $b \in {\Sigma'}^G$, existe $n \in \mathbb{N}$ tal que $b^{p^n} \in \Sigma$ (donde $0 < p = \operatorname{car} \Sigma$). Por tanto, para cada $b \in \bar{A}$, existe $n \in \mathbb{N}$ tal que $b^{p^n} \in A$ (pues b^{p^n} es entero sobre A). Entonces la aplicación $\operatorname{Spec} \bar{A} \to \operatorname{Spec} A$ es biyectiva, pues la aplicación $\operatorname{Spec} A \to \operatorname{Spec} \bar{A}$, $\mathfrak{p} \mapsto \mathfrak{p}'$, donde $\mathfrak{p}' := \{b \in \bar{A} : b^{p^n} \in \mathfrak{p} \text{ para algún } n\}$, es su inversa. □

40. Proposición: *Los morfismos de anillos planos $A \to B$ cumplen el teorema de descenso de ideales.*

Demostración. Sea $\mathfrak{p}_x \subset B$ un ideal primo, $\mathfrak{p}_y = \mathfrak{p}_x \cap A$ y $\mathfrak{p}_{y'} \subset \mathfrak{p}_y$ un ideal primo. El morfismo $A_y \to B_x$ es fielmente plano. Denotemos $f^* : \operatorname{Spec} B_x \to \operatorname{Spec} A_y$ el morfismo inducido en los espectros. Por la fórmula de la fibra $f^{*-1}(y') = \operatorname{Spec}(B_x/\mathfrak{p}_{y'}B_x)_{y'} \neq \emptyset$ porque $(B_x/\mathfrak{p}_{y'}B_x)_{y'} = A_{y'}/\mathfrak{p}_{y'}A_{y'} \otimes_{A_y} B_x \neq 0$. Por tanto, existe un ideal primo $\mathfrak{p}_{x'} \subset \mathfrak{p}_x$ tal que $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$. □

41. Proposición: *Sea $f : A \to B$ un morfismo de anillos, $\mathfrak{p}_x \subset B$ un ideal primo y $\mathfrak{p}_y := \mathfrak{p}_x \cap A$.*

1. *Si f cumple el teorema del descenso de ideales, entonces* $\dim B_x \geq \dim A_y$.
2. *Si f^* es un morfismo de fibras de dimensión cero, entonces* $\dim B_x \leq \dim A_y$.

Demostración. 1. Sea

$$\mathfrak{m}_y \supset \mathfrak{p}'_1 \supset \cdots \supset \mathfrak{p}'_n$$

una cadena estricta de ideales primos de A. Por el teorema del descenso podemos construir una cadena de ideales primos de B,

$$\mathfrak{m}_x \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_m,$$

tal que $\mathfrak{p}'_i = A \cap \mathfrak{p}_i$. Por tanto, $\dim B_x \geq \dim A_y$.

2. Toda cadena estricta de ideales primos de B,

$$\mathfrak{m}_x \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_m,$$

induce cortando con A, una cadena de ideales primos $\mathfrak{m}_y \supset A \cap \mathfrak{p}_1 \supset \cdots \supset A \cap \mathfrak{p}_m$ cuyas inclusiones son estrictas, pues las fibras de f^* son de dimensión cero. Por tanto, $\dim B_x \leq \dim A_y$. □

Como corolario obtenemos la siguiente proposición.

42. Proposición: *Sea $i : A \to B$ un morfismo entero e inyectivo de anillos. Sea $\mathfrak{p}_x \subset B$ un ideal primo y $\mathfrak{p}_y := \mathfrak{p}_x \cap A$. Si i es un morfismo plano, o A y B son anillos íntegros y A es íntegramente cerrado en su cuerpo de fracciones, entonces*

$$\dim B_x = \dim A_y.$$

3.4. Anillos de Dedekind

1. Teorema: *Sea $\mathcal{O}$ un anillo íntegro local noetheriano de dimensión* 1. *$\mathcal{O}$ es un dominio de ideales principales si y solo si es íntegramente cerrado en su cuerpo de fracciones* Σ.

Demostración. Los dominios de ideales principales son dominios de factorización única, luego íntegramente cerrados en su cuerpo de fracciones.

Probemos el recíproco. Sea f un elemento no nulo del ideal maximal $\mathfrak{m}$ de $\mathcal{O}$. $\mathcal{O}/f\mathcal{O}$ es un anillo local de dimensión cero. Por tanto, el ideal maximal $\mathfrak{m}$ en $\mathcal{O}/f\mathcal{O}$ es nilpotente. Es decir, existe un $n \in \mathbb{N}$ de modo que $\mathfrak{m}^n \subseteq f\mathcal{O}$. Sea $n \in \mathbb{N}$ mínimo verificando $\mathfrak{m}^n \subseteq f\mathcal{O}$. Sea $g \in \mathfrak{m}^{n-1}$ de modo que $g \notin f\mathcal{O}$. Basta probar que $\mathfrak{m} = \frac{f}{g} \cdot \mathcal{O}$, pues tendríamos que $\mathfrak{m}$ es un $\mathcal{O}$-módulo principal y $\mathcal{O}$ d.i.p. Basta probar, pues, que $\frac{g}{f} \cdot \mathfrak{m} = \mathcal{O}$. Se verifica que $\frac{g}{f} \cdot \mathfrak{m} \subseteq \frac{1}{f} \cdot \mathfrak{m}^n \subseteq \mathcal{O}$. Si $\frac{g}{f} \cdot \mathfrak{m} \neq \mathcal{O}$, tendremos que $\frac{g}{f} \cdot \mathfrak{m} \subseteq \mathfrak{m}$. Por tanto, $\frac{g}{f} \cdot$ es un endomorfismo de $\mathfrak{m}$, que ha de satisfacer el correspondiente polinomio característico. Luego $\frac{g}{f}$ es entero sobre $\mathcal{O}$, así pues $\frac{g}{f} \in \mathcal{O}$. Contradicción porque $g \notin f\mathcal{O}$.

□

2. Definición: Un anillo A íntegro se dice que es un dominio de Dedekind si es noetheriano de dimensión 1 e íntegramente cerrado en su cuerpo de fracciones.

3. Proposición: *Sea A un anillo íntegro, que no sea un cuerpo. A es un dominio de Dedekind si y solo si A_x es un dominio de ideales principales para todo punto cerrado* $x \in \operatorname{Spec} A$.

4. Teorema: *Si A es un dominio de Dedekind e $I \subseteq A$ un ideal no nulo, entonces I se escribe de modo único como producto de ideales primos.*

Demostración. Sean $\{x_1, \ldots, x_m\} = (I)_0$. Sabemos por la proposición anterior que A_{x_i} es un anillo de ideales principales. Por tanto, $I_{x_i} = \mathfrak{p}_{x_i}^{n_i} A_{x_i}$, para cierto $n_i \in \mathbb{N}$ único. El ideal

$$\mathfrak{p}_{x_1}^{n_1} \cdot \ldots \cdot \mathfrak{p}_{x_m}^{n_m}$$

es igual localmente a I, luego son iguales globalmente. Los exponentes n_i están determinados porque lo están al localizar. □

5. Teorema: *Sea A un dominio de integridad. Si todo ideal propio de A se escribe de modo único como producto de ideales primos (salvo ordenación de los factores) entonces A es un dominio de Dedekind.*

Demostración. Sea $\mathfrak{m}_x \subset A$ un ideal maximal. Por la unicidad $\mathfrak{m}_x^2 \neq \mathfrak{m}_x$. Sea $a \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$, es decir, $0 \neq \bar{a} \in \mathfrak{m}_x/\mathfrak{m}_x^2$. Observemos que $(\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x/\mathfrak{m}_x^2$, porque dado $s \in A \setminus \mathfrak{m}_x$, $\bar{s}$ es invertible en $A/\mathfrak{m}_x$ y el morfismo $s\cdot\colon \mathfrak{m}_x/\mathfrak{m}_x^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$, $\bar{m} \mapsto s \cdot \bar{m} = \overline{sm} = \bar{s} \cdot \bar{m}$ es isomorfismo. Por tanto, $0 \neq \bar{a} \in \mathfrak{m}_x/\mathfrak{m}_x^2 = (\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x$. Escribamos $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ como producto de ideales primos. Reordenando podemos suponer que $\mathfrak{p}_i \subseteq \mathfrak{m}_x$ si y sólo si $i \leq r$ (para cierto $r \leq n$). Localizando en x, tenemos que $a \cdot A_x = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot A_x \subseteq \mathfrak{m}_x^r A_x$, pero $a \notin \mathfrak{m}_x^2 A_x$, luego $r = 1$ y $a \cdot A_x = \mathfrak{p}_1 \cdot A_x$. Sea $b \in \mathfrak{m}_x$ tal que $b \notin aA_x$. Escribamos $(a,b) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ como producto de ideales primos. Reordenando podemos suponer que $\mathfrak{q}_i \subseteq \mathfrak{m}_x$ si y solo si $i \leq s$ (para cierto $s \leq n$). Localizando en x, tenemos que $(a,b) \cdot A_x = \mathfrak{q}_1 \cdots \mathfrak{q}_s \cdot A_x \subseteq \mathfrak{m}_x^s A_x$, pero $a \notin \mathfrak{m}_x^2 A_x$, luego $s = 1$ y $(a,b) \cdot A_x = \mathfrak{q}_1 \cdot A_x$ que es un ideal primo. Igualmente, $(a,b^2)A_x$ es un ideal primo y ha de coincidir con $(a,b)A_x$. Entonces, $(\bar{b}) = (\bar{b}^2)$ en el anillo íntegro A_x/aA_x, luego $\bar{b}$ es invertible, lo cual es contradictorio porque $A_x/(a,b)A_x$ es no nulo. En conclusión, $\mathfrak{m}_x A_x = aA_x$.

Dado un ideal primo $0 \neq \mathfrak{p} \subsetneq \mathfrak{m}_x$, tenemos que todos los elementos de $\mathfrak{p}A_x$ son multiplos de a y es fácil ver que $\mathfrak{p}A_x = a \cdot \mathfrak{p}A_x = \mathfrak{m}_x \mathfrak{p} A_x$, luego $\mathfrak{p} = \mathfrak{m}_x \mathfrak{p}$ (porque localmente son iguales) y llegamos a contradicción. Luego todos los ideales primos de A, no nulos, son maximales.

Sólo nos falta probar que A es noetheriano. Basta ver que $\mathfrak{m}_x$ es finito generado. Tenemos $(a) = \mathfrak{m}_x \cdot \mathfrak{m}_{x_2}^{n_2} \cdots \mathfrak{m}_{x_r}^{n_r}$ Sea $b \in A$ tal que su clase en $A/\mathfrak{m}_x \times A/\mathfrak{m}_{x_2} \times \cdots \times A/\mathfrak{m}_{x_r}$ sea igual a $(\bar{0}, \bar{1}, \ldots, \bar{1})$, entonces $\mathfrak{m}_x = (a,b)$, como se comprueba localmente.

□

Los anillos de Dedekind no son dominios de factorización única en general, aunque estos teoremas estén muy cerca de afirmarlo.

6. Breve reseña histórica: Kummer, para probar el teorema de Fermat, es decir, para demostrar que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras ($xyz \neq 0$) consideró la descomposición

$$x^n = z^n - y^n = (z - \xi^1 y) \cdots (z - \xi^n y),$$

siendo $\xi = e^{\frac{2\pi i}{n}}$ y trabajó con los números $\sum a_i \xi^i$, $a_i \in \mathbb{Z}$. Es decir, trabajó en el anillo (concepto general introducido más tarde por Dedekind) $\mathbb{Z}[\xi]$. Argumentando sobre la factorización única, probó que la descomposición anterior no es posible, con $x, y, z \in \mathbb{Z}$ no nulos. Dirichlet le hizo observar a Kummer el error (cometido también por Cauchy y Lamé) de suponer que todos los anillos considerados eran dominios de factorización única. Consideremos por sencillez el anillo de Kummer $\mathbb{Z}[\sqrt{-5}]$, tenemos dos descomposiciones en factores irreducibles $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Para restaurar la factorización única, Kummer introdujo los números ideales (no dio una definición general). Si bien $1 + \sqrt{-5}$ y 2 son irreducibles observemos que $(1 + \sqrt{-5})^2$

es múltiplo de 2. Es como si hubiese un m.c.d. "ideal" de 2 y $1+\sqrt{-5}$. En la extensión $\mathbb{Z}[\sqrt{-5}] \hookrightarrow \mathbb{Z}[(1+\sqrt{-5})/\sqrt{2}, \sqrt{2}]$ tenemos la factorización única por irreducibles $6 = \sqrt{2}^2 \cdot ((1+\sqrt{-5})/\sqrt{2}) \cdot (1-\sqrt{-5})/\sqrt{2}$ (si bien ya estamos en anillos de enteros que no son los de partida). Dedekind observó que lo que estaba definiendo Kummer era el concepto de ideal (recordemos que en los dominios de ideales principales $(a_1,\dots,a_n) = (m.c.d.(a_1,\dots,a_n))$, el concepto de ideal primo y que había probado que en tales anillos (dominios de Dedekind) todo ideal es producto de ideales primos. Hilbert (con las "torres de Hilbert") probó que todo anillo de enteros se mete en otro anillo mayor donde sus ideales se hacen principales.

7. Proposición : *Sea A un dominio de Dedekind y M un A-módulo finito generado. Entonces,*

$$M \simeq M/T(M) \oplus T(M).$$

Además, $M/T(M)$ es un A-módulo proyectivo y $T(M) \simeq \oplus_{i,j} A/\mathfrak{p}_{x_i}^{n_{ij}}$, con $x_i \in \mathrm{Spec}_{max} A$.

Demostración. $M/T(M)$ es un módulo proyectivo porque lo es localmente libre, ya que localmente es un módulo finito generado sin torsión sobre un dominio de ideales principales. Por tanto, el morfismo de paso al cociente $M \to M/T(M)$ tiene sección y $M \simeq M/T(M) \oplus T(M)$. El soporte de $T(M)$ es un número finito de puntos cerrados $\{x_1,\dots,x_n\}$, luego $T(M) = \oplus_i T(M)_{x_i} = \oplus_i T_{A_{x_i}}(M_{x_i})$ y $T_{A_{x_i}}(M_{x_i}) \simeq \oplus_j A_{x_i}/\mathfrak{p}_{x_i}^{n_{ij}} A_{x_i} = \oplus_j A/\mathfrak{p}_{x_i}^{n_{ij}}$. □

8. Proposición: *Sea A un dominio de Dedekind y M un A-módulo finito generado sin torsión. Entonces, M es suma directa de A-módulos proyectivos de rango* 1.

Demostración. Procedemos por inducción sobre el rango de M. Si el rango de M es 1 hemos terminado. Supongamos que el rango de M es $n > 1$. Sea $m \in M$ no nulo y consideremos el morfismo inyectivo $i\colon A \hookrightarrow M$, $a \mapsto a \cdot m$. $M/\mathrm{Im}\, i$ es suma directa de un A-módulo M' sin torsión de rango $n-1$ y $T(M/\mathrm{Im}\, i)$. Tenemos entonces un epimorfismo $\pi\colon M \to M'$, que tiene sección porque M' es proyectivo. Por tanto, $M \simeq \mathrm{Ker}\,\pi \oplus M'$. Hemos terminado porque M' y $\mathrm{Ker}\,\pi$ son suma directa de A-módulos proyectivos de rango 1, por la hipótesis de inducción. □

Veamos cómo son los módulos proyectivos de rango 1.

3.4.1. Ideales fraccionarios

Sea A un anillo íntegro de cuerpo de fracciones K.
Dados dos A-submódulos $I_1, I_2 \subseteq K$, se define

$$I_1 \cdot I_2 := \langle i_1 \cdot i_2, \forall i_1 \in I_1, \forall i_2 \in I_2 \rangle$$
$$[I_1 \colon I_2] := \{f \in K \colon f \cdot I_2 \subseteq I_1\}$$

que son A-submódulos de K. Observemos que

$$[I_1 : I_2 + I_3] = [I_1 : I_2] \cap [I_1 : I_3].$$

y si $I_2 \subseteq I_3$ entonces $[I_1 : I_2] \supseteq [I_1 : I_3]$.

9. Proposición: *Sean I, J dos A-submódulos de K y supongamos que J es un A-módulo finito generado. Sea $S \subset A$ un sistema multiplicativo, entonces*

$$[I : J]_S = [I_S : J_S].$$

Demostración. Escribamos $J = f_1 A + \cdots + f_r A_r$, con $f_i \in K$. Entonces,

$$[I : J]_S = (\cap_{i=1}^r [I : f_i A])_S = (\cap_{i=1}^r f_i^{-1} I)_S = \cap_{i=1}^r f_i^{-1} I_S = \cap_{i=1}^r [I_S : f_i A_S] = [I_S : J_S].$$

□

10. Definición: Llamemos ideal fraccionario de K a los A-submódulos no nulos finito generados de K. [2]

Todo módulo M finito generado sin torsión de rango 1 es isomorfo a un ideal fraccionario de K, ya que el morfismo de localización $M \hookrightarrow M_{A-\{0\}} \simeq K$ es inyectivo.

Supongamos que A es noetheriano, que I es un ideal fraccionario de K y que J es un A-submódulo no nulo de K. Dado $f \in J$ no nulo, observemos que $[I : J] \subset [I : fA] = f^{-1} I$ que es un A-módulo finito generado, luego $[I : J]$ es finito generado. En conclusión, la suma, producto y división de ideales fraccionarios es ideal fraccionario.

11. Ejemplo: Calculemos los ideales fraccionarios de $\mathbb{Q}$. Sea $I = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$ un ideal fraccionario de $\mathbb{Q}$. Sea $b = b_1 \cdots b_n$ entonces

$$I = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle = \langle \frac{a'_1}{b}, \ldots, \frac{a'_n}{b} \rangle = \frac{1}{b} \cdot \langle a'_1, \ldots, a'_n \rangle = \frac{1}{b} \cdot m.c.d.(a'_1, \ldots, a'_n) \cdot \mathbb{Z} = \frac{a}{b} \cdot \mathbb{Z}.$$

12. Proposición: *Dos ideales fraccionarios I, I' son isomorfos (como A-módulos) si y solo si existe $f \in K$ tal que $I' = f \cdot I$.*

Demostración. $\Rightarrow$) Dado un isomorfismo $I \simeq I'$, localizando por $A \setminus \{0\}$, obtenemos un isomorfismo de K-espacios vectoriales $K \simeq K$, que es multiplicar por una $f \in K$, luego $I' = f \cdot I$.

□

[2] Advertencia: los ideales fraccionarios de K no son ideales de K.

Por tanto, si $I_1 \simeq I_1'$ e $I_2 \simeq I_2'$ entonces $I_1 \cdot I_2 \simeq I_1' \cdot I_2'$.

13. Proposición: *La aplicación*

$$\{\textit{Ideales finito generados de } A\}/\simeq \longrightarrow \{\textit{Ideales fraccionarios de } K\}/\simeq,\ [\mathfrak{a}] \mapsto [\mathfrak{a}]$$

es un isomorfismo de semigrupos.

Demostración. Evidentemente la aplicación es inyectiva. Dado un ideal fraccionario I, existe $a \in A$ tal que $a \cdot I$ es un ideal de A, por tanto $[I] = [aI]$ y la aplicación es epiyectiva. □

14. Nota: A partir de ahora en esta subsección supondremos que A es un dominio de Dedekind y que K es el cuerpo de fracciones de A.

15. Proposición: *Sea A un domino de Dedekind de cuerpo de fracciones K y $I \subset K$ un ideal fraccionario. Entonces, $I \cdot [A : I] = A$ y por tanto el conjunto de ideales fraccionarios de K es un grupo.*

Demostración. Basta probar que $I_x \cdot [A_x : I_x] = A_x$ para todo $x \in \operatorname{Spec}_{max} A$. Podemos suponer que A es un dominio de ideales principales local y tenemos que probar que $I \cdot [A : I] = A$. I es un A-módulo finito generado sin torsión de rango 1 (porque $I_{A\setminus\{0\}} = K$), luego es libre de rango 1, es decir $I = f \cdot A$. Entonces, $I \cdot [A : I] = fA \cdot f^{-1}A = A$. □

Dado un ideal fraccionario I, denotemos $I^{-1} = [A : I]$, que es el inverso de I. Obviamente, $I^{-n} := I^{-1} \overset{n}{\cdots} I^{-1}$ es igual a $[A : I^n]$, para todo $n > 0$, pues ambos son el inverso de I^n. Observemos que

$$(\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m}) \cdot (\mathfrak{m}_{x_1}^{n_1'} \cdots \mathfrak{m}_{x_m}^{n_m'}) = \mathfrak{m}_{x_1}^{n_1+n_1'} \cdots \mathfrak{m}_{x_m}^{n_m+n_m'},\ \text{para todo } n_i, n_i' \in \mathbb{Z}.$$

16. Proposición: *Sea I un ideal fraccionario de K. Existen ciertos $x_1, \ldots, x_m \in \operatorname{Spec} A$ distintos (y únicos) y ciertos $n_1, \ldots, n_m \in \mathbb{Z}$ no nulos (únicos), de modo que*

$$I = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m}.$$

Demostración. Sea $a \in A$ tal que $a \cdot I$ sea un ideal de A. Por el teorema 3.4.4, $(a) = \mathfrak{m}_{x_1}^{r_1} \cdots \mathfrak{m}_{x_m}^{r_m}$ y $a \cdot I = \mathfrak{m}_{x_1}^{s_1} \cdots \mathfrak{m}_{x_m}^{s_m}$, con $r_i, s_i \geq 0$. Por tanto,

$$I = (a)^{-1} \cdot aI = \mathfrak{m}_{x_1}^{-r_1} \cdots \mathfrak{m}_{x_m}^{-r_m} \cdot \mathfrak{m}_{x_1}^{s_1} \cdots \mathfrak{m}_{x_m}^{s_m} = \mathfrak{m}_{x_1}^{s_1-r_1} \cdots \mathfrak{m}_{x_m}^{s_m-r_m}.$$

Supongamos $\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m} = \mathfrak{m}_{x_1}^{n_1'} \cdots \mathfrak{m}_{x_m}^{n_m'}$, con $n_i, n_i' \in \mathbb{Z}$. Reordenando, podemos suponer que $n_i \geq n_i'$ si y solo si $1 \leq i < s$. Entonces, $\mathfrak{m}_{x_1}^{n_1-n_1'} \cdots \mathfrak{m}_{x_{s-1}}^{n_{s-1}-n_{s-1}'} = \mathfrak{m}_{x_s}^{n_s'-n_s} \cdots \mathfrak{m}_{x_m}^{n_m'-n_m}$, y por el teorema 3.4.4, $n_j - n_j' = 0$ para todo j.

□

17. Definición: El grupo de Picard de A, que denotaremos $\mathrm{Pic}\,A$, es el grupo de las clases de isomorfía de los ideales no nulos de A.

18. Proposición: $\mathrm{Pic}\,A = \{1\}$ *si y solo si* A *es un dominio de ideales principales.*

Demostración. $\Rightarrow$) Dado un ideal no nulo $I \subseteq A$, tenemos que $[I] = [A]$, es decir, I es isomorfo a A, luego existe $f \in K$ tal que $I = f\cdot$, luego I es principal.

$\Leftarrow$) Si todo ideal es principal, entonces todo ideal es isomorfo a A, luego $\mathrm{Pic}\,A = \{1\}$. □

3.4.2. Anillos de enteros y de curvas íntegras

19. Definición: Diremos que un cuerpo es un cuerpo de números algebraicos si es una extensión finita de cuerpos de $\mathbb{Q}$. Diremos que un anillo íntegro A es un anillo enteros si el morfismo $\mathbb{Z} \hookrightarrow A$ es inyectivo y finito.

20. Ejemplos: $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$ y $\mathbb{Z}[\sqrt{-5}, \sqrt[7]{3}]$ son anillos de números enteros.

21. Teorema: *Sea* A *un anillo de enteros de cuerpo de fracciones* Σ *y* $\bar{\Sigma}$ *una extensión finita de cuerpos de* Σ*. Entonces, el cierre entero de* A *en* $\bar{\Sigma}$*,* $\bar{A}$*, es un anillo de enteros de cuerpo de fracciones* $\bar{\Sigma}$ *y el morfismo* $A \to \bar{A}$ *es finito.*

Demostración. El morfismo $\mathbb{Z} \hookrightarrow A$ es finito, localizando en $S := \mathbb{Z}\backslash 0$, tenemos que A_S es una $\mathbb{Q}$-álgebra finita íntegra, luego es cuerpo. Por tanto, $A_S = \Sigma$, el morfismo $\mathbb{Q} \hookrightarrow \Sigma$ es finito. Además, el cierre entero de A en $\bar{\Sigma}$ coincide con el cierre entero de $\mathbb{Z}$ en $\bar{\Sigma}$. Por la proposición 3.3.15, $\bar{A}$ es una $\mathbb{Z}$-álgebra finita, luego es un anillo de enteros, de cuerpo de fracciones $\bar{\Sigma}$. En particular, $A \to \bar{A}$ es un morfismo finito. □

22. Definición: Dado un cuerpo de números K, diremos que el cierre entero de $\mathbb{Z}$ en K es el anillo de enteros de K.

23. Proposición: *Sea* K *un cuerpo de números. Un elemento* $a \in K$ *es entero (sobre* $\mathbb{Z}$*) si y solo si el polinomio característico del endomorfismo* $\mathbb{Q}$*-lineal* $a\cdot\colon K \to K$*,* $b \mapsto a \cdot b$ *es un polinomio con coeficientes enteros*

Demostración. $\Leftarrow$) Es evidente.

$\Rightarrow$) Sea $\{a_1, \ldots, a_n\}$ una base del $\mathbb{Q}$-espacio vectorial K, con $a = a_1$. Multiplicando cada a_i, para $i \geq 2$, por ciertos números enteros podemos suponer que los polinomios característicos de los a_i son polinomios con coeficientes enteros, luego podemos suponer que la base está formada por elementos enteros. $A = \mathbb{Z}[a_1, \ldots, a_n]$ es un anillo de enteros de K y es un $\mathbb{Z}$-módulo libre de rango n. Consideremos una base del $\mathbb{Z}$-módulo

A (que es una base del $\mathbb{Q}$-espacio vectorial K). En esta base la matriz del endomorfismo $a\cdot\colon K \to K$ es una matriz con coeficientes enteros, luego el polinomio característico de $a\cdot$ es un polinomio con coeficientes enteros.

□

24. Ejemplo: Probemos que $\mathbb{Z}[\sqrt{-5}]$ es un anillo de Dedekind. Calculemos los elementos $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ enteros sobre $\mathbb{Z}$. La matriz de $(a + b\sqrt{-5})\cdot\colon \mathbb{Q}[\sqrt{-5}] \to \mathbb{Q}[\sqrt{-5}]$ en la base $\{1, \sqrt{-5}\}$ es igual a

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}$$

y su polinomio característico es igual a $x^2 - 2ax + (5b^2 + a^2)$, luego $2a, 5b^2 + a^2 \in \mathbb{Z}$. Si a es entero, entonces b es es entero. Si a no es entero, entonces $a = \frac{n}{2}$ con n impar, luego $b = \frac{m}{2}$ con m impar y $5m^2 + n^2 = \dot{4}$, luego $0 = \overline{5m^2 + n^2} = \overline{1 \cdot 1 + 1} = \bar{2}$ en $\mathbb{Z}/4\mathbb{Z}$, y hemos llegado a contradicción. En conclusión, $\mathbb{Z}[\sqrt{-5}] = \overline{\mathbb{Z}[\sqrt{-5}]}$ y es de Dedekind.

25. Definición: Sea A un anillo íntegro de dimensión de Krull 1. Diremos que un punto cerrado $x \in \operatorname{Spec} A$ es no singular si A_x es d.i.p.; diremos que es singular si A_x no es d.i.p.

Por tanto, A será un dominio de Dedekind si y solo si no tiene puntos singulares.

26. Definición: Diremos que $\operatorname{Spec} A$ es una curva algebraica íntegra (afín) si A es una k-álgebra de tipo finito íntegra y de dimensión de Krull 1. Diremos que una curva íntegra es no singular si no tiene puntos singulares.

27. Ejemplos: La recta afín $\mathbb{A}^1 = \operatorname{Spec} k[x]$, la circunferencia $\operatorname{Spec} k[x,y]/(x^2 + y^2 - 1)$, el nodo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3)$ y la cúspide $\operatorname{Spec} k[x,y]/(y^2 - x^3)$ son curvas íntegras afines.

28. Teorema: *Sea A el anillo de una curva afín íntegra (resp. un anillo de enteros). Sea Σ el cuerpo de fracciones de A, $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces,*

1. *$\bar{A}$, es el anillo de una curva afín íntegra (resp. un anillo de enteros) no singular de cuerpo de fracciones $\bar{\Sigma}$ y el morfismo $A \to \bar{A}$ es finito.*
2. *Si $\bar{\Sigma} = \Sigma$, dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to \bar{A}_x$ es isomorfismo si y solo si x es no singular. Además, el conjunto de puntos singulares de A es un conjunto finito de puntos cerrados de $\operatorname{Spec} A$. "Diremos que $A \to \bar{A}$ es el morfismo de desingularización y que $\bar{A}$ es la desingularización de A".*

Demostración. 1. Es consecuencia de 3.3.17 (resp. de 3.4.21).

2. $\bar{A}$ es un A-módulo finito generado, de cuerpo de fracciones Σ, luego $\bar{A}/A$ es un A-módulo finito generado cuyo soporte es un número finito de puntos cerrados (pues se anula en el punto genérico). Basta ver entonces que el soporte de $\bar{A}/A$ son los puntos singulares de $\operatorname{Spec} A$.

Si x es un punto no singular, entonces A_x es local y regular de dimensión 1, luego íntegramente cerrado. Por tanto, $A_x = \bar{A}_x$. Recíprocamente, si $A_x = \bar{A}_x$, entonces A_x es íntegramente cerrado, pues lo es $\bar{A}$ y por tanto $\bar{A}_x$ (por 3.3.14).

□

3.4.3. Fibras de un morfismo finito

Conviene que el lector lea la definición 0.6.71.

29. Definición: Sea $A \to B$ un morfismo finito y sea $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido. Sea $y \in \operatorname{Spec} B$ y $x := f(y)$.

1. Diremos que $\dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x$ es el número de puntos (contando multiplicidades y grados sobre x) de la fibra de x por el morfismo f.
2. Diremos que $m_y := l_B(B_y/\mathfrak{p}_x B_y)$ es la multiplicidad con la que aparece y en la fibra de x.
3. Diremos que $\operatorname{gr}_x y := \dim_{A_x/\mathfrak{p}_x A_x} B_y/\mathfrak{p}_y B_y$ es el grado de y sobre x.

Esta definición viene justificada por la igualdad,

$$\text{Nº de puntos contando mult. y grd. de } f^{-1}(x) = \dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x$$
$$= \sum_{y \in f^{-1}(x)} l_{A_x}(B_x/\mathfrak{p}_x B_x)_y = \sum_{y \in f^{-1}(x)} l_{B_y}(B_y/\mathfrak{p}_x B_y) \cdot \operatorname{gr}_x y = \sum_{y \in f^{-1}(x)} m_y \cdot \operatorname{gr}_x y$$

30. Teorema: *Sea A un dominio de Dedekind, B un anillo íntegro y $A \hookrightarrow B$ un morfismo finito inyectivo. El número de puntos de las fibras de* $\operatorname{Spec} B \to \operatorname{Spec} A$*, contando multiplicidades y grados, es igual a* $\dim_{\Sigma_A} \Sigma_B$ *(donde Σ_A y Σ_B son los cuerpos de fracciones de A y B).*

Demostración. Sea $x \in \operatorname{Spec} A$ un punto cerrado. B_x es un A_x-módulo finito generado sin torsión y A_x es un dominio de ideales principales. Por tanto, $B_x = A_x^n$. Observemos que $B_{A\setminus\{0\}}$ es una $\Sigma_A = A_{A\setminus\{0\}}$-álgebra finita íntegra, luego es un cuerpo y ha de coincidir con Σ_B. Localizando $B_x = A_x^n$ por $A\setminus\{0\}$, tenemos que $\Sigma_B = \Sigma_A^n$, luego $n = \dim_{\Sigma_A} \Sigma_B$. Además,

$$n = \dim_{A/\mathfrak{m}_x}(A_x^n/\mathfrak{m}_x A_x^n) = \dim_{A/\mathfrak{m}_x}(B_x/\mathfrak{m}_x B_x).$$

□

31. Definición: Sea $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ un morfismo finito. Sea $y \in \operatorname{Spec} B$ un punto cerrado e $x = \pi(y)$. Diremos que π ramifica en y si $B_y/\mathfrak{m}_x B_y$ no es una $A/\mathfrak{m}_x$-álgebra separable; y en este caso se dice que y es un punto de ramificación de π y que x es un punto rama de π.

Observemos que y no es un punto de ramificación si y solo si $B_y/\mathfrak{m}_x B_y$ es un cuerpo y es una extensión $A/\mathfrak{m}_x$-separable. Por tanto, si y no es un punto de ramificación la multiplicidad con la que aparece y en la fibra de x es igual a 1. $B/\mathfrak{m}_x B$ es una $A/\mathfrak{m}_x$-álgebra finita, luego

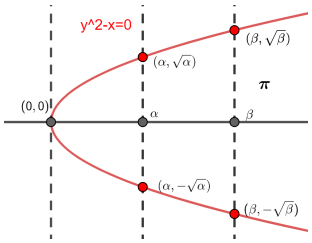
$$B/\mathfrak{m}_x B = \prod_{y \in \operatorname{Spec} B/\mathfrak{m}_x B} (B/\mathfrak{m}_x B)_y = \prod_{y \in \pi^{-1}(x)} B_y/\mathfrak{m}_x B_y$$

y no es separable si y solo si alguno de los $B_y/\mathfrak{m}_x B_y$ no es separable. Por tanto,

$$\pi(\{\text{Puntos de ramificación de } \pi\}) = \{\text{Puntos rama de } \pi\}.$$

32. Ejemplo: Consideremos el morfismo finito e inyectivo

$$\mathbb{C}[x] \to \mathbb{C}[x,y]/(y^2 - x), \quad p(x) \mapsto \overline{p(x)}.$$



Sea $\pi\colon \operatorname{Spec}\mathbb{C}[x,y]/(y^2 - x) \to \operatorname{Spec}\mathbb{C}[x]$, $(\alpha,\beta) \mapsto \alpha$ el morfismo inducido. Calculemos los puntos rama y los puntos de ramificación de π. Dado $\alpha \in \operatorname{Spec}_{max}\mathbb{C}[x]$, tenemos que $\pi^{-1}(\alpha) = \operatorname{Spec}\mathbb{C}[x,y]/(x-\alpha, y^2 - x) = \operatorname{Spec}\mathbb{C}[y]/(y^2 - \alpha)$ y $\mathbb{C}[y]/(y^2 - \alpha)$ es una $\mathbb{C}$-álgebra finita separable si y solo si $\alpha \neq 0$. Por tanto, α es un punto rama si y solo si $\alpha \neq 0$. Observemos que $\pi^{-1}(0) = \{(0,0)\}$ y que $(\mathbb{C}[y]/(y^2))_{(0,0)} = \mathbb{C}[y]/(y^2)$ no es una $\mathbb{C}$-álgebra finita separable. Por tanto, $(0,0)$ es el único punto de ramificación de π.

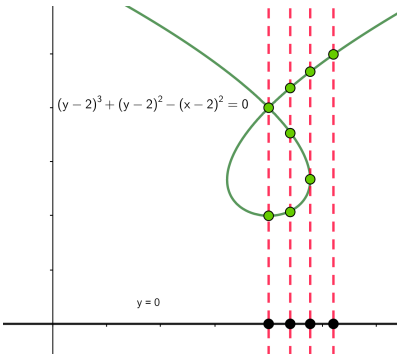
33. Ejercicio: Consideremos el morfismo

$$\begin{array}{ccc} \mathbb{C}[x] & \to & \mathbb{C}[x,y]/((y-2)^3 + (y-2)^2 - (x-2)^2) \\ p(x) & \mapsto & \overline{p(x)} \end{array}$$

y el morfismo inducido

$$\begin{array}{ccc} \operatorname{Spec}\mathbb{C}[x,y]/((y-2)^3 + (y-2)^2 - (x-2)^2) & \xrightarrow{\pi} & \operatorname{Spec}\mathbb{C}[x] \\ (\alpha,\beta) & \mapsto & \alpha \end{array}$$

Calcula los puntos rama y de ramificación de π.



34. Proposición: *Sea A un anillo íntegro de cuerpo de fracciones Σ. Sea $p(x) \in A[x]$ un polinomio mónico separable y sea $0 \neq \Delta \in A$ el discriminante de $p(x)$. Consideremos el morfismo finito $A \hookrightarrow A[x]/(p(x))$ y el morfismo inducido $\pi\colon \operatorname{Spec} A[x]/(p(x)) \to \operatorname{Spec} A$. Entonces,*

$$\{\textit{Puntos rama de } \pi\} = (\Delta)_0 \cap \operatorname{Spec}_{max} A.$$

Demostración. El punto z es un punto rama si y solo $(A[x]/(p(x)))/\mathfrak{p}_z = A/\mathfrak{p}_z[x]/(\overline{p(x)})$ no es una $A/\mathfrak{p}_z$-álgebra separable, es decir, $\overline{p(x)} \in A/\mathfrak{p}_z[x]$ no es separable, que equivale a decir que el discriminante de $\overline{p(x)}$ es nulo, o equivalentemente $\bar{\Delta} = 0$ en $A/\mathfrak{p}_z$, es decir, $z \in (\Delta)_0$. □

35. Definición: Sea $\phi\colon A \to B$ un morfismo finito entre dominios de Dedekind. Sea $\mathfrak{m}_y$ un ideal maximal de B y $\mathfrak{m}_x = \mathfrak{m}_y \cap B$. Entonces $\mathfrak{m}_x B_y = \mathfrak{m}_y^{e_y} B_y$, para cierto $e_y \in \mathbb{N}$, que llamaremos índice de ramificación de y.

36. Teorema: *Sea $\phi\colon A \to B$ un morfismo finito entre dominios de Dedekind. Sea $\mathfrak{m}_x \subset A$ un ideal maximal e y un punto en la fibra de x. La multiplicidad con la que aparece y en la fibra de x es igual al índice de ramificación de y.*

Demostración. Se deduce de las igualdades

$$l_{B_y}(B/\mathfrak{m}_x B)_y = l_{B_y}(B/\mathfrak{m}_y^{e_y}) = \sum_{j=0}^{e_y - 1} l_{B_y}(\mathfrak{m}_y^j/\mathfrak{m}_y^{j+1}) = e_y,$$

donde la última igualdad es por ser $\mathfrak{m}_y B_y$ principal.

□

37. Proposición: *Sea $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ un morfismo finito. Sea $y \in \operatorname{Spec} B$ un punto cerrado y $x = \pi(y)$. Si A_x es un anillo de ideales principales y la multiplicidad con la que aparece y en la fibra de x es 1, entonces B_y es un anillo de ideales principales.*

Demostración. B_y es un anillo noetheriano porque B_x lo es, ya que es un A_x-módulo finito generado. Tenemos que $\mathfrak{m}_x B_y = \mathfrak{m}_y B_y$, luego $\mathfrak{m}_y B_y = (t)$ es principal. Por el lema de Nakayama, dados $b_1, b_2 \in B_y$, no nulos, si $(b_1) = \mathfrak{m}_y(b_2)$ entonces $(b_1) \subsetneq (b_2)$. Dado $b_1 \in B_y$, no nulo, si no es invertible entonces $b_1 = t \cdot b_2$. Si b_2 no es invertible entonces $b_2 = t \cdot b_3$. Este proceso ha de terminar porque la cadena $(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \cdots$ ha de ser finita. Por tanto, $b_1 = t^n \cdot inv$. Ahora es fácil probar que todo ideal de B_y es principal. □

38. Corolario: *Sea $A \hookrightarrow B$ un morfismo de anillos finito entre anillos íntegros y sea $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido en espectros. Si A es un dominio de Dedekind, entonces*

$$\{\textit{Ptos. singulares de } \operatorname{Spec} B\} \subseteq \{\textit{Ptos. de ramificación de } \pi\} \subseteq \pi^{-1}(\{\textit{Ptos. rama de } \pi\}).$$

39. Ejemplo: Calculemos los puntos singulares de $\operatorname{Spec} \mathbb{Q}[x,y]/(y^2-x^3)$. Consideremos el morfismo finito $\mathbb{Q}[x] \hookrightarrow \mathbb{Q}[x,y]/(y^2-x^3)$, $p(x) \mapsto \overline{p(x)}$ y el morfismo inducido $\pi\colon \operatorname{Spec} \mathbb{Q}[x,y]/(y^2-x^3) \to \operatorname{Spec} \mathbb{Q}[x]$. Dado un ideal primo $\mathfrak{m}_z = (p(x))$ de $\mathbb{Q}[x]$, se tiene que $\pi^{-1}(z) = \mathbb{Q}(z)[y]/(y^2-x^3)$ (donde $\mathbb{Q}(z) := \mathbb{Q}[x]/(p(x))$), que es una $\mathbb{Q}(z)$-álgebra separable para todo z, salvo para $\mathfrak{m}_z = (x)$. Por tanto, el único punto posiblemente singular es o, con $\mathfrak{m}_o = (\bar{x}, \bar{y})$. Ahora bien, o es singular porque $\mathfrak{m}_o/\mathfrak{m}_o^2 = (\bar{x}, \bar{y})$ no es principal, luego por Nakayama $\mathfrak{m}_o \cdot \mathbb{Q}[x,y]/(y^2-x^3)$ no es principal.

40. Ejemplo: Sea $\xi_m = e^{2\pi i/m} \in \mathbb{C}$. Veamos que $\mathbb{Z}[\xi_m]$ es de Dedekind. Consideremos el morfismo finito $\mathbb{Z} \hookrightarrow \mathbb{Z}[\xi] = \mathbb{Z}[x]/(\Phi_m(x))$. Supongamos $m = p^n$, con p primo. El polinomio mínimo anulador de ξ_{p^n}, $\Phi_{p^n}(x)$, que divide a $x^{p^n}-1$, es separable módulo todo primo $q \neq p$. Por tanto, si $\mathfrak{m}_y \subset \mathbb{Z}[\xi_m]$, cumple que $\mathfrak{m}_y \cap \mathbb{Z} = (q)$, tenemos que $\mathfrak{m}_y \cdot \mathbb{Z}[\xi_{p^n}]_y = (q)$, para $q \neq p$. El único punto singular posible de $\operatorname{Spec} \mathbb{Z}[\xi_{p^n}] = \operatorname{Spec} \mathbb{Z}[x]/(\Phi_{p^n}(x))$, es $\mathfrak{m}_y = (p, \bar{x}-1)$. Observemos que

$$\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}}) = (x^{p^{n-1}})^{p-1} + \cdots + x^{p^{n-1}} + 1$$

Por tanto, $\mathbb{Z}[x]/(\Phi_{p^n}(x), x-1) = \mathbb{Z}/(p)$ y $(p, \bar{x}-1) = (\bar{x}-1)$. Luego, y es no singular.

Escribamos ahora, $m = p^n \cdot m'$, con m' primo con p. Por inducción, podemos suponer que $\mathbb{Z}[\xi_{m'}]$ es no singular al localizar en todo punto. Observemos que $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{m'}] \otimes_{\mathbb{Z}} \mathbb{Z}[\xi_{p^n}]$. Observemos que ξ_{p^n} es separable en fibras sobre $\mathbb{Z}[\xi_{m'}]$, salvo quizás en los puntos $y \in \operatorname{Spec} \mathbb{Z}[\xi_{m'}]$ tales que $\mathfrak{m}_y \cap \mathbb{Z} = (p)$. Luego, los únicos puntos singulares posibles de $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{m'}, \xi_{p^n}]$ son de la forma $\mathfrak{m}_{y'} = (\mathfrak{m}_y, \xi_{p^n}-1)$ (donde $\mathfrak{m}_y \cap \mathbb{Z} = (p)$). Ahora bien, $\mathfrak{m}_y \mathbb{Z}[\xi_{m'}]_y = (p)$. Luego, $\mathfrak{m}_{y'} \cdot \mathbb{Z}[\xi_m]_{y'} = (p, \xi_{p^n}-1) = (\xi_{p^n}-1)$, e y' es no singular.

Criterio diferencial de singularidad

41. Proposición: *Sea A un anillo íntegro noetheriano. A es un dominio de Dedekind si y solo si para todo ideal primo maximal $\mathfrak{m}_x$, se cumple que* $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$.

Demostración. Si A es un dominio de Dedekind, por la proposición 3.4.3 $\mathfrak{m}_x A_x = (t)$, luego $(\bar{t}) = \mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x = (\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x/\mathfrak{m}_x^2$ y $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$. Recíprocamente, si $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$ entonces $\mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x = (\bar{t})$ y por el lema de Nakayama $\mathfrak{m}_x A_x = (t)$. Entonces A_x es d.i.p., y por la proposición 3.4.3 A es un dominio de Dedekind. □

42. Definición: Dado un ideal maximal $\mathfrak{m}_x \subset A$ y $f \in \mathfrak{m}_x$, denotaremos $d_x f := \bar{f} \in \mathfrak{m}_x/\mathfrak{m}_x^2$. Si A es una k-álgebra y $A/\mathfrak{m}_x = k$, denotaremos $f(x) := \bar{f} \in A/\mathfrak{m}_x = k$ y $d_x f := \overline{f - f(x)} \in \mathfrak{m}_x/\mathfrak{m}_x^2$. Se dice que $d_x f$ es la diferencial de f en x y que $\mathfrak{m}_x/\mathfrak{m}_x^2$ es el módulo de las diferenciales en x.

43. Ejemplo: Sea $\mathfrak{m}_\alpha := (x_1-\alpha_1,\dots,x_n-\alpha_n) \subset k[x_1,\dots,x_n]$ y $p(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$. Entonces, $p(x_1,\dots,x_n) = p(\alpha) + \sum_i \frac{\partial p}{\partial x_i}(\alpha)(x_i-\alpha_i) + \sum_{ij}(x_i-\alpha_i)(x-\alpha_j)\cdot h_{ij}(x)$. Por tanto,

$$d_\alpha p(x_1,\dots,x_n) = \frac{\partial p}{\partial x_1}(\alpha) d_\alpha x_1 + \cdots + \frac{\partial p}{\partial x_n}(\alpha) d_\alpha x_n$$

y $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$ es un k-espacio vectorial de base $\{d_\alpha x_i = \overline{x_i - \alpha_i}\}$.

44. Proposición: *Sea $\mathfrak{m}_x \subset A$ un ideal maximal. Sea $I = (f_1,\dots,f_n) \subset A$ un ideal incluido en $\mathfrak{m}_x$ y sea $\bar{\mathfrak{m}}_x \subset A/I$ el ideal de las clases de $\mathfrak{m}_x$. Se cumple que*

$$\bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\langle d_x f_1,\dots,d_x f_n\rangle.$$

Demostración. Observemos que $\bar{\mathfrak{m}}_x = \mathfrak{m}_x/I$. Por tanto,

$$\bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \mathfrak{m}_x/(I+\mathfrak{m}_x^2) = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\bar{I} = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\langle d_x f_1,\dots,d_x f_n\rangle.$$

□

45. Ejemplo: Sea $p(x,y) \in \mathbb{C}[x,y]$ y $(\alpha,\beta) \in \mathbb{C}^2$ tal que $p(\alpha,\beta) = 0$, entonces $(\alpha,\beta) \in \mathrm{Spec}_{max}\,\mathbb{C}[x,y]/(p(x,y))$.

Denotemos la imagen de $\mathfrak{m}_{(\alpha,\beta)}$ en $\mathbb{C}[x,y]/(p(x,y))$, $\bar{\mathfrak{m}}_{(\alpha,\beta)}$. Como

$$\bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = (\mathfrak{m}_{(\alpha,\beta)}/\mathfrak{m}_{(\alpha,\beta)}^2)/(d_{(\alpha,\beta)}p(x,y)),$$

$\dim \bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = 1$ si y solo si $d_{(\alpha,\beta)}p(x,y) \neq 0$.

Luego, $\mathcal{O} = (\mathbb{C}[x,y]/(p(x,y)))_{(\alpha,\beta)}$ es un dominio de ideales principales si y solo si $d_{(\alpha,\beta)}p(x,y) \neq 0$. Por ejemplo, si $\frac{\partial p}{\partial y}(\alpha,\beta) \neq 0$, entonces $\bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = (d_{(\alpha,\beta)}x)$, luego $\bar{\mathfrak{m}}_{(\alpha,\beta)}\cdot\mathcal{O} = (x-\alpha)$.

46. Ejemplo: $\mathrm{Spec}\,\mathbb{C}[x,y]/(y^2-x^3)$ tiene un único punto singular: el origen. En efecto, $0 = d_{(\alpha,\beta)}(y^2-x^3) = -3\alpha^2 d_{(\alpha,\beta)}x + 2\beta d_{(\alpha,\beta)}y$ si y solo si $(\alpha,\beta) = (0,0)$.

3.5. Dimensión en variedades algebraicas

1. Teorema: *La dimensión de Krull de $k[x_1,\dots,x_n]$ es n.*

Demostración. Procedamos por inducción sobre n. El caso $n=1$ es obvio.
Sea

$$0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$$

una cadena de ideales primos de $k[x_1,\dots,x_n]$. Sea $p \in \mathfrak{p}_1$, no nulo e irreducible. Como $k[x_1,\dots,x_n]$ es un dominio de factorización única, el ideal (p) es un ideal primo. Si $(p) \neq \mathfrak{p}_1$, lo añadimos a la cadena anterior, con lo que podemos suponer que $(p) = \mathfrak{p}_1$. Por el lema de normalización de Noether y la observación 3.3.25, existe un morfismo finito inyectivo $k[x_1,\dots,x_r] \hookrightarrow k[x_1,\dots,x_n]/(p)$, con $r < n$. Por inducción sobre n, la dimensión de Krull de $k[x_1,\dots,x_r]$ es r, luego las cadenas de ideales primos en $k[x_1,\dots,x_n]/(p)$ son de longitud menor o igual que $n-1$. Haciendo cociente por (p), la cadena anterior define una cadena de ideales primos

$$\bar{0} \subset \bar{\mathfrak{p}}_2 \subset \cdots \subset \bar{\mathfrak{p}}_m$$

luego $m-1 \leq n-1$ y $\dim k[x_1,\dots,x_n] \leq n$. Por otra parte,

$$0 \subset (x_1) \subset (x_1,x_2) \subset \cdots \subset (x_1,\dots,x_n)$$

es una cadena de longitud n, luego $\dim k[x_1,\dots,x_n] \geq n$. En conclusión $k[x_1,\dots,x_n]$ tiene dimensión de Krull n. □

2. Teorema: *Sea A una k-álgebra de tipo finito íntegra. La dimensión de Krull de A coincide con el grado de trascendencia de su cuerpo de fracciones.*

Demostración. Por el lema de normalización de Noether, existe un morfismo finito inyectivo $k[x_1,\dots,x_n] \hookrightarrow A$, que induce un morfismo finito entre sus cuerpos de fracciones (pruébese)

$$k(x_1,\dots,x_n) \hookrightarrow \Sigma$$

Luego

$$\dim A \overset{3.3.37}{=} \dim k[x_1,\dots,x_n] = n = \operatorname{grtr} k(x_1,\dots,x_n) = \operatorname{grtr} \Sigma.$$

□

3. Proposición: *Sea X una variedad algebraica afín irreducible y $U \subset X$ un abierto no vacío. Entonces,* $\dim U = \dim X$.

Demostración. Si $V \subset V'$ es una inclusión de abiertos, entonces $\dim V \leq \dim V'$. Podemos suponer que $X = \operatorname{Spec} A$ es una variedad íntegra. Sea $U_a \subset U$ un abierto básico, no vacío. La dimensión de $U_a = \operatorname{Spec} A_a$ coincide con la de $X = \operatorname{Spec} A$, porque el cuerpo de fracciones de A_a es igual al de A. Como $\dim U_a \leq \dim U \leq \dim X$, todos los $\leq$ son igualdades. □

En general, toda variedad algebraica es unión de variedades algebraicas irreducibles y la dimensión de la variedad es el máximo de las dimensiones de sus componentes irreducibles. Observemos que $\dim A = \dim A_{\mathrm{red}}$. Por tanto, la dimensión de una variedad irreducible $\operatorname{Spec} A$ coincide con la dimensión de $\operatorname{Spec} A_{\mathrm{red}}$, que es una variedad algebraica íntegra.

4. Proposición : *Sean $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $X \times_k Y := \operatorname{Spec} A \otimes_k B$ variedades algebraicas. Se cumple que*

$$\dim(X \times_k Y) = \dim X + \dim Y$$

Demostración. Sean $f\colon k[x_1,\dots,x_n] \hookrightarrow A$, $g\colon k[y_1,\dots,y_m] \hookrightarrow B$ morfismos finitos inyectivos, entonces $k[x_1,\dots,x_n] \otimes k[y_1,\dots,y_m] \to A \otimes B$, $p(x) \otimes q(y) \mapsto f(p(x)) \otimes g(q(y))$ es un morfismo inyectivo finito y

$$\dim X + dim Y = n + m = \dim X \times Y.$$

□

5. Proposición: *Sea $f : X \to Y$ un morfismo entre variedades algebraicas. Sea $C \subset X$ un cerrado. Demuestra que*

$$\dim C \geq \dim \overline{f(C)}$$

Demostración. Podemos suponer que C es irreducible. Denotemos $X = \operatorname{Spec} B$, $C = (\mathfrak{p})_0 = \operatorname{Spec} B/\mathfrak{p}$, $Y = \operatorname{Spec} A$ y $\phi\colon A \to B$ el morfismo de k-álgebras tal que $\phi^* = f$. Entonces, el morfismo $A/\phi^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p}$ es inyectivo y $\overline{f(C)} = (\phi^{-1}(\mathfrak{p}))_0 = \operatorname{Spec} A/\phi^{-1}(\mathfrak{p})$. El cuerpo de fracciones de $A/\phi^{-1}(\mathfrak{p})$ está incluido en el cuerpo de fracciones de $B/\mathfrak{p}$, luego el grado de trascendencia del primero es menor o igual que el del segundo y $\dim \overline{f(C)} \leq \dim C$. □

6. Teorema del ideal principal de Krull: *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra. Sea $f \in A$, no nula ni invertible. Entonces*

$$\dim(f)_0 = \dim X - 1$$

Es más, todas las componentes irreducibles de $(f)_0$ son de dimensión $\dim X - 1$.

Demostración. Si $X = \operatorname{Spec} k[x_1,\dots,x_n]$ y descomponemos $f = p_1^{n_1}\cdot\ldots\cdot p_s^{n_s}$ en producto de irreducibles, tenemos que $(f)_0 = \cup(p_i)_0$. Basta probar que $\dim(p_i)_0 = n-1$. Ahora bien, el grado de trascendencia del cuerpo de fracciones de $k[x_1,\dots,x_n]/(p_i)$ es $n-1$, luego $\dim(p_i)_0 = n-1$.

Ahora en general. Escribamos $(f)_0 = C_1 \cup \cdots \cup C_s$ como unión de componentes irreducibles. Tenemos que probar que $\dim C_1 = \dim X - 1$. Sea $a \in A$ que se anule en todo $C_2 \cup \cdots \cup C_s$ y no se anule en todo C_1. Por 3.5.2, $\dim X = \dim U_a$ y $\dim C_1 = \dim C_1 \cap U_a$. Ahora bien, $C_1 \cap U_a$ coincide con los ceros de f en U_a. En conclusión, si probamos que la dimensión de los ceros de f en U_a es igual a $\dim U_a - 1$, tendremos que $\dim C_1 = \dim X - 1$. Sustituyendo X por U_a podemos suponer que $(f)_0$ solo tiene una única componente irreducible.

Por el lema de normalización de Noether, existe un morfismo $k[x_1,\dots,x_n] \hookrightarrow A$ finito e inyectivo. La inclusión $i\colon k[x_1,\dots,x_n][f] \hookrightarrow A$ es un morfismo finito inyectivo. Además, $i^{*-1}((f)_0) = (f)_0$ luego $i^*((f)_0) = (f)_0$. Por tanto, la dimensión de $(f)_0$ en $\operatorname{Spec} k[x_1,\dots,x_n][f]$ es la misma que la de $(f)_0$ en $\operatorname{Spec} A$. Por tanto, podemos suponer que $A = k[x_1,\dots,x_n][f]$.

Sea $p(x_1,\dots,x_n,x_{n+1})$ un polinomio irreducible tal que $p(x_1,\dots,x_n,f) = 0$. El epimorfismo

$$k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1})) \to k[x_1,\dots,x_n][f],\ \bar{x}_{n+1} \mapsto f$$

es un isomorfismo, porque $k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}))$ es un anillo de dimensión n, íntegro y si hubiese núcleo la dimensión de $k[x_1,\dots,x_n][f]$ sería menor que n.

En conclusión $A = k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}))$ y $f = x_{n+1}$. Por tanto,

$$\begin{aligned}\dim(f)_0 &= \dim A/(f) = \dim k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}),x_{n+1})\\ &= \dim k[x_1,\dots,x_n]/(p(x_1,\dots,x_n,0)) = n-1.\end{aligned}$$

□

7. Definición: Una cadena de cerrados irreducibles diremos que es maximal si no está incluida en ninguna otra mayor.

8. Corolario: *Todas las cadenas maximales de cerrados irreducibles de una variedad algebraica irreducible tienen la misma longitud, que es la dimensión de Krull de la variedad.*

Demostración. Sea $X = \operatorname{Spec} A$ la variedad algebraica irreducible. Como

$$\operatorname{Spec} A = \operatorname{Spec} A_{\mathrm{red}},$$

podemos suponer que la variedad algebraica es íntegra. Demostraremos el corolario por inducción sobre la dimensión de Krull.

Sea $X \supset X_1 \supset \cdots \supset X_m$ una cadena de cerrados irreducibles maximal. Sea $f \in A$ una función no nula que se anule en X_1. Si $(f)_0 = Y_1 \cup \cdots \cup Y_r$ es la descomposición de $(f)_0$ en cerrados irreducibles, X_1 es una de las componentes de la descomposición. Por el teorema anterior $\dim X_1 = \dim X - 1$. $X_1 \supset \cdots \supset X_m$ es una cadena de cerrados irreducibles maximal, luego por la hipótesis de inducción $m-1 = \dim X_1 = \dim X - 1$, y por tanto $m = \dim X$. □

9. Definición: Se dice que una variedad algebraica es catenaria si todas las cadenas maximales de cerrados irreducibles con extremos cualesquiera prefijados tienen la misma longitud.

10. Corolario: *Las variedades algebraicas son catenarias.*

Demostración. Sean $Y \supset Y'$ cerrados irreducibles de una variedad algebraica X. Toda cadena maximal de extremos $Y' \subset Y'_1 \subset \cdots \subset Y_{\restriction m} = Y$ induce, adjuntando una cadena maximal de Y', una cadena maximal de Y, luego tiene longitud $m = \dim Y - \dim Y'$, por el corolario anterior. □

11. Proposición: *Si* $X = \operatorname{Spec} A$ *es una variedad algebraica irreducible y* $x \in X$ *un punto cerrado, entonces* $\dim X = \dim A_x$.

Demostración. La dimensión de Krull de A_x coincide con la máxima longitud de las cadenas de cerrados irreducibles de X que pasan por x. Ahora bien, todas las cadenas maximales de cerrados irreducibles tienen longitud $\dim X$.

□

12. Proposición: *Sea* $X = \operatorname{Spec} A$ *una variedad algebraica irreducible de dimensión* n *e* $Y \subset X$ *un cerrado irreducible de dimensión* m. *El número mínimo* r *para el cual existen* r *funciones* $f_1, \ldots f_r$ *de* X *tales que una de las componentes irreducibles de* $(f_1, \ldots, f_r)_0$ *sea* Y *es* $r = n - m$ *(puede imponerse además que todas las componentes sean de dimensión* m*).*

Demostración. Es fácil probar, aplicando recurrentemente el teorema del ideal principal de Krull, que todas las componentes irreducibles de $(f_1, \ldots, f_r)_0$ tienen dimensión mayor o igual que $n - r$. Por tanto, tenemos que probar solo la existencia de tales funciones para $r = n - m$.

Sea f_1 una función que se anule en todo Y y no en X. Escribamos $(f_1)_0 = \cup_i C_i$, donde C_i son cerrados irreducibles de dimensión $n-1$. Si $m = n - 1$, hemos terminado.

Sea f_2 una función que se anule en todo Y y no se anule en todo C_i, para cada i. Existe tal función: sea g_i que se anule en Y y en todos los C_j para $j \neq i$, y no se anule en todo C_i, entonces $f_2 = \sum_i g_i$. Tenemos que $(f_1, f_2)_0$ es unión de cerrados irreducibles de dimensión $n-2$ y $(f_1, f_2)_0$ contiene a Y. Siguiendo de este modo obtenemos las funciones $f_1, \ldots, f_r$ requeridas.

□

13. Corolario: *Sea X una variedad algebraica irreducible de dimensión n y $x \in X$ un punto cerrado. El número mínimo de funciones $f_1, \ldots, f_r$ tales que $(f_1, \ldots, f_r)_0 \cap U = \{x\}$, en algún entorno abierto U de x, es n.*

14. Proposición: *1. Si $X = \operatorname{Spec} A$ es una k-variedad irreducible de dimensión n y $\bar{k}$ es el cierre algebraico de k, entonces $X \times_k \bar{k} := \operatorname{Spec}(A \otimes_k \bar{k}$ es unión de $\bar{k}$-variedades irreducibles de dimensión n.*

2. Si k es algebraicamente cerrado y X y Y son k-variedades irreducibles, entonces $X \times Y$ es irreducible.

3. Sean Y, Y' subvariedades irreducibles de $X = \mathbb{A}^n$. Si $Z \neq \emptyset$ es una componente irreducible de $Y \cap Y'$, entonces

$$\dim Z \geq \dim Y + \dim Y' - n.$$

Demostración. 1. Sea $\bar{z}$ una componente irreducible de $X \times_k \bar{k}$ El morfismo de anillos $i : A \hookrightarrow A \otimes_k \bar{k}$ es entero y plano, sea i^* el morfismo inducido en espectro por i y sea $x = i^*(z)$. Como i es entero, $\bar{x} = i^*(\bar{z})$. Entonces, $\mathfrak{p}_x = \mathfrak{p}_z \cap A$ es un ideal primo minimal de A, por el teorema del descenso de ideales para morfismos planos y porque las fibras de i^* son de dimensión 0. Por tanto, $\dim X = \dim \bar{x} = \dim \bar{z}$.

2. Sean $f \neq 0$ y g dos funciones algebraicas de $X \times Y$ y supongamos que $f(x,y) \cdot g(x,y) = 0$. Sea (α, β) un punto cerrado de $X \times Y$, tal que $f(\alpha, \beta) \neq 0$. Entonces, $f(\alpha, y) \cdot g(\alpha, y) = 0$, luego $g(\alpha, y) = 0$. En un entorno abierto U de α, se cumple que $f(\alpha', \beta) \neq 0$, para todo punto cerrado $\alpha' \in U$, luego g se anula en todos los puntos cerrados de $U \times Y$. Por tanto, g se anula en todos los puntos cerrados de $X \times Y$, luego g es nilpotente. Ahora es fácil probar que $(X \times Y)_{red}$ es íntegra, luego $X \times Y$ es irreducible.

3. Obviamente, $(Y \cap Y') \times_k \bar{k} = (Y \times_k \bar{k}) \cap (Y' \times_k \bar{k})$. Podemos suponer por el apartado 1. que k es algebraicamente cerrado. $Y \times_k Y'$ es una variedad irreducible (por 2.) de dimensión $\dim Y + \dim Y'$ y es una subvariedad de $X \times X = \operatorname{Spec} k[x_1, \ldots, x_n, x'_1, \ldots, x'_n]$. $Y \cap Y' = (Y \times Y') \cap (x_1 - x'_1, \ldots, x_n - x'_n)_0$ y se concluye por el teorema del ideal principal.

□

15. Ejercicio: Sea $f: X \to Y$ un morfismo entre variedades algebraicas irreducibles y supongamos que $Y = \overline{f(X)}$. Prueba;

1. Si $y \in f(X)$ es un punto cerrado. entonces todas las componentes irreducibles de $f^{-1}(y)$ tienen dimensión mayor o igual que $\dim X - \dim Y$.
2. Si $C \subset Y$ es un cerrado irreducible y Z una componente irreducible de $f^{-1}(C)$ tal que $\overline{f(Z)} = C$, entonces $\dim Z \geq \dim C + \dim X - \dim Y$.

Resolución: 1. El problema es local en Y. Podemos suponer que $y = (f_1, \ldots, f_n)_0$, con $n = \dim Y$. Entonces, por el teorema del ideal principal todas las componentes irreducibles de $(f_1 \circ f, \ldots, f_n \circ f)_0$ tienen dimensión mayor o igual que $\dim X - n = \dim X - \dim Y$.

2. Se razona de modo análogo.

16. Ejercicio: Sea $f: X \to Y$ un morfismo cerrado epiyectivo entre variedades algebraicas irreducibles. Sea $y \in f(X)$ un punto cerrado. Demuéstrese que el conjunto de puntos $y \in Y$ tales que

$$\dim f^{-1}(y) = \dim X - \dim Y =: r$$

es un abierto no vacío de Y.

Resolución: Procedemos por inducción sobre $\dim Y$. Si $\dim Y = 0$ es obvio. Probemos que existe un abierto U tal que todo $y \in U$ cumple que $\dim f^{-1}(y) = \dim X - \dim Y$. Existe un abierto no vacío $U \subset Y$ y un morfismo finito epiyectivo $f^{-1}(U) \to U \times \mathbb{A}^r$ de modo que $f_{|f^{-1}(U)}$ es la composición de los morfismos $f^{-1}(U) \to U \times \mathbb{A}^r \to U$. U es el abierto buscado. Sea $C = Y - U$ y $\{C_i\}$ las componentes irreducibles de C, que son de dimensión menor que Y. Sean $\{Z_{ij}\}$ las componentes irreducibles de $f^{-1}(C_i)$. Sabemos que $\dim Z_{ij} - \dim C_i \geq r$. Por hipótesis de inducción, los puntos $y \in C_i$ tales que $f^{-1}(y)$ es de dimensión r es un abierto (vacío o no) de C_i. Hemos concluido.

3.6. Variedades algebraicas lisas

En esta sección queremos mostrar que el concepto de diferencial en un punto y más en general el concepto de diferencial de una función son conceptos algebraicos. Dada una variedad algebraica $X = \operatorname{Spec} A$, se cumple que el módulo dual del A-módulo generado por todas las diferenciales de las funciones de X es el módulo de derivaciones, luego derivar es también un concepto algebraico (dicho de otro modo, es una aplicación lineal que cumple la regla de Leibnitz). En Geometría Algebraica las variedades lisas se corresponden con las variedades diferenciables (algebraicas), y son aquellas variedades cuyo módulo de diferenciales es libre (de rango la dimensión de la variedad). Desarrollaremos el cálculo diferencial en las variedades algebraicas y daremos criterios diferenciales que caracterizan a las variedades lisas.

3.6.1. Módulo de las diferenciales de Kähler y módulo de derivaciones

Justifiquemos o introduzcamos la definición de diferencial de Kähler, a partir de la definición conocida de diferencial en Análisis o Geometría Diferencial.

Como es bien conocido, el incremento en un punto $\alpha \in \mathbb{R}$, de una función real f, se define $\Delta_\alpha f := f - f(\alpha)$. Esta definición es ampliable a las funciones algebraicas sobre la recta afín, es decir, para $k[x]$: Dado $p(x) \in k[x]$ y $\alpha \in k$ (equivalentemente, el punto "racional" $\alpha \in \operatorname{Spec} k[x]$, donde $\mathfrak{m}_\alpha = (x-\alpha)$), se define el incremento de $p(x)$ en α como $\Delta_\alpha p(x) := p(x) - p(\alpha)$. Más en general, dada una k-álgebra A y un punto racional $\alpha \in \operatorname{Spec} A$ (es decir, $A/\mathfrak{m}_\alpha = k$), se define el incremento de una función $f \in A$ en el punto α como $\Delta_\alpha f := f - f(\alpha)$ (donde $f(\alpha) := \bar{f} \in A/\mathfrak{m}_\alpha = k$).

La diferencial de una función real infinitamente diferenciable f, en un punto $\alpha \in \mathbb{R}$, se define como $d_\alpha f = f - f(\alpha) \mod (x-\alpha)^2$. Es decir, si $\mathfrak{m}_\alpha$ es el ideal de las funciones diferenciables que se anulan en α, entonces

$$d_\alpha f := \overline{\Delta_\alpha f} = \overline{f - f(\alpha)} \in \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

En general, dada una k-álgebra A y un punto racional $\alpha \in \operatorname{Spec} A$, se define la diferencial de la función $f \in A$ en el punto α como $d_\alpha f := \overline{\Delta_\alpha f} = \overline{f - f(\alpha)} \in \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$. El k-espacio vectorial $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, se le denomina espacio cotangente en α de $\operatorname{Spec} A$.

El siguiente paso es abstraernos del punto concreto $\alpha \in \mathbb{R}$. El incremento de una función diferenciable $f(x)$, en un punto $\bar{x}$, cualquiera, lo podemos definir como $\Delta f(x) := f(x) - f(\bar{x})$ (con precisión, $\Delta f(x)$ es la función definida en $\mathbb{R} \times \mathbb{R}$, cuyo valor en cada punto $(x, \bar{x})$ es $f(x) - f(\bar{x})$). Obviamente, $\Delta f(x)$ se anula sobre la diagonal de $\mathbb{R} \times \mathbb{R}$ y su restricción a $\mathbb{R} \times \alpha$ es $\Delta_\alpha f$. Además, si Δ es el ideal de las funciones diferenciales de $\mathbb{R} \times \mathbb{R}$ que se anulan en la diagonal, entonces la restricción de Δ a $\mathbb{R} \times \alpha$ es $\mathfrak{m}_\alpha$. Puede demostrarse que la definición de diferencial de una función, en Geometría Diferencial o Análisis, es $df := \overline{\Delta f} = \overline{f(x) - f(\bar{x})} \in \Delta/\Delta^2$. Se dice que Δ/Δ^2 es el $\mathscr{C}^\infty(\mathbb{R})$-módulo de las diferenciales de las funciones diferenciales de $\mathbb{R}$.

Consideremos el anillo $k[x]$ de las funciones algebraicas de la recta afín $\mathbb{A}^1$ y el anillo $k[x] \otimes_k k[x]$ de funciones algebraicas de $\mathbb{A}_1 \times_k \mathbb{A}_1 = \mathbb{A}_2$. Los morfismos

$$k[x] \rightrightarrows k[x, \bar{x}],\ p(x) \mapsto p(x),\ p(x) \mapsto p(\bar{x})$$

son obviamente los morfismos $k[x] \rightrightarrows k[x] \otimes_k k[x]$, $p(x) \mapsto p(x) \otimes 1$ y $p(x) \mapsto 1 \otimes p(x)$, que inducen por tomas de espectros las dos proyecciones naturales de $\mathbb{A}_1 \times_k \mathbb{A}_1$ en $\mathbb{A}_1$. La inmersión diagonal $\mathbb{A}_1 \to \mathbb{A}_1 \times_k \mathbb{A}_1$, $\alpha \mapsto (\alpha, \alpha)$ es el morfismo inducido por el morfismo de anillos $k[x] \otimes_k k[x] \xrightarrow{\phi} k[x]$, $p(x) \otimes q(x) \mapsto p(x) \cdot q(x)$. El ideal de las funciones algebraicas que se anulan en la diagonal es $\operatorname{Ker} \phi$.

Más en general, sea k un anillo y A una k-álgebra. Si definimos $\mathrm{Spec}A \times_k \mathrm{Spec}A := \mathrm{Spec}(A \otimes_k A)$, los morfismos $A \to A \otimes_k A$, $a \mapsto a \otimes 1$ y $a \mapsto 1 \otimes a$, pueden interpretarse como los morfismos que asignan a cada función $f(x)$ de $\mathrm{Spec}A$, las funciones de $\mathrm{Spec}A \times_k \mathrm{Spec}A$ $f(x)$ y $f(\bar{x})$. Diremos que el morfismo $\mathrm{Spec}A \hookrightarrow \mathrm{Spec}A \times \mathrm{Spec}A$, inducido por el epimorfismo de anillos

$$A \otimes_k A \to A, \quad a \otimes b \mapsto a \cdot b$$

es la inmersión "diagonal" de $\mathrm{Spec}A$ en $\mathrm{Spec}A \times \mathrm{Spec}A$.

1. Definición: Sea $k \to A$ un morfismo de anillos. El núcleo del morfismo

$$A \otimes_k A \to A, \quad a \otimes b \mapsto a \cdot b$$

se denomina ideal de la diagonal y lo denotaremos por Δ. Dada $f \in A$, llamaremos incremento de f en un punto cualquiera a $f \otimes 1 - 1 \otimes f \in \Delta$.

Observemos que Δ es un $A \otimes_k A$-módulo, luego es un $A = A \otimes 1$-módulo.

2. Proposición: *Δ es un A-módulo generado por los incrementos de funciones.*

Demostración. Si $\sum_i a_i \otimes b_i \in \Delta$, entonces $\sum_i a_i b_i = 0$, luego

$$\sum_i a_i \otimes b_i = \sum_i a_i \otimes b_i - \sum_i a_i b_i \otimes 1 = \sum_i - a_i \otimes 1 \cdot (b_i \otimes 1 - 1 \otimes b_i).$$

□

3. Definición: Δ/Δ^2 se denomina módulo de las diferenciales de Kähler de A sobre k y se le denota por $\Omega_{A/k}$. El morfismo

$$\begin{aligned} d : A &\to \Omega_{A/k} \\ a &\mapsto \overline{a \otimes 1 - 1 \otimes a} \end{aligned}$$

se denomina diferencial, y sus imágenes $da \in \Omega_{A/k}$ se denominan diferenciales exactas.
.

$\Omega_{A/k}$ es un $A \otimes_k A$-módulo anulado por Δ. Por tanto, es un $A = (A \otimes_k A/\Delta)$-módulo y sus estructuras de $A \otimes 1$-módulo y $1 \otimes A$-módulo coinciden. Por la proposición anterior, $\Omega_{A/k}$ es un A-módulo generado por las diferenciales exactas.

Δ y $A \otimes_k A$ son $A \otimes 1$-módulos ó $1 \otimes A$-módulos. La sucesión exacta de A-módulos

$$0 \to \Delta \to A \otimes_k A \to A \to 0$$

escinde, pues $A \to A \otimes_k A, a \mapsto a \otimes 1$ (ó $A \to A \otimes_k A, a \mapsto 1 \otimes a$) es una sección del epimorfismo $A \otimes_k A \to A$.

4. Proposición: *Sea $\mathfrak{m}_\alpha$ un ideal de A tal que $A/\mathfrak{m}_\alpha = k$. Se cumple que*

$$\Delta \otimes_A A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha.$$

Es decir, "la restricción a $\operatorname{Spec} A \times \alpha$ *del ideal de las funciones que se anulan en la diagonal es el ideal de las funciones que se anulan en α"*

Demostración. Dado que la sucesión exacta

$$0 \to \Delta \to A \otimes_k A \to A \to 0$$

escinde, si tensamos por $\otimes_A A/\mathfrak{m}_\alpha$ obtenemos la sucesión exacta

$$0 \to \Delta \otimes_A A/\mathfrak{m}_\alpha \to A \to A/\mathfrak{m}_\alpha \to 0$$

y se concluye que $\Delta \otimes_A A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha$. □

5. Corolario: *Sea $\mathfrak{m}_\alpha$ un ideal de A tal que $A/\mathfrak{m}_\alpha = k$. Entonces*

$$\Omega_{A/k} \underset{A}{\otimes} A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

Demostración. Es inmediato de la definición de módulo de diferenciales de Kähler y de la proposición anterior. □

6. Observación: Si $\mathfrak{m}_\alpha$ es un ideal de A tal que $A/\mathfrak{m}_\alpha = k$, entonces la composición de la diferencial $d\colon A \to \Omega_{A/k}$ con el paso al cociente $\Omega_{A/k} \to \Omega_{A/k} \underset{A}{\otimes} A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, define un morfismo

$$d_\alpha\colon A \to \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

que se denomina diferencial en α, y que vale $d_\alpha(f) = \overline{f - f(\alpha)}$, donde $f(\alpha)$ es la clase de f en $A/\mathfrak{m}_\alpha = k$.

7. Proposición: *Si $k \to k'$ es un morfismo de anillos, entonces que*

$$\Omega_{A/k} \underset{k}{\otimes} k' = \Omega_{A \underset{k}{\otimes} k'/k'}$$

Demostración. Denotemos Δ_A el ideal de la diagonal definido a partir de A. Denotemos $A_{k'} = A \otimes_k k'$.

Si tensamos la sucesión exacta

$$0 \to \Delta_A \to A \otimes_k A \to A \to 0$$

por $\otimes_k k'$, obtenemos la sucesión exacta

$$0 \to \Delta_A \otimes_k k' \to A_{k'} \otimes_{k'} A_{k'} \to A_{k'} \to 0$$

Luego, $\Delta_A \otimes_k k' = \Delta_{A_{k'}}$. Por tanto, $\Omega_{A/k} \otimes_k k' = (\Delta_A/\Delta_A^2) \otimes_k k' = (\Delta_A \otimes_k k')/(\Delta^2 \otimes_k k') = \Delta_{A_{k'}}/\Delta_{A_{k'}}^2 = \Omega_{A_{k'}/k'}$.

□

Derivaciones

8. Definición: Sea A una k-álgebra y M un A-módulo. Diremos que una aplicación $D: A \to M$ es una k-derivación si verifica las siguientes condiciones:

1. D es un morfismo de k-módulos.
2. $D(ab) = bD(a) + aD(b)$ para todo $a, b \in A$.

Observemos que $D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = 2D(1)$, luego $D(1) = 0$. Además, dado $\lambda \in k$, $D(\lambda) = \lambda D(1) = 0$.

El conjunto de todas las k-derivaciones de A en M se denota por $\mathrm{Der}_k(A, M)$. Si definimos

$$(D + D')(a) := D(a) + D'(a) \quad \text{y} \quad (aD)(b) := a \cdot Db$$

tenemos que el conjunto de todas las k-derivaciones de A en M tiene estructura de A-módulo.

9. Proposición: *La diferencial $d: A \to \Omega_{A/k}$ es una k-derivación.*

Demostración. Si denotamos $\delta a = a \otimes 1 - 1 \otimes a$, es una comprobación inmediata que $\delta(ab) = (a \otimes 1) \cdot \delta b + (\delta a) \cdot (1 \otimes b)$. Haciendo módulo Δ^2 obtenemos $d(ab) = adb + bda$. □

10. Corolario: *Si $\mathfrak{m}_\alpha$ es un ideal tal que $A/\mathfrak{m}_\alpha = k$, entonces $d_\alpha: A \to \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$ es una k-derivación.*

Demostración. Inmediato. □

11. Proposición: *Sea $\mathfrak{m}$ un ideal de A tal que $A/\mathfrak{m} = k$. Sea M un k-módulo, luego A-módulo a través del cociente $A \to A/\mathfrak{m} = k$. Se cumple que*

$$\mathrm{Der}_k(A, M) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, M).$$

En particular,

$$\mathrm{Der}_k(A, k) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k) \underset{Not}{=} (\mathfrak{m}/\mathfrak{m}^2)^*$$

Demostración. Dada una k-derivación $D: A \to M$, define por restricción un morfismo $D_{|\mathfrak{m}}: \mathfrak{m} \to M$, que se anula sobre $\mathfrak{m}^2$, pues $D(\mathfrak{m}^2) \subseteq \mathfrak{m}D(\mathfrak{m}) = 0$ porque M está anulado por $\mathfrak{m}$. Por tanto, define un morfismo $\bar{D}_{|\mathfrak{m}}: \mathfrak{m}/\mathfrak{m}^2 \to M$. Recíprocamente, cada morfismo de espacios vectoriales $w: \mathfrak{m}/\mathfrak{m}^2 \to M$, define, componiendo con $A \to \mathfrak{m}/\mathfrak{m}^2$, una k-derivación $A \to M$. Dejamos al lector que compruebe que estas asignaciones son inversas entre sí.

□

12. Teorema: *Tenemos el isomorfismo canónico*

$$\mathrm{Hom}_A(\Omega_{A/k}, M) = \mathrm{Der}_k(A, M),\ w \mapsto w \circ d.$$

Demostración. Por la proposición anterior, para todo A-módulo M se cumple que

$$\mathrm{Der}_A(A \otimes_k A, M) = \mathrm{Hom}_A(\Delta/\Delta^2, M).$$

Por tanto, basta probar que para todo morfismo de anillos $k \to k'$ y todo $A \otimes_k k'$-módulo M, se tiene un isomorfismo

$$\mathrm{Der}_k(A, M) \simeq \mathrm{Der}_{k'}(A \otimes_k k', M)$$

Dada una k-derivación $D : A \to M$, tenemos la k'-derivación $D' : A \otimes_k k' \to M$, definida por $D'(a \otimes \lambda) = (1 \otimes \lambda) \cdot D(a)$. Recíprocamente, toda k'-derivación $D' : A \otimes_k k' \to M$, define, componiendo con $A \to A \otimes_k k'$, una k-derivación de A en M. Una asignación es la inversa de la otra. □

13. Proposición: *Sea S un sistema multiplicativamente cerrado de A. Se verifica*

$$(\Omega_{A/k})_S = \Omega_{A_S/k},\ \frac{da}{s} \mapsto \frac{1}{s} \cdot da$$

Demostración. Empecemos probando que si M es un A_S-módulo entonces $\mathrm{Der}_k(A, M) = \mathrm{Der}_k(A_S, M)$. Basta ver para ello, que toda derivación $D \in \mathrm{Der}_k(A, M)$ extiende de modo único a una derivación de A_S. La única derivación D' que puede coincidir con D en A es:

$$D'(a/s) := (sDa - aDs)/s^2.$$

Ahora ya, tenemos

$$\begin{aligned}\mathrm{Hom}_{A_S}(\Omega_{A_S/k}, M) &= \mathrm{Der}_k(A_S, M) = \mathrm{Der}_k(A, M) = \mathrm{Hom}_A(\Omega_{A/k}, M) \\ &= \mathrm{Hom}_{A_S}((\Omega_{A/k})_S, M).\end{aligned}$$

Luego $(\Omega_{A/k})_S = \Omega_{A_S/k}$.

□

Dejamos al lector que demuestre con el mismo método

14. Proposición: $\Omega_{(A \otimes_k B)/k} = (\Omega_{A/k} \otimes_k B) \oplus (A \otimes_k \Omega_{B/k})$, $d(a \otimes b) \mapsto da \otimes b + a \otimes db$.

15. Proposición: $\Omega_{(A \times B)/k} = \Omega_{A/k} \oplus \Omega_{B/k}$, $d((a, b)) = (da, db)$.

Para terminar estudiemos las sucesiones exactas de diferenciales. Comencemos para ello con las sucesiones exactas de derivaciones.

16. Proposición: *Si B es una A-álgebra y N un B-módulo, la siguiente sucesión es exacta:*

$$\begin{array}{ccccccc} 0 & \to & \mathrm{Der}_A(B,N) & \to & \mathrm{Der}_k(B,N) & \to & \mathrm{Der}_k(A,N) \\ & & D & \mapsto & D & & \\ & & & & D & \mapsto & D_{|A} \end{array}$$

Demostración. Es evidente. □

Si B es una A-álgebra, el morfismo $A \to \Omega_{B/k}$, $a \mapsto da$ induce por 3.6.12, un morfismo $\Omega_{A/k} \to \Omega_{B/k}$, $da \mapsto da$. De otro modo, con las notaciones obvias, tenemos que Δ_A está "incluido" en Δ_B, luego tenemos un morfismo $\Omega_{A/k} = \Delta_A/\Delta_A^2 \to \Delta_B/\Delta_B^2 = \Omega_{B/k}$. Por tanto, tenemos un morfismo natural

$$\Omega_{A/k} \otimes_A B \to \Omega_{B/k}, da \otimes b \mapsto bda$$

El morfismo $B \to \Omega_{B/A}$, $d \mapsto db$, es una k-derivación, porque es una A-derivación. De nuevo, por 3.6.12, tenemos el morfismo de B-módulos $\Omega_{B/k} \to \Omega_{B/A}$, $db \mapsto db$, que es claramente epiyectivo.

17. Proposición: *Si B es una A-álgebra, la siguiente sucesión es exacta:*

$$\Omega_{A/k} \otimes_A B \to \Omega_{B/k} \to \Omega_{B/A} \to 0$$

Demostración. Basta probar que para todo B-módulo N, la sucesión

$$0 \to \underset{\mathrm{Der}_A(B,N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{B/A},N)}} \to \underset{\mathrm{Der}_k(B,N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{B/k},N)}} \to \underset{\mathrm{Der}_k(A,N)}{\underset{\|}{\underset{\mathrm{Hom}_A(\Omega_{A/k},N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B,N)}}}}$$

es exacta. Lo es por la proposición anterior.

□

18. Proposición: *Si I es un ideal de A y N es un A/I-módulo, la restricción a I de cualquier k-derivación $D : A \to N$ es un morfismo de A-módulos. La siguiente sucesión es exacta*

$$0 \to \mathrm{Der}_k(A/I,N) \to \mathrm{Der}_k(A,N) \to \mathrm{Hom}_A(I,N)$$

Demostración. Es evidente. □

19. Proposición: *Sea $I \subset A$ un ideal y consideremos el morfismo $I/I^2 \to \Omega_{A/k} \otimes A/I$, $\bar{i} \mapsto di \otimes 1$. La siguiente sucesión es exacta*

$$I/I^2 \to \Omega_{A/k} \otimes_A A/I \to \Omega_{(A/I)/k} \to 0$$

Demostración. Basta probar que para todo A/I-módulo N, la sucesión

$$\begin{array}{ccccc} 0 \to \underset{\text{Der}_k(A/I,N)}{\underset{\|}{\text{Hom}_{A/I}(\Omega_{(A/I)/k},N)}} & \to & \underset{\text{Hom}_A(\Omega_{A/k},N)\ =\ \text{Der}_k(A,N)}{\underset{\|}{\text{Hom}_{A/I}(\Omega_{A/k} \otimes_A (A/I),N)}} & \to & \underset{\text{Hom}_A(I,N)}{\underset{\|}{\text{Hom}_{A/I}(I/I^2,N)}} \end{array}$$

es exacta, luego se termina por la proposición anterior. □

Calculemos los módulos de derivaciones y diferenciales en algunos ejemplos.

Sea $A = k[x_1,\ldots,x_n]$ el anillo de polinomios y M un A-módulo. Si una k-derivación

$$D\colon k[x_1,\ldots,x_n] \to M$$

se anula sobre los x_i entonces $D = 0$: Por linealidad basta probar que es nula sobre los monomios x^α y para ello procedamos por inducción sobre $|\alpha| = \alpha_1 + \ldots + \alpha_n$. Supongamos $\alpha_1 \neq 0$, sea β, tal que $\beta_1 = \alpha_1 - 1$ y $\beta_i = \alpha_i$, para $i > 1$ (luego $|\beta| < |\alpha|$), entonces $D(x^\alpha) = D(x_1 \cdot x^\beta) = x^\beta \cdot Dx_1 + x_1 \cdot Dx^\beta = 0 + 0 = 0$.

Dado $m \in M$, sea $m\frac{\partial}{\partial x_i}$ la derivación definida por $m\frac{\partial}{\partial x_i}(p(x)) := \frac{\partial p(x)}{\partial x_i} \cdot m$. Dada una derivación D entonces $D = \sum_i (Dx_i) \cdot \frac{\partial}{\partial x_i}$, pues la diferencia entre los dos términos de la igualdad es una derivación que se anula en todos los x_i. Ahora ya, es clara la siguiente proposición.

20. Proposición: $\text{Der}_k(k[x_1,\ldots,x_n],M) = M\frac{\partial}{\partial x_1} \oplus \cdots \oplus M\frac{\partial}{\partial x_n}$.

21. Proposición: $\Omega_{k[x_1,\ldots,x_n]/k} = k[x_1,\ldots,x_n]dx_1 \oplus \cdots \oplus k[x_1,\ldots,x_n]dx_n$, $dp \mapsto \sum_i \frac{\partial f}{\partial x_i} dx_i$.

Demostración. Se deduce de las igualdades

$$\begin{aligned} Hom_{k[x_1,\ldots,x_n]}(\Omega_{k[x_1,\ldots,x_n]/k},M) &= \text{Der}_k(k[x_1,\ldots,x_n],M) = M\frac{\partial}{\partial x_1} \oplus \cdots \oplus M\frac{\partial}{\partial x_n} \\ &= \text{Hom}_{k[x_1,\ldots,x_n]}(k[x_1,\ldots,x_n]dx_1 \oplus \cdots \oplus k[x_1,\ldots,x_n]dx_n,M) \end{aligned}$$

□

22. Proposición: *Sea* $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$. *Entonces*

$$\Omega_{A/k} = (Adx_1 \oplus \cdots \oplus Adx_n)/(dp_1,\dots,dp_r)$$

donde $dp_i = \sum_j \frac{\partial p_i}{\partial x_j} dx_j$.

Demostración. Considérese la sucesión exacta $0 \to (p_1,\dots,p_r) \to k[x_1,\dots,x_n] \to A \to 0$ y aplíquese la sucesión exacta de diferenciales 3.6.19. □

23. Teorema: *Sea* k *un cuerpo. Una* k*-álgebra finita* A *es separable si y solo* $\Omega_{A/k} = 0$.

Demostración. Por cambio de cuerpo base podemos suponer que A es racional. Podemos suponer que A es racional y local, de ideal maximal $\mathfrak{m}$.

Por el lema de Nakayama, $\Omega_{A/k} = 0$ si y solo si $\mathfrak{m}/\mathfrak{m}^2 = \Omega_{A/k} \otimes_A A/\mathfrak{m} = 0$, que equivale a decir que $\mathfrak{m} = 0$, es decir, que A es separable. □

24. Ejercicios:

1. Sea $A = k[x](p(x))$. Prueba que $\Omega_{A/k} = k[x]/(p, p')dx$. Prueba que $\Omega_{A/k} = 0 \Leftrightarrow p(x)$ tiene raíces dobles.

2. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcula $\Omega_{A/k}$, $\Omega_{A/K}$ y $\Omega_{K/k}$.

3. Prueba que $\Omega_{\varinjlim A_i/k} = \varinjlim \Omega_{A_i/k}$.

4. Sea A una k-álgebra finita y racional. Prueba que $\Omega_{A/k} = 0 \Leftrightarrow A = k \times \overset{n}{\cdots} \times k$.

5. Sea $A = k[x]$, $B = k[x,y]$. Dar la interpretación geométrica de la sucesión exacta $0 \to \mathrm{Der}_A(B,M) \to \mathrm{Der}_k(B,M) \to \mathrm{Der}_k(A,M) \to 0$, siendo $M = k[x,y]/(x,y)$.

6. Si B es una A-álgebra finita y A es una k-álgebra finita, prueba que: B es separable sobre $k \Leftrightarrow A$ es separable y $\Omega_{B/A} = 0$.

7. Sea A una k-álgebra finita local y racional. Prueba: A tiene un elemento primitivo $\Leftrightarrow \Omega_{A/k}$ tiene un generador.

8. Sea A un anillo íntegro y local y sea B una A-álgebra, que como A-módulo es finito generada y libre. Prueba que $B \to \mathrm{Hom}_A(B,A)$, $b \mapsto \mathrm{tr}(b \cdot -)$ es isomorfismo si y solo si $\Omega_{B/A} = 0$.

9. Sea $A = k[x]/(p(x))$, siendo k de característica cero. Prueba la exactitud de la sucesión
$$0 \to \pi_0^k(A) \to A \xrightarrow{d} \Omega_{A/k}$$
¿Es cierto este resultado si k es de característica p?

10. Sea $K \to \overline{K} = K(\alpha)$ una extensión finita. Prueba:

    a) Si $\overline{K}$ es separable, entonces $\Omega_{\overline{K}[x]/K} = \overline{K}[x]$.

    b) Si $\overline{K}$ no es separable, entonces $\Omega_{\overline{K}[x]/K} = \overline{K}[x] \oplus \overline{K}[x]$.

3.6.2. Variedades lisas

25. Definición: Sea $X = \operatorname{Spec} A$ una variedad algebraica. Diremos que X es lisa en un punto cerrado $x \in X$ si $\Omega_{A_x/k}$ es un A_x-módulo libre de rango $\dim A_x$. Diremos que X es lisa si es lisa en todos sus puntos cerrados.

26. Ejemplos: El espacio afín $\mathbb{A}^n = \operatorname{Spec} k[x_1, \ldots, x_n]$ es liso.

La cúspide $y^2 - x^3 = 0$ es lisa en todos los puntos cerrados salvo en el origen: Escribamos $A = \mathbb{C}[x,y]/(y^2 - x^3)$. Para todo punto cerrado $\alpha \in \operatorname{Spec} A$, $\dim A_\alpha = 1$. Consideremos la sucesión exacta

$$0 \to \langle 3x^2 dx \oplus 2y dy \rangle \to A dx \oplus A dy \to \Omega_{A/k} \to 0$$

Para $\alpha = (0,0)$, $\Omega_{A/k} \otimes_A A/\mathfrak{m}_\alpha$ es un $A/\mathfrak{m}_\alpha$-espacio vectorial de dimensión 2, luego $(\Omega_{A/k})_\alpha$ no es libre de rango 1. Por el lema 3.6.29, para todo $\alpha \neq (0,0)$, $(\Omega_{A/k})_\alpha$ es un módulo libre de rango 1.

El nodo es $y^2 - x^2 + x^3 = 0$ es liso en todos los puntos salvo el origen.

27. Proposición: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica. Si $x \in X$ es un punto racional liso, entonces $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x$.*

Demostración. Es consecuencia inmediata de la igualdad $\Omega_{A/k} \otimes_A A/\mathfrak{m}_x = \mathfrak{m}_x/\mathfrak{m}_x^2$. □

Observemos que en general $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 \geq \dim A_x$, porque si $\{\bar{f}_1, \ldots, \bar{f}_n\}$ es una base de $\mathfrak{m}_x/\mathfrak{m}_x^2$, entonces $\mathfrak{m}_x = (f_1 \ldots, f_n)$ y $0 = \dim(A_x/(f_1, \ldots, f_n)) \geq \dim A_x - n$.

28. Proposición: *Sea $X = \operatorname{Spec} A$ una variedad algebraica y $x \in X$ un punto cerrado. Si $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x$ entonces A_x es íntegra.*

En particular, si $x \in X$ es un punto racional liso, entonces A_x es íntegra.

Demostración. Procedemos por inducción sobre $n = \dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2$. Si $n = 0$ entonces A_x es un cuerpo. Supongamos $n > 0$. Dado $f \in \mathfrak{m}_x$, tal que $d_x f \neq 0$, sea $\bar{A}_x := A_x/(f)$ y $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en $\bar{A}_x$. Entonces, $\dim \bar{A}_x \geq n - 1$ y $\dim_{\bar{A}/\bar{\mathfrak{m}}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \leq n - 1$. Luego, $\dim_{\bar{A}/\bar{\mathfrak{m}}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim \bar{A}_x = n - 1$. Por hipótesis de inducción $\bar{A}_x$ es íntegro. Por tanto, $(f)_0 \subset \operatorname{Spec} A_x$ es una hipersuperficie irreducible (que pasa por x), incluida en todas

las componentes irreducibles de dimensión n y no contiene, pues, ninguna componente irreducible de $\operatorname{Spec} A_x$. Sean $g_1, g_2 \in A_x$. Por noetherianidad tendremos que $g_1 = f_1^{n_1} \cdots f_r^{n_r} \cdot g_1'$, $g_2 = f_1^{m_1} \cdots f_r^{m_r} \cdot g_2'$, con $n_i, m_i \geq 0$, $d_x f_i \neq 0$ y g_1', g_2' no divisibles por ninguna $f \in \mathfrak{m}_x$, tal que $d_x f \neq 0$. Si $g_1 \cdot g_2 = 0$, entonces $(g_1' \cdot g_2')_0 = \operatorname{Spec} A_x$. Dada $f \in \mathfrak{m}_x$ con $d_x f \neq 0$, como (f) es primo se cumple que f divide a g_1' o g_2' y hemos llegado a contradicción.

□

29. Lema: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, M un $\mathcal{O}$-módulo finito generado y $f : M \to L$ un morfismo en un libre finito generado. Si $\bar{f} : M/\mathfrak{m}M \to L/\mathfrak{m}L$ es inyectivo, entonces f es inyectivo y los módulos M y $\operatorname{Coker} f$ son libres.*

Demostración. Sea $m_1, \ldots, m_r \in M$ tales que $\bar{m}_1, \ldots, \bar{m}_r \in M/\mathfrak{m}M$ sean una base. Por el lema de Nakayama, $\{m_1, \ldots, m_r\}$ es un sistema generador de M. Sea $\{\overline{f(m_1)}, \ldots, \overline{f(m_r)}, \bar{l}_1, \ldots, \bar{l}_r\}$ una base de $L/\mathfrak{m}L$. Por el lema 0.10.3, $\{f(m_1), \ldots, f(m_r), l_1, \ldots, l_s\}$ es una base de L. Luego, $\{m_1, \ldots, m_r\}$ es una base de M, f es inyectivo y $\operatorname{Coker} f$ es libre de base $\{l_1, \ldots, l_s\}$. □

30. Proposición : *Sea $X = \operatorname{Spec} A$ una variedad algebraica y $x \in X$ un punto racional liso. Sea $Y = \operatorname{Spec} A/I$ una subvariedad de X que pasa por x. Entonces, Y es lisa en $x \iff$ el ideal $I_x \subset A_x$ está generado por funciones cuyas diferenciales en x son linealmente independientes.*

Demostración. Sea $\mathfrak{m}_x \in A$ el ideal de todas las funciones que se anulan en x, $n = \dim A_x = \dim_k \mathfrak{m}_x/\mathfrak{m}_x^2$ y $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en A/I.

$\Leftarrow$) $I_x = (f_1, \ldots, f_r)$, con $d_x f_1, \ldots, d_x f_r \in \mathfrak{m}_x/\mathfrak{m}_x^2$ linealmente independientes. Tenemos la sucesión exacta

$$I_x/I_x^2 \to (\Omega_{A/k} \otimes_A (A/I))_x \to (\Omega_{(A/I)/k})_x \to 0$$

Al tensar por $\otimes_A A/\mathfrak{m}_x$, obtenemos la sucesión exacta

$$0 \to \langle d_x f_1, \ldots, d_x f_r \rangle \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Por el lema 3.6.29, $(\Omega_{(A/I)/k})_x$ es libre de rango $n - r$. Además, $\dim_k \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = n - r$ y $\dim(A/I)_x \geq n - r$. Luego, $\dim(A/I)_x = n - r$ e Y es lisa en x.

$\Rightarrow$) Consideremos la sucesión exacta

$$I_x/I_x^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Sean $f_1,\dots,f_r \in I$ tales que $d_x f_1,\dots,d_x f_r$ sean una base de la imagen de I en $\mathfrak{m}_x/\mathfrak{m}_x^2$. Observemos que $n-r = \dim_k \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim(A/I)_x$. Sea $J := (f_1,\dots,f_r) \subseteq I$. Por la implicación $\Leftarrow$), $(A/J)_x$ es lisa de dimensión de Krull $n-r$. Tenemos que $\dim(A/J)_x = \dim(A/I)_x$ y $(A/J)_x$ es íntegra. El morfismo de paso al cociente $\pi\colon (A/J)_x \to (A/I)_x$ es isomorfismo: Si $\operatorname{Ker}\pi \neq 0$, entonces la dimensión de Krull de $(A/I)_x = (A/J)_x/\operatorname{Ker}\pi$ sería menor que la de $(A/J)_x$ y llegaríamos a contradicción. Luego $(A/J)_x = (A/I)_x$ y $I_x = J_x = (f_1,\dots,f_r)$. □

En bien conocido en Geometría Diferencial que si X es una variedad diferenciable e Y el cerrado definido por r funciones diferenciables $f_1,\dots,f_r \in \mathscr{C}^\infty(X)$, tales que $d_y f_1,\dots,d_y f_r$ son linealmente independientes para todo $y \in Y$, entonces Y es una subvariedad diferenciable de X.

31. Ejercicio: Sea $X = \operatorname{Spec} k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ y $\alpha = (\alpha_1,\dots,\alpha_n)$ un punto racional de X. Supongamos que $\dim X = n-r$. Prueba que X es liso en x si y solo si la matriz $(\frac{\partial p_i}{\partial x_j}(0))_{i,j\leq n}$ tiene rango r.

32. Proposición: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica y k' el cierre algebraico de k. Entonces, X es lisa $\iff$ $X_{k'} := \operatorname{Spec}(A \otimes_k k')$ es lisa.*

Demostración. El morfismo $A \hookrightarrow A \otimes_k k'$ es inyectivo, entero y plano. Sea $\pi\colon X_{k'} \to X$ el morfismo inducido en espectros. Para todo punto cerrado $x' \in X_{k'}$, $\dim(A \otimes_k k')_{x'} = \dim A_{\pi(x')}$. Además la imagen por π de un punto cerrado es un punto cerrado y las fibras de puntos cerrados son puntos cerrados (y no son vacías).

$\Omega_{A/k}$ es un A-módulo plano si y solo si $\Omega_{A_K/K} = \Omega_{A/k} \otimes_k K = \Omega_{A/k} \otimes_A A_K$ es un A_K-módulo plano, porque $A \to A_K$ es un morfismo fielmente plano. Luego, $\Omega_{A/k}$ es un A-módulo localmente libre de rango n si y solo si $\Omega_{A_K/K} = \Omega_{A/k} \otimes_k K = \Omega_{A/k} \otimes_A A_K$ es un A_K-módulo localmente libre de rango n.

□

33. Criterio jacobiano de lisitud: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica lisa. Sea $Y = \operatorname{Spec}(A/I) \subset X$ una subvariedad. Entonces, Y es lisa si y solo si*

1. *$\Omega_{(A/I)/k}$ es localmente libre.*
2. *La sucesión $0 \to I/I^2 \to \Omega_{A/k} \otimes_A A/I \to \Omega_{(A/I)/k} \to 0$ es exacta.*

Demostración. Por cambio de cuerpo base podemos suponer que k es algebraicamente cerrado. La cuestión es local, luego podemos suponer que A es local de ideal maximal $\mathfrak{m}_x$. Denotemos por $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en A/I.

$\Leftarrow$) Por ser $\Omega_{(A/I)/k}$ un módulo libre, la sucesión de 2. escinde. Por tanto, al tensar por $\otimes_A A/\mathfrak{m}_x$ obtenemos la sucesión exacta

$$0 \to I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0,$$

luego I está generado por un sistema de parámetros cuyas diferenciales en x son linealmente independientes. Por 3.6.30, A/I es lisa.

$\Rightarrow$) Si Y es lisa, ya sabemos que satisface la condición 1. Sólo queda probar que la sucesión de 2. es exacta por la izquierda. Por el lema anterior, basta ver que

$$I/\mathfrak{m}_x I \xrightarrow{\bar{i}} \mathfrak{m}_x/\mathfrak{m}_x^2$$

es inyectivo, que lo es por 3.6.30. □

3.6.3. Módulo de diferenciales de una variedad en el punto genérico

Queremos probar que las variedades algebraicas íntegras (sobre un cuerpo algebraicamente cerrado) son lisas en un abierto no vacío. Para ello probaremos que el rango del módulo de diferenciales de Kahler coincide con la dimensión de la variedad.

34. Proposición: *Sea $k \to K = k(\xi_1, \dots, \xi_m)$ una extensión de tipo finito. Se verifica*

$$\dim_K \Omega_{K/k} \geq \operatorname{gr\,tr}_k K$$

Además, la desigualdad es una igualdad si y solo si existe una base de trascendencia $\{x_1, \dots, x_n\}$ tal que $k(x_1, \dots, x_n) \hookrightarrow K$ sea una extensión separable.

Demostración. Sea $\Sigma \to \Sigma(\xi)$ una extensión. Se cumple que

$$\dim_{\Sigma(\xi)} \Omega_{\Sigma(\xi)/k} = \begin{cases} \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es trascendente.} \\ \dim_\Sigma \Omega_{\Sigma/k} \text{ ó } \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es algebraico.} \end{cases}$$

En efecto: Consideremos $\Sigma[x]$. Tenemos que

$$\Omega_{\Sigma[x]/k} = \Omega_{\Sigma \otimes_k k[x]/k} = (\Omega_{\Sigma/k} \otimes_k k[x]) \oplus (\Sigma \otimes_k \Omega_{k[x]/k}) = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma[x]) \oplus \Sigma[x]dx$$

Localizando en el punto genérico de $\Sigma[x]$,

$$\Omega_{\Sigma(x)/k} = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma(x)) \oplus \Sigma(x)dx$$

y se concluye la primera parte. Supongamos ahora que ξ es algebraico. Así pues, $\Sigma(\xi) = \Sigma[x]/(p(x))$. De la sucesión exacta $0 \to (p(x)) \to \Sigma[x] \to \Sigma(\xi) \to 0$, se obtiene la sucesión exacta de diferenciales

$$\begin{array}{rcl}(p(x))/(p(x)^2) & \to & \Omega_{\Sigma[x]/k} \underset{\Sigma[x]}{\otimes} \Sigma(\xi) \to \Omega_{\Sigma(\xi)/k} \to 0 \\ p(x) & \mapsto & dp(x)\end{array}$$

Como

$$\Omega_{\Sigma[x]/k} \underset{\Sigma[x]}{\otimes} \Sigma(\xi) = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma(\xi)) \oplus \Sigma(\xi)dx$$

se concluye que

$$\dim_{\Sigma(\xi)} \Omega_{\Sigma(\xi)/k} = \begin{cases} \dim_\Sigma \Omega_{\Sigma/k}, & \text{si } dp(x) \neq 0 \\ \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } dp(x) = 0 \end{cases}$$

La primera parte de la proposición se deduce recurrentemente de lo anterior. En particular, observemos que si $\Sigma_1 \hookrightarrow \Sigma_2$ es una extensión de tipo finito y $\Omega_{\Sigma_2/\Sigma_1} = 0$ entonces $\Sigma_1 \hookrightarrow \Sigma_2$ es algebraica, luego finita.

Sea $\{x_1,\dots,x_n\}$ una base de trascendencia de K y $K' = k(x_1,\dots,x_n)$. Si $K' \hookrightarrow K$ es separable, de la sucesión de diferenciales

$$(**) \qquad \Omega_{K'/k} \otimes_{K'} K \xrightarrow{i^*} \Omega_{K/k} \to \underset{\|}{\Omega_{K/K'}} \to 0 \\ 0$$

deducimos que i^* es un epimorfismo, entonces $\dim_K \Omega_{K/k} \leq \dim_{K'} \Omega_{K'/k} = n = \operatorname{grtr}_k K$, luego $\dim_K \Omega_{K/k} = \operatorname{grtr}_k K$.

Recíprocamente, si $\dim_K \Omega_{K/k} = \operatorname{grtr}_k K = n$, sean $x_1,\dots,x_n \in K$ tales que las diferenciales $dx_1,\dots,dx_n$ sean una base de $\Omega_{K/k}$. De la sucesión $(**)$ obtenemos que i^* es epiyectiva, luego $\Omega_{K/K'} = 0$. Por tanto, $K' \hookrightarrow K$ es finita y separable y $\{x_1,\dots,x_n\}$ es una base de trascendencia. □

35. Teorema: *Sea k un cuerpo perfecto y K una extensión de tipo finito de k. Entonces,*

1. $\dim_K \Omega_{K/k} = \operatorname{grtr}_k K$.
2. *Dados $\xi_1,\dots,\xi_n \in K$, $\{d\xi_1,\dots,d\xi_n\}$ es una base del K-espacio vectorial $\Omega_{K/k}$ $\iff$ $\{\xi_1,\dots,\xi_n\}$ es una base de trascendencia de la k-extensión K y $k(\xi_1,\dots,\xi_n) \hookrightarrow K$ es un morfismo finito separable.*

Demostración. Basta demostrar 2.

$\Rightarrow$) El morfismo $k(\xi_1,\dots,\xi_n) \hookrightarrow K$ es separable, por la sucesión exacta $(**)$ de la proposición anterior. Sólo tenemos que ver que $\xi_1,\dots,\xi_n$ son algebraicamente independientes. Sea $p(x_1,\dots,x_n) \neq 0$ un polinomio de grado mínimo tal que $p(\xi_1,\dots,\xi_n) = 0$. Entonces, $dp(\xi_1,\dots,\xi_n) = \sum_i \frac{\partial p}{\partial x_i}(\xi_1,\dots,\xi_n)d\xi_i = 0$, luego $\frac{\partial p}{\partial x_i}(\xi_1,\dots,\xi_n) = 0$ para todo

i, de donde se deduce que $\frac{\partial p}{\partial x_i}(x_1,\dots,x_n)=0$ y $p(x_1,\dots,x_n)=q(x_1^p,\dots,x_n^p)$. Tenemos $\sqrt[p]{p(x_1,\dots,x_n)}=\sqrt[p]{q(x_1^p,\dots,x_n^p)}\in k[x_1,\dots,x_n]$ por ser k perfecto. Además, $\sqrt[p]{p(x_1,\dots,x_n)}$ es un polinomio de grado menor que el de $p(x_1,\dots,x_n)$, que anula a $\xi_1,\dots,\xi_n$. Contradicción, no existe $p(x_1,\dots,x_n)\neq 0$ tal que $p(\xi_1,\dots,\xi_n)=0$.

$\Leftarrow$) Por la sucesión exacta $(**)$ de la demostración de la proposición anterior, el morfismo $\Omega_{k(\xi_1,\dots,\xi_n)/k}\otimes_{k(\xi_1,\dots,\xi_n)}K\to\Omega_{K/k}$ es epiyectivo, luego $\{d\xi_1,\dots,d\xi_n\}$ generan el K-espacio vectorial $\Omega_{K/k}$. Además, como $\dim_K\Omega_{K/k}\geq \operatorname{grtr}_k K=\operatorname{grtr}_k k(\xi_1,\dots,\xi_n)=n$, $\{d\xi_1,\dots,d\xi_n\}$ es una base del K-espacio vectorial $\Omega_{K/k}$. □

36. Corolario: *Sea k un cuerpo perfecto y K, K' dos k-extensiones de cuerpos. Entonces, la k-álgebra $K\otimes_k K'$ es reducida.*

Demostración. K es límite inductivo de k-subextensiones de tipo finito y el límite inductivo de subanillos reducidos es reducido. Podemos suponer que K es una extensión de tipo finito y, por el teorema 3.6.35, que K es una extensión finita separable de $k(x_1,\dots,x_n)$. $k(x_1,\dots,x_n)\otimes_k K'$ es una localización de $k[x_1,\dots,x_n]\otimes_k K'=K'[x_1,\dots,x_n]$, luego es íntegro. Sea Σ el cuerpo de fracciones de $k(x_1,\dots,x_n)\otimes_k K'$. Entonces,

$$K\otimes_k K'=K\otimes_{k(x_1,\dots,x_n)}(k(x_1,\dots,x_n)\otimes_k K')\subseteq K\otimes_{k(x_1,\dots,x_n)}\Sigma$$

ésta última es reducida, luego $K\otimes_k K'$ luego es reducida.

□

37. Corolario: *Sea k un cuerpo algebraicamente cerrado y X, Y dos k-variedades íntegras. Entonces, $X\times_k Y$ es una variedad íntegra.*

Demostración. $X\times_k Y$ es irreducible por la proposición 3.5.14. Escribamos $X=\operatorname{Spec}A$ e $Y=\operatorname{Spec}A'$, y sean Σ y Σ' los cuerpos de fracciones de A y A'. Como el morfismo $A\otimes_k A'\hookrightarrow\Sigma\otimes_k\Sigma'$ es inyectivo, entonces $A\otimes_k A'$ es reducida. Por tanto, $X\times_k Y$ es una variedad íntegra. □

38. Proposición: *Sea $X=\operatorname{Spec}A$ una variedad algebraica íntegra sobre un cuerpo perfecto. El conjunto de puntos cerrados lisos de X es un abierto no vacío (del conjunto de puntos cerrados de X).*

Demostración. Sea Σ el cuerpo de fracciones de A. Sabemos que $\dim_\Sigma\Omega_{\Sigma/k}=\operatorname{grtr}\Sigma=\dim X$. Por tanto, si $x\in X$ es un punto cerrado tal que $\Omega_{A_x/k}$ es un A_x-módulo libre, su rango coincide con $\dim X$, como se ve localizando en el punto genérico, luego es liso. Recíprocamente, si x es liso entonces $\Omega_{A_x/k}$ es un A_x-módulo libre. Como el conjunto de puntos donde $\Omega_{A/k}$ es libre es un abierto (no vacío porque contiene al punto genérico), se concluye. □

3.7. Variedades Proyectivas

En Geometría Lineal el marco "afín" pronto se muestra excesivamente estrecho y es necesario la introducción de los espacios proyectivos. Lo mismo sucede en Geometría Algebraica, donde habrá que introducir el concepto de variedad proyectiva. Por poner un ejemplo de esta necesidad, digamos que el teorema de Bézout, que afirma que dos curvas planas de grados n y m, se cortan en $n \cdot m$ puntos, es un enunciado en el plano proyectivo, pues es necesario para la validez de este teorema considerar los puntos del infinito.

En Geometría Proyectiva el espacio proyectivo $\mathbb{P}(E)$ asociado a un espacio vectorial E se define como el conjunto de rectas (que pasan por el origen) de E. Así las rectas de E (que pasan por el origen) se corresponden biunívocamente con los puntos de $\mathbb{P}(E)$. En Geometría Algebraica vamos a definir de modo equivalente, a partir de $\mathbb{A}^{n+1} = \operatorname{Spec}\mathbb{C}[x_0,\dots,x_n]$, el espacio proyectivo n-dimensional. Las subvariedades V que vamos a considerar en $\mathbb{A}^{n+1}$ son las variedades homogéneas, es decir, las que contengan para todo punto cerrado $p \in V$ la recta que pasa por p y el origen, y tales que $V \neq \{\text{origen}\}$. Así, las subvariedades irreducibles homogéneas de dimensión mínima serán las rectas que pasan por el origen, que se corresponderán con los puntos cerrados del espacio proyectivo que queremos asociarle a $\mathbb{A}^{n+1}$.

Sea $p(x_0,\dots,x_n) \in \mathbb{C}[x_0,\dots,x_n]$ una función que se anula en una variedad homogénea V, escribamos $p(x_0,\dots,x_n) = p_s(x_0,\dots,x_n)+\cdots+p_m(x_0,\dots,x_n)$ como suma de polinomios homogéneos. Si $(a_0,\dots,a_n)$ es un punto de V, entonces también lo es $(\lambda a_0,\dots,\lambda a_n)$, luego

$$0 = p(\lambda a_0,\dots,\lambda a_n) = \lambda^s p_s(a_0,\dots,a_n)+\cdots+\lambda^m p_m(a_0,\dots,a_n), \quad \text{para todo } \lambda.$$

Por tanto, $p_i(a_0,\dots,a_n)$ se anula en V, para todo i. En conclusión, $V = (I)_0$, donde I es un ideal generado por polinomios homogéneos. Es fácil ver el recíproco, es decir, si $V = (I)_0$ donde I es un ideal generado por polinomios homogéneos, entonces V es una variedad homogénea.

Sea $\mathbb{P}^n = \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]$ el conjunto de los ideales primos homogéneos (es decir, generados por polinomios homogéneos) de $\mathbb{C}[x_0,\dots,x_n]$, distintos de $(x_0,\dots,x_n)$. Si consideramos en $\mathbb{P}^n$ la topología inducida por $\mathbb{A}^{n+1}$, entonces los puntos cerrados de $\mathbb{P}^n$ se corresponden con las variedades homogéneas de $\mathbb{A}^{n+1}$ de dimensión mínima, que son justamente las rectas de $\mathbb{A}^{n+1}$ que pasan por el origen.

En Geometría Proyectiva se demuestra que $\mathbb{P}^n$ está recubierto por los subconjuntos $U_i^h := \{\text{rectas de } \mathbb{C}^{n+1} \text{ que pasan por el origen y no yacen en el hiperplano } x_i = 0\}$ y que éstos se corresponden con los puntos del espacio afín $\mathbb{A}^n$, del modo siguiente: El morfismo

$$\mathbb{A}^{n+1}\setminus\{x_i = 0\} \to \mathbb{A}^n,\ (\alpha_0,\dots,\alpha_n) \mapsto (\frac{\alpha_0}{\alpha_i},\dots,\frac{\alpha_n}{\alpha_i})$$

tiene por fibras las rectas que pasan por el origen y no yacen en el hiperplano $x_i = 0$, es decir, induce la igualdad

$$U_i^h = \{\text{rectas } \langle(\alpha_0,\ldots,\alpha_n)\rangle \mid \alpha_i \neq 0\} \longrightarrow\!\!\!\!\!\!= \mathbb{A}^n$$

$$\langle(\alpha_0,\ldots,\alpha_n)\rangle \longmapsto (\tfrac{\alpha_0}{\alpha_i},\ldots,\tfrac{\alpha_n}{\alpha_i})$$

En Geometría Algebraica, si $U_i^h := \{x \in \mathrm{Proj}\,\mathbb{C}[x_0,\ldots,x_n],\ x \notin (x_i)_0\}$ probaremos que la composición de los morfismos

$$U_i^h \hookrightarrow \mathbb{A}^{n+1} - (x_i)_0 \longrightarrow \mathbb{A}^n$$

$$(\alpha_0,\ldots,\alpha_n) \longmapsto (\tfrac{\alpha_0}{\alpha_i},\ldots,\tfrac{\alpha_n}{\alpha_i})$$

$$\mathbb{C}[x_0,\ldots,x_n]_{x_i} \hookleftarrow \mathbb{C}[\tfrac{x_0}{x_i},\ldots,\tfrac{x_n}{x_i}]$$

induce un homeomorfismo $U_i^h \simeq \mathrm{Spec}\,\mathbb{C}[\frac{x_0}{x_i},\ldots,\frac{x_n}{x_i}]$. Además probaremos que $\mathbb{P}^n = \cup_i U_i^h$.

Simplificando, podemos decir que la Geometría Algebraica es la disciplina que estudia y clasifica las variedades algebraicas homogéneas.

3.7.1. Álgebras graduadas

Procedamos ahora con todo rigor y generalidad.

1. Definición: Sea R un anillo y supongamos que como grupo, con la operación $+$, es suma directa de subgrupos R_i, con $i \in \mathbb{Z}$. Diremos que el anillo $R = \oplus_{n\in\mathbb{Z}} R_n$ es un álgebra graduada, si para cada $r_i \in R_i$ y $r_j \in R_j$, se cumple que $r_i \cdot r_j \in R_{i+j}$. Diremos que $r_i \in R_i$ es un elemento homogéneo de grado i.

2. Ejemplo: $k[x_1,\ldots,x_m]$ es álgebra graduada como sigue: Para $n \geq 0$,

$$k[x_1,\ldots,x_m]_n := \langle x^\alpha;\ \forall\, \alpha \in \mathbb{N}^m \text{ tal que } |\alpha| := \alpha_1 + \cdots + \alpha_m = n\rangle_k.$$

y $k[x_1,\ldots,x_m]_n := 0$, para $n < 0$.

3. Si R es un álgebra graduada, entonces $1 \in R$ es un elemento homogéneo de grado cero: Escribamos $1 = \sum_{i=-n}^{n} f_n$, con $n \in \mathbb{N}$ y $f_i \in R_i$. Multiplicando en la igualdad por cualquier $g_m \in R_m$, obtenemos $g_m = \sum_{i=-n}^{n} g_m \cdot f_n$, luego $g_m \cdot f_i = 0$ para todo $i \neq 0$ y todo g_m, luego $f_i = 0$, para todo $i \neq 0$ y $1 = f_0 \in R_0$.

4. Definición: Sea $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo, si está generado por elementos homogéneos.

5. Proposición: *Sea R un álgebra graduada e $I \subset R$ un ideal. Las siguientes afirmaciones sin equivalentes:*

1. *I es un ideal homogéneo.*
2. *$I = \oplus I_n$, siendo $I_n := I \cap R_n$ los elementos homogéneos de I de grado n.*
3. *Si $f = f_n + f_{n+1} + \cdots + f_{n+m} \in I$, entonces $f_n, \ldots, f_{n+m} \in I$.*

Demostración. $\oplus I_n \subset I$ y es un ideal homogéneo de R. Dejamos la demostración como ejercicio al lector.

□

6. Ejercicio: Prueba que la intersección de un número arbitrario de ideales homogéneos es un ideal homogéneo.

7. Ejercicio: Prueba que un ideal homogéneo $\mathfrak{p} \subseteq R$ es primo si y solo si cumple que si el producto de dos elementos homogéneos pertenece a $\mathfrak{p}$ entonces uno de los dos pertenece a $\mathfrak{p}$.

8. Proposición: *Sea R una álgebra graduada y $\mathfrak{p} \subset R$ un ideal primo. El ideal homogéneo $\mathfrak{q} = \underset{n\in\mathbb{Z}}{\oplus} (\mathfrak{p} \cap R_n)$ es primo. Por lo tanto, los ideales primos minimales de R son homogéneos.*

Demostración. Si $f_n \cdot f_m \in \mathfrak{q}$, entonces $f_n \cdot f_m \in \mathfrak{p}$, luego $f_n \in \mathfrak{p}$ o $f_m \in \mathfrak{p}$, por tanto, $f_n \in \mathfrak{q}$ o $f_m \in \mathfrak{q}$. □

9. Definición: Diremos que un morfismo de álgebras $\phi\colon R \to R'$ entre álgebras graduadas es graduado (de grado r) si transforma funciones homogéneas de grado n en funciones homogéneas de grado nr, para todo $n \in \mathbb{Z}$.

10. Si $I = \underset{n\in\mathbb{Z}}{\oplus} I_n$ es un ideal homogéneo de R, entonces R/I es un álgebra graduada de modo natural: $[R/I]_n := \{\bar{r}_n, \forall r_n \in R_n\}$.

En efecto, , $R/I = \underset{n\in\mathbb{Z}}{\oplus} R_n/I_n = \underset{n\in\mathbb{Z}}{\oplus} [R/I]_n$. Además, si $\bar{r}_n \in [R/I]_n$ y $\bar{r}_m \in [R/I]_m$, entonces $\bar{r}_n \cdot \bar{r}_m = \overline{r_n \cdot r_m} \in [R/I]_{n+m}$.

El morfismo de paso al cociente $R \to R/I$ es un morfismo graduado (de grado 1).

11. Ejemplo: Sea $\alpha \in k^{n+1}$ no nulo y $p(x_0,\dots,x_n) \in k[x_0,\dots,x_n]$ homogéneo. Para cierto i se cumple que $\alpha_i \neq 0$ y $p = \sum_{j\neq i} h_j \cdot (x_j - \frac{\alpha_j}{\alpha_i}x_i) + q(x_i)$. Por tanto, $p(\alpha) = 0$ si y solo si $q = 0$, es decir, si y solo si $p(x_0,\dots,x_n) \in \mathfrak{p}_{[\alpha]} := (\alpha_j x_k - \alpha_k x_j)_{0\leq j,k\leq n} = (\alpha_j x_i - \alpha_i x_j)_{0\leq j\leq n}$. Por tanto, el morfismo $k[x_0,\dots,x_n]/\mathfrak{p}_{[\alpha]} \to k[x_i]$, $\bar{x}_j \mapsto \frac{\alpha_j}{\alpha_i}x_i$ es isomorfismo. Luego, $\mathfrak{p}_{[\alpha]}$ es un ideal primo homogéneo. El único ideal primo homogéneo que contiene estrictamente a $\mathfrak{p}_{[\alpha]}$ es el ideal $(x_0,\dots,x_n)$, ya que el único ideal primo homogéneo de $k[x_i]$ que contiene estrictamente a (0) es (x_i).

Observemos que $(\mathfrak{p}_{[\alpha]})_0^{rac}$ se identifica con los puntos de las recta que pasa por α y el origen, cuyas ecuaciones son $x_j - \frac{\alpha_j}{\alpha_i}x_i = 0$, para todo $j \neq i$. Si $0 \neq \alpha' \in k^{n+1}$ está en esta recta, es decir, existe $\lambda \in k$ tal que $\alpha' = \lambda \cdot \alpha$, entonces $\mathfrak{p}_{[\alpha']} = \mathfrak{p}_{[\alpha]}$. Si $0 \neq \beta \in k^{n+1}$, no está en esta recta, entonces $(\mathfrak{p}_{[\beta]})_0^{rac} \neq (\mathfrak{p}_{[\alpha]})_0^{rac}$ y $\mathfrak{p}_{[\beta]} \neq \mathfrak{p}_{[\alpha]}$.

12. Sea R un álgebra graduada y $S \subset R$ un sistema multiplicativo formado por elementos homogéneos. R_S es un álgebra graduada de modo natural:

$$[R_S]_n := \{\frac{r_{n+m}}{s_m} \in R_S,\ \forall\, r_{n+m} \in R_{n+m},\ \forall\, s_m \in S \cap R_m\}.$$

En efecto, dados $\frac{f_{n+m}}{s_m}, \frac{g_{n+m'}}{t_{m'}} \in [R_S]_n$, entonces $\frac{f_{n+m}}{s_m} + \frac{g_{n+m'}}{t_{m'}} = \frac{t_{m'}f_{n+m} + s_m g_{n+m'}}{s_m t_{m'}} \in [R_S]_n$. Dado $\frac{f}{s_m} \in R_S$, $\frac{f}{s_m} = \frac{f_r + f_{r+1} + \cdots + f_s}{s_m} = \frac{f_r}{s_m} + \frac{f_{r+1}}{s_m} + \cdots + \frac{f_s}{s_m} \in \sum_n [R_S]_n$. Si $\sum_n \frac{f_{n+m_n}}{s_{m_n}} = 0$, entonces $\frac{\sum_n s_n \cdot f_{n+m_n}}{1} = 0$, con $s_n = \prod_{r\neq n} s_{m_r}$ y existe $t \in S$ tal que $\sum_n t \cdot s_n \cdot f_{n+m_n} = 0$. Sea $s = \operatorname{gr} \prod_m s_{m_n}$, entonces $\operatorname{gr}(t \cdot s_n \cdot f_{n+m_n}) = \operatorname{gr} t + s + n$. Por tanto, $t \cdot s_n \cdot f_{n+m_n} = 0$, para todo n y $\frac{f_{n+m_n}}{s_{m_n}} = 0$, para todo n. En conclusión, $R_S = \oplus_n [R_S]_n$.

El morfismo de localización $R \to R_S$ es un morfismo graduado (de grado 1).

3.7.2. Espectro proyectivo

13. Definición: Llamaremos ideal irrelevante de R al ideal $(\oplus_{n\neq 0} R_n) \subseteq R$.

14. Ejemplo: El ideal irrelevante de $k[x_0,x_1,\dots,n]$ es $(x_0,x_1,\dots,x_n)$.

Si $f_n \in R_n$, con $n \neq 0$, es invertible entonces el ideal irrelevante de R es R.

15. Definición: Llamaremos espectro proyectivo de R, y lo denotaremos $\operatorname{Proj} R$, al conjunto de ideales primos homogéneos de R que no contienen al ideal irrelevante.

Si R_0 es un cuerpo, entonces todo ideal primo homogéneo está incluido en $\oplus_{n\neq 0} R_n$, luego $\operatorname{Proj} R = \{x \in \operatorname{Spec} R :\ \mathfrak{p}_x \text{ homogéneo y } \mathfrak{p}_x \subsetneq \oplus_{n\neq 0} R_n\}$.

16. Definición: Llamaremos espacio proyectivo de dimensión n (sobre k) a

$$\mathbb{P}^n_k := \operatorname{Proj} k[x_0,\dots,x_n] = \{\text{Ideales primos homogéneos } \mathfrak{p} \underset{\neq}{\subset} (x_0,\dots,x_n)\}.$$

17. Ejemplo: $\mathbb{P}^0_k = \operatorname{Proj} k[x_0] = \{(0)\}$, es decir, es un único punto.

18. Ejemplo: $\mathbb{P}^1_{\mathbb{C}} = \operatorname{Proj} k\mathbb{C}[x_0,x_1] = \{(0),(p_n(x,y)) \text{ con } p_n(x,y) \text{ irreducible y homogéneo}\}$. Como

$$p_n(x_0,x_1) = x_0^n p_n(1,\frac{x_1}{x_0}) = x_0^n \prod_{i=1}^{n}(a_i\frac{x_1}{x_0}+b_i) = \prod_{i=1}^{n}(a_i x_1 + b_i x_0)$$

es irreducible, entonces $n=1$ y

$$\mathbb{P}^1_{\mathbb{C}} = \begin{cases} (0) \\ (ax_1+bx_0),\ \forall (a,b)\in\mathbb{C}^2-\{(0,0)\} \end{cases}$$

19. Evidentemente $\operatorname{Proj} R \subset \operatorname{Spec} R$. Consideraremos $\operatorname{Proj} R$ como espacio topológico con la topología inicial heredada de la topología de Zariski de $\operatorname{Spec} R$. Por tanto, los cerrados de $\operatorname{Proj} R$ son $(I)^h_0 := (I)_0 \cap \operatorname{Proj} R := \{x \in \operatorname{Proj} R : I \subseteq \mathfrak{p}_x\}$. Si I' es el ideal homogéneo mínimo conteniendo a I, entonces $(I)^h_0 = (I')^h_0$. Además, $(I')^h_0 = \underset{f\in I',\text{homog}}{\cap} (f)^h_0$. Por tanto, una base de cerrados de $\operatorname{Proj} R$ son los cerrados $(f)^h_0$, con f homogéneo; y una base de abiertos de la topología de $\operatorname{Proj} R$ son los abiertos

$$U^h_f := \operatorname{Proj} R \setminus (f)^h_0 = \{x \in \operatorname{Proj} R, f \notin \mathfrak{p}_x\}, \qquad (f \text{ homogéneo}).$$

20. Si $C \subset \operatorname{Proj} R$ es un cerrado, entonces $I_C = \{f \in R : f \in \mathfrak{p}_x, \forall x \in C\}$ es un ideal homogéno y $C = (I_C)^h_0$. Si C es irreducible, entonces $I_C = \mathfrak{p}_x$ es un ideal primo homogéneo y $C = \bar{x} \subset \operatorname{Proj} R$. Todo subespacio de un espacio noetheriano es noetheriano. Si R es noetheriano, entonces $\operatorname{Proj} R \subseteq \operatorname{Spec} R$, es un espacio noetheriano. En particular, $\operatorname{Proj} R$ es unión de un número finito de cerrados irreducibles, luego $\operatorname{Proj} R = \bar{x}_1 \cup \cdots \cup \bar{x}_r$, siendo $\mathfrak{p}_{x_1},\dots,\mathfrak{p}_{x_r}$ los ideales primos homogéneos minimales de R (que no contengan al irrelevante).

Un punto $x \in \operatorname{Proj} R \subset \operatorname{Spec} R$ es cerrado si y solo si $\mathfrak{p}_x$ es un ideal primo homogéneo maximal (entre los ideales primos homogéneos que no contienen al ideal irrelevante),

21. Ejemplo: Consideremos en $\mathbb{C}^{n+1}-\{(0,\dots,0)\}$ la siguiente relación de equivalencia: $\alpha \sim \beta$ si y solo existe $\lambda \in \mathbb{C}$ tal que $\alpha = \lambda\beta$. La aplicación

$$\begin{array}{ccc} \mathbb{C}^{n+1}-\{(0,\dots,0)\}/\sim & \longrightarrow & \{\text{Puntos cerrados de } \mathbb{P}^n_{\mathbb{C}}\} \\ [(\alpha_0,\dots,\alpha_n)] & \longmapsto & \mathfrak{p}_{[\alpha]} := (\alpha_i x_j - \alpha_j x_i)_{ij} \end{array}$$

es biyectiva: Por el ejemplo 3.7.11, nos falta probar que si $z \in \mathbb{P}^n_{\mathbb{C}}$ es un punto cerrado de $\mathbb{P}^n_{\mathbb{C}}$ entonces $\mathfrak{p}_z = \mathfrak{p}_{[\alpha]}$ para algún α. Sea $0 \neq \alpha \in \mathbb{C}^{n+1}$ un punto cerrado de $\bar{z} = (\mathfrak{p}_z)_0 \in \operatorname{Spec}\mathbb{C}[x_0,\dots,x_n]$. El ideal generado por todas las funciones homogéneas que se anulan en α, contiene a $\mathfrak{p}_{[\alpha]}$, luego ha de coincidir con éste; y $\mathfrak{p}_z$, que lo contiene, ha de coincidir con $\mathfrak{p}_{[\alpha]}$.

22. Si $\phi\colon R \to R'$ es un morfismo graduado entonces el morfismo $\phi^*\colon \operatorname{Spec}R' \to \operatorname{Spec}R$ inducido, aplica ideales primos homogéneos en ideales primos homogéneos. Sea $C = (\bigoplus_{n\neq 0}\phi(R_n))_0$, tenemos definido un morfismo

$$\begin{array}{rccl} \phi^*\colon \operatorname{Proj}R' \setminus C & \to & \operatorname{Proj}R & \\ x & \mapsto & \phi^*(x), & \text{donde } \mathfrak{p}_{\phi^*(x)} = \phi^{-1}(\mathfrak{p}_x). \end{array}$$

23. Ejemplo: Sea $\phi\colon k[x_0,x_1,x_2] \to k[x_0,x_1,x_2]$, $\phi(x_i) = \sum_j \lambda_{ij}x_j$ un morfismo de k-algebras tal que $\det(\lambda_{ij}) \neq 0$. Entonces, ϕ es un isomorfismo graduado, que induce un isomorfismo $\phi^*\colon \mathbb{P}^2_k \to \mathbb{P}^2_k$.

24. Proposición: *Sea I un ideal homogéneo de R. El morfismo de paso al cociente $R \to R/I$ es un morfismo graduado que induce un homeomorfismo*

$$\operatorname{Proj}(R/I) = (I)_0^h.$$

Demostración. En la igualdad $\operatorname{Spec}(R/I) = (I)_0$, los ideales primos homogéneos de R/I se corresponden con los ideales primos homogéneos de R que contienen a I. □

25. Ejemplo: Sea $X = \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]/(p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n))$. Establezcamos en $\mathbb{C}^{n+1} - \{0\}$ la relación de equivalencia: $\alpha \sim \alpha'$ si existe $\lambda \in k$ tal que $\alpha' = \lambda \cdot \alpha$. La aplicación

$$\begin{array}{rcl} \left\{\alpha \in \mathbb{C}^{n+1} - \{0\}\colon \begin{array}{r} p_1(\alpha) = 0 \\ \cdots \\ p_r(\alpha) = 0 \end{array}\right\}/\sim & \longrightarrow & \{\text{Puntos cerrados de } X\} \\ [(\alpha_0,\dots,\alpha_n)] & \longmapsto & (\alpha_j\bar{x}_i - \alpha_i\bar{x}_j)_{ij} \end{array}$$

es biyectiva: Sabemos que un polinomio homogéneo $p \in \mathbb{C}[x_0,\dots,x_n]$ cumple que $p(\alpha) = 0$ si y solo si $p \in \mathfrak{p}_{[\alpha]} := (\alpha_i x_j - \alpha_j x_i)_{ij}$. Denotemos $I = (p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n))$. Tenemos que

$$\begin{aligned} \{\text{Puntos cerrados de } X\} &= \{\text{Puntos cerrados de } (I)_0^h\} = \{\mathfrak{p}_{[\alpha]} \in \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]\colon I \subseteq \mathfrak{p}_{[\alpha]}\} \\ &= \{\alpha \in \mathbb{C}^{n+1} - \{0\}\colon p_i(\alpha) = 0, \forall i\}/\sim. \end{aligned}$$

26. Proposición : *Sea $f \in R$ un elemento homogéneo. El morfismo de localización $R \to R_f$ es un morfismo graduado que induce un homeomorfismo*

$$\mathrm{Proj}R_f = U_f^h.$$

Demostración. En la igualdad $\mathrm{Spec}R_f = U_f$, los ideales primos homogéneos de R_f se corresponden con los ideales primos homogéneos de R que no contiene a f. □

El conjunto de rectas que pasan por el origen de una variedad homogénea X, que no yacen en el plano $x_i = 0$, se identifica el conjunto de los puntos de corte del plano $x_i - 1 = 0$ con la variedad homogénea. Además, $X - \{x_i = 0\} = (X \cap \{x_i - 1 = 0\}) \times (\mathbb{A}^1 - \{0\})$. Con rigor y detalle:

27. Sea R una álgebra graduada. La aplicación

$$\begin{array}{ccc} \mathrm{Spec}R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \mathrm{Proj}R \\ \mathfrak{p} & \longmapsto & \underset{n\in\mathbb{N}}{\oplus} [\mathfrak{p}]_n \end{array}$$

es continua, ya que para cada $f \in R_n$, $\pi_R^{-1}((f)_0^h) = (f)_0 \cap (\mathrm{Spec}R - (\underset{n\neq 0}{\oplus} R_n)_0)$. En particular, para toda $f \in R_n$, con $n \neq 0$, $\pi_R^{-1}(U_f^h) = U_f$. Evidentemente, el diagrama

$$\begin{array}{ccc} \mathrm{Spec}R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \mathrm{Proj}R \\ \uparrow & & \uparrow \\ \mathrm{Spec}R_f & \xrightarrow{\pi_{R_f}} & \mathrm{Proj}R_f \end{array}$$

es conmutativo. Si $\varphi\colon R \simeq S$ es un isomorfismo de álgebras graduadas, el diagrama

$$\begin{array}{ccc} \mathrm{Spec}R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \mathrm{Proj}R \\ {\scriptstyle\varphi^*}\uparrow\wr & & \wr\uparrow{\scriptstyle\varphi^*} \\ \mathrm{Spec}S - (\underset{n\neq 0}{\oplus} S_n)_0 & \xrightarrow[\pi_S]{} & \mathrm{Proj}S \end{array}$$

es conmutativo.

Si R es una álgebra graduada, entonces R_0 es un subanillo.

28. Proposición: *Sea $f \in R$ homogénea de grado 1, entonces*

1. *$\varphi\colon \mathrm{Proj}R_f \to \mathrm{Spec}[R_f]_0$, $\mathfrak{p} \mapsto [\mathfrak{p}]_0$ es un homeomorfismo.*

2. *El morfismo de* $[R_f]_0$*-álgebras* $\phi\colon [R_f]_0 \otimes_{\mathbb{Z}} \mathbb{Z}[x,1/x] \to R_f$, $x \mapsto f$ *es un isomorfismo y tenemos el diagrama conmutativo*

$$\begin{array}{ccc} \operatorname{Spec} R_f & \xrightarrow{\pi_{R_f}} & \operatorname{Proj} R_f \\ {\scriptstyle \phi^*}\| & & \|{\scriptstyle \varphi} \\ \operatorname{Spec}[R_f]_0 \times_{\mathbb{Z}} (\mathbb{A}^1_{\mathbb{Z}} - \{0\}) & \xrightarrow[\pi_1]{} & \operatorname{Spec}[R_f]_0 \end{array}$$

donde π_1 *es la proyección en el primer factor.*

3. $[R_f]_0 \simeq R/(f-1)$*, luego* $\operatorname{Proj} R_f = \operatorname{Spec}[R_f]_0 \simeq \operatorname{Spec} R/(f-1) = (f-1)_0$.

Demostración. Denotemos $S = R_f$.

1. y 2. El morfismo $S_0[x,1/x] \to S$, $x \mapsto f$ es un isomorfismo graduado, porque el morfismo inverso es $\frac{s_n}{f^m} \mapsto \frac{s_n}{f^n} \cdot x^{n-m}$. Podemos suponer que $S = S_0[x,1/x]$ y $f = x$.

La composición φ de los morfismos naturales

$$\operatorname{Proj} S_0[x,1/x] \hookrightarrow \operatorname{Spec} S_0[x,1/x] \to \operatorname{Spec} S_0,$$

que asigna a cada ideal primo homogéneo $\mathfrak{q} \subset S_0[x,1/x]$ el ideal primo $[\mathfrak{q}]_0 := \mathfrak{q} \cap S_0$ es un homeomorfismo: Si $\mathfrak{q}$ es un ideal primo homogéneo de $S_0[x,1/x]$, entonces $\mathfrak{q} = \bigoplus_n [\mathfrak{q}]_0 \cdot x^n$. Si $\mathfrak{q}_0$ es un ideal primo de S_0 entonces $\mathfrak{q} := \bigoplus_n \mathfrak{q}_0 \cdot x^n$ es un ideal primo de $S_0[x,1/x]$ y $[\mathfrak{q}]_0 = \mathfrak{q}_0$. Por tanto, ϕ es biyectiva. Es un homeomorfismo porque aplica cerrados en cerrados. En efecto, $\varphi((s_0 \cdot x^n)^h_0) = \varphi((s_0)^h_0 = (s_0)_0$ (para todo $s_0 \in S_0$ y $n \in \mathbb{N}$). Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec} S_0[x,1/x]) & \xrightarrow{\pi_{S_0[x,1/x]}} & \operatorname{Proj} S_0[x,1/x] \\ \| & & \|{\scriptstyle \varphi} \\ \operatorname{Spec} S_0 \times_{\mathbb{Z}} (\mathbb{A}^1 - \{0\}) & \xrightarrow[\pi_1]{} & \operatorname{Spec} S_0 \end{array} \qquad \begin{array}{ccc} \mathfrak{q} & \longmapsto & \bigoplus_n [\mathfrak{q}]_n \\ & \searrow & \downarrow \\ & & [\mathfrak{q}]_0 \end{array}$$

3. $R/(f-1) = S/(f-1) = S_0[x,1/x]/(x-1) = S_0$. □

Si A es una k-álgebra, entonces $A \otimes_{\mathbb{Z}} \mathbb{Z}[x,1/x] = A \otimes_k k \otimes_{\mathbb{Z}} \mathbb{Z}[x,1/x] = A \otimes_k k[x,1/x]$, luego $\operatorname{Spec} A \times_{\mathbb{Z}} (\mathbb{A}^1_{\mathbb{Z}} - \{0\}) = \operatorname{Spec} A \times_k (\mathbb{A}^1_k - \{0\})$.

3.7.3. Variedades proyectivas

29. Definición: Llamaremos variedad proyectiva (sobre k) al espectro proyectivo de un álgebra graduada del tipo $k[\xi_0,\dots,\xi_n] = k[x_0,\dots,x_n]/I$, siendo I un ideal homogéneo. Es decir, una variedad proyectiva es un cerrado del espacio proyectivo $\mathbb{P}^n_k$. Si además es de dimensión 1, diremos que es una curva proyectiva.

Por sencillez, siempre que escribamos $k[\xi_0,\dots,\xi_n]$ supondremos que cada ξ_i es de grado 1.

Se cumple que $[k[\xi_0,\dots,\xi_n]_{\xi_i}]_0 = k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, donde $k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$ es la k-subálgebra de $R_0[\xi_0,\dots,\xi_n]_{\xi_i}$ generada por $\xi_0/\xi_i,\dots,\xi_n/\xi_i$.

Denotaremos el ideal irrelevante $\mathfrak{m}_{or} = (\xi_0,\dots,\xi_n) \subset k[\xi_0,\dots,\xi_n]$.

30. Teorema: *Se cumple que*

1. $\operatorname{Proj} k[\xi_0,\dots,\xi_n] = \bigcup_{i=0}^{n} U_{\xi_i}^h$.
2. $U_{\xi_i}^h = \operatorname{Spec} k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}] = \operatorname{Spec} k[\xi_0,\dots,\xi_n]/(\xi_i - 1)$.
3. *Sea* $\pi\colon \operatorname{Spec} k[\xi_0,\dots,\xi_n] - \{or\} \longrightarrow \operatorname{Proj} k[\xi_0,\dots,\xi_n]$, $\mathfrak{p} \mapsto \bigoplus_{m\in\mathbb{N}} [\mathfrak{p}]_m$. *Entonces,*

$$\pi^{-1}(U_{\xi_i}^h) = U_{\xi_i} = U_{\xi_i}^h \times (\mathbb{A}^1 - \{0\}).$$

Demostración. 1. $\operatorname{Proj} k[\xi_0,\dots,\xi_n] = \bigcup_{i=0}^{n} U_{\xi_i}^h$, ya que $\bigcap_{i=0}^{n} (\xi_i)_0^h = (\xi_0,\dots,\xi_n)_0^h = \emptyset$.

2. y 3. son consecuencia de la proposición 3.7.28.

□

31. Observación: Vía las iguald. $U_{\xi_i}^h = \operatorname{Spec} R_0[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}] = \operatorname{Spec} R_0[\xi_0,\dots,\xi_n]/(\xi_i - 1)$, tenemos

$$\begin{aligned}(q_1(\xi_0,\dots,\xi_n),\dots,q_r(\xi_0,\dots,\xi_n))_0^h \cap U_{\xi_i}^h &= (q_1(\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}),\dots,q_r(\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}))_0 \\ &= (q_1(\xi_0,\dots,\overset{i}{1},\dots,\xi_n),\dots,q_r(\xi_0,\dots,\overset{i}{1},\dots,\xi_n))_0.\end{aligned}$$

32. Un subconjunto C de un espacio topológico X es cerrado si y solo si dada un recubrimiento $\{U_i\}$ por abiertos de X, se cumple que $U_i \cap C$ es un cerrado de U_i, para todo i. Sea $X = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$ una variedad proyectiva. Si $U \subset X$ es un abierto y $x \in U$ es un punto cerrado de U, entonces x es un punto cerrado de X: Sea $\{U_{\xi_i}^h\}$ un recubrimiento de X, entonces x es un punto cerrado de $x \in U_{\xi_i}^h \cap U$ (para todo i, tal que $x \in U_{\xi_i}^h$), luego es un punto cerrado de $U_{\xi_i}^h$. Por tanto, $\{x\} \cap U_{\xi_i}^h$ es un cerrado para todo i, luego x es un punto cerrado de X.

33. Proposición: *Dos cerrados* C, C' *de una variedad proyectiva* $\operatorname{Proj} k[\xi_0,\dots,\xi_n]$ *son iguales si y solo si tienen los mismos puntos cerrados.*

Demostración. Si C tiene los mismos puntos cerrados que C', entonces $C \cap U^h_{\xi_i}$ tiene los mismos puntos cerrados que $C' \cap U^h_{\xi_i}$, luego $C \cap U^h_{\xi_i} = C' \cap U^h_{\xi_i}$, para todo i, luego $C = C'$. □

34. Proposición : *Si $f_m \in k[\xi_0,\dots,\xi_n]$ es una función homogénea tal que para todo punto cerrado $z \in \operatorname{Proj} k[\xi_0,\dots,\xi_n]$, $f_m(z) = 0$ (es decir, $f_m \in \mathfrak{p}_z$), entonces f_m es nilpotente.*

Demostración. Como {Conjunto de puntos cerrados de $(f_m)^h_0$} = {Conjunto de puntos cerrados de $\operatorname{Proj} k[\xi_0,\dots,\xi_n]$}, entonces $(f_m)^h_0 = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$, luego f_m pertenece a todos los ideales primos minimales de $k[\xi_0,\dots,\xi_n]$, luego es nilpotente. □

35. Si $z \in Z = \operatorname{Spec} A$, denotaremos $\mathcal{O}_{Z,z} = A_z$. Si $z \in U_a \subset \operatorname{Spec} A = Z$, entonces $\mathcal{O}_{U_a,z} = A_z = \mathcal{O}_{Z,z}$. Sea $x \in \operatorname{Spec} k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}] = U^h_{\xi_i} \subset X = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$, denotaremos $\mathcal{O}_{X,x} := \mathcal{O}_{U^h_{\xi_i},x}$. Si $x \in U^h_{\xi_j}$, entonces $U^h_{\xi_i} \cap U^h_{\xi_j} = \operatorname{Spec} k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]_{\frac{\xi_j}{\xi_i}} = \operatorname{Spec} k[\frac{\xi_0}{\xi_j},\dots,\frac{\xi_n}{\xi_j}]_{\frac{\xi_i}{\xi_j}}$, luego $\mathcal{O}_{U^h_{\xi_i},x} = \mathcal{O}_{U^h_{\xi_i}\cap U^h_{\xi_j},x} = \mathcal{O}_{U^h_{\xi_j},x}$.

Diremos que $x \in U^h_{\xi_i} \subset X = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$ es un punto racional de X, si el ideal maximal de $\mathcal{O}_{X,x}$ es racional, es decir, si x es un punto racional de $U^h_{\xi_i}$. Si k es algebraicamente cerrado, los puntos cerrados de X coinciden con los puntos racionales.

36. Ejemplo : Sea $X = \operatorname{Proj} k[x_0,\dots,x_n]/(p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n))$ y denotemos por X_{rac} el conjunto de los puntos racionales de X. Probemos que

$$X_{rac} = \left\{ \alpha \in k^{n+1}, \text{ no nulo} : \begin{array}{c} p_1(\alpha) = 0 \\ \cdots \\ p_r(\alpha) = 0 \end{array} \right\} / \sim$$

donde $\alpha \sim \alpha'$ si existe $\lambda \in k$ tal que $\alpha' = \lambda \cdot \alpha$. Denotemos al término de la derecha de la igualdad por S. Sea $S_i := \{[\alpha] \in S : \alpha_i \neq 0\}$. La aplicación $S \to X_{rac}$, $[\alpha] \mapsto \alpha$, donde $\mathfrak{p}_\alpha = (\alpha_i \bar{x}_j - \alpha_j \bar{x}_i)_{i,j}$, restringida a cada S_i es la aplicación biyectiva

$$\begin{array}{rcl} S_i & \to & \left\{ (\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n) \in k^{n+1} : \begin{array}{c} p_1(\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n) = 0 \\ \cdots \\ p_r(\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n) = 0 \end{array} \right\} = (U^h_{\xi_i})_{rac} \\ [(\alpha_0,\dots,\alpha_n)] & \mapsto & (\frac{\alpha_0}{\alpha_i},\dots,\overset{i}{1},\dots,\frac{\alpha_n}{\alpha_i}) \end{array}$$

Además, $\alpha_i = 0$ si y solo si $[(\alpha_0,\dots,\alpha_n)]$ se aplica en un punto (racional) de $(\xi_i)^h_0$.

3.7.4. Teoría de la dimensión en variedades proyectivas

37. La dimensión del espacio topológico $\operatorname{Proj} R$ coincide con con el máximo de las longitudes de las cadenas de inclusiones de ideales primos homogéneos de R que no contengan al ideal irrelevante.

38. Sea $\bar{x}_1 \subset \cdots \subset \bar{x}_m$ una cadena de cerrados irreducibles de longitud máxima de $\operatorname{Proj} R$ y U un abierto que contiene a x_1. Entonces, $x_2 \in U$, porque si $x_2 \in U^c$, entonces $\bar{x}_2 \subseteq U^c$ y $x_1 \in U^c$. Luego, $x_i \in U$, para todo i. Entonces, $\bar{x}_1 \cap U \subset \cdots \subset \bar{x}_m \cap U$ es una cadena de cerrados irreducibles en U. Como la dimensión de un abierto es siempre menor o igual que la del espacio, entonces $\dim \operatorname{Proj} R = \dim U$. Por lo tanto,

$$\dim \operatorname{Proj} k[\xi_0,\ldots,\xi_n] = \max\{\dim U^h_{\xi_i}, \forall i\}.$$

39. Proposición: *Sea X una variedad proyectiva irreducible y $U \subset X$ un abierto no vacío. Entonces,* $\dim X = \dim U$.

Demostración. Para toda pareja de abiertos V y V' no vacíos, $V \cap V' \neq \emptyset$ porque X es irreducible. Si $V \subset V'$ entonces $\dim V \leq \dim V'$. Existe un abierto afín V tal que $\dim X = \dim V$. Por la proposición 3.5.3, $\dim(U \cap V) = \dim V = \dim X$ y $\dim(U \cap V) \leq \dim U \leq \dim X$. Por tanto, $\dim U = \dim X$. □

40. Proposición: *Sea $\mathfrak{m}_{or} = (\xi_0,\ldots,\xi_n) \subset k[\xi_0,\ldots,\xi_n]$ el ideal irrelevante. Entonces,*

$$\dim \operatorname{Proj} k[\xi_0,\ldots,\xi_n] = \dim k[\xi_0,\ldots,\xi_n]_{or} - 1 = (\dim \operatorname{Spec} k[\xi_0,\ldots,\xi_n]) - 1.$$

Demostración. Los ideales primos minimales de $k[\xi_0,\ldots,\xi_n]$ son homogéneos y están incluidos en $\mathfrak{m}_{or}$. Haciendo cociente en cada uno de estos ideales primos, podemos suponer que $k[\xi_0,\ldots,\xi_n]$ es un anillo íntegro. Sabemos que $\dim k[\xi_0,\ldots,\xi_n] = \dim k[\xi_0,\ldots,\xi_n]_{or}$. Todos los abiertos no vacíos de $\operatorname{Proj} k[\xi_0,\ldots,\xi_n]$ (igualmente los de $\operatorname{Spec} k[\xi_0,\ldots,\xi_n]$) tienen la misma dimensión. Por el proposición 3.7.28, se concluye. □

41. Proposición: *Sea $f \in k[\xi_0,\ldots,\xi_n]$ una función homogénea de grado mayor que cero. Entonces,*

$$\dim(f)^h_0 \geq \dim \operatorname{Proj} k[\xi_0,\ldots,\xi_n] - 1$$

Demostración. En efecto,

$$\dim(f)^h_0 \overset{3.7.40}{=} \dim(f)_0 - 1 \overset{*}{\geq} \dim \operatorname{Spec} k[\xi_0,\ldots,\xi_n] - 2 \overset{3.7.40}{=} \dim \operatorname{Proj} k[\xi_0,\ldots,\xi_n] - 1,$$

donde $\overset{*}{\geq}$ es consecuencia del teorema del ideal principal de Krull, teniendo en cuenta todas las componentes irreducibles de $\operatorname{Spec} k[\xi_1,\ldots,\xi_n]$ pasan por or y f se anula en or (donde $\mathfrak{m}_{or} = (\xi_0,\ldots,\xi_n)$). □

42. Proposición: *Las variedades proyectivas son catenarias.*

Demostración. Dados dos cerrados irreducibles $\bar{x}_1 \subset \bar{x}_2$, sea U un abierto, que sea una variedad algebraica afín y que contenga a x_1. Toda cadena maximal de inclusiones de cerrados irreducibles de extremos $\bar{x}_1$ y $\bar{x}_2$ induce, cortando con U, una cadena maximal de inclusiones de cerrados dee U (de extremos $\bar{x}_1 \cap U$ y $\bar{x}_2 \cap U$). Se concluye por 3.5.10. □

3.8. Apéndice: Revestimientos

3.8.1. Introducción

Cuando consideramos una k-variedad algebraica $X = \operatorname{Spec} A$, estamos considerando implícitamente el morfismo $X \to \operatorname{Spec} k$. En la Geometría Algebraica Moderna es fundamental el estudio de los morfismos $X \to S$ tales que para punto $s = \operatorname{Spec} k \in S$, $\pi^{-1}(s)$ sea una k-variedad algebraica, es decir, el estudio de las parametrizaciones (por S) de variedades algebraicas.

Conviene empezar por las "parametrizaciones de variedades algebraicas de dimensión 0", es decir, por los morfismos finitos. Si imponemos que todas estas variedades algebraicas tengan los mismos puntos (contando grados y multiplicidades) entonces estaremos hablando de los revestimientos.

Por el lema de normalización de Noether, las curvas pueden entenderse como parametrizaciones (por $\mathbb{A}^1$) de variedades algebraicas de dimensión cero, es decir, dado una curva (íntegra) $C = \operatorname{Spec} A$ tenemos un revestimiento $C \to \mathbb{A}^1$, por el lema de normalización de Noether. Dado un anillo de enteros A, el morfismo único $\operatorname{Spec} A \to \operatorname{Spec} Z$ es también un revestimiento.

Si $X \to S$ es un revestimiento y G es un grupo finito de S-automorfismos de X, tal que $X/G = S$, puede estudiarse el grupo G vía el estudio de los grupos de automorfismos de las fibras. Si suponemos que X y S son íntegros, la fibra del punto genérico de S, es una extensión de Galois de grupo G. Por ejemplo, consideremos un polinomio mónico $p(x) \in \mathbb{Z}[x]$ y sea $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ el cuerpo de descomposición de $p(x)$. Consideremos el revestimiento $\operatorname{Spec} \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \to \operatorname{Spec} \mathbb{Z}$. Estamos diciendo, que el estudio del grupo de Galois de $p(x) \in \mathbb{Q}[x]$, puede realizarse estudiando el grupo de Galois de $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$, variando los primos p. Observemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito y que conocemos cuáles son la extensiones de Galois de este cuerpo y que el grupo de Galois de estas extensiones está generado por el automorfismo de Fröbenius.

3.8.2. Teoría de Galois de revestimientos puros

Los anillos considerados en esta sección y las siguientes son noetherianos (si no queremos mantener esta hipótesis, cuando digamos módulo plano deberemos decir módulo proyectivo).

1. Definición: Llamaremos revestimiento a todo morfismo $A \to B$ finito y fielmente plano (luego inyectivo).

Recordemos que un morfismo de anillos $A \to B$ plano es fielmente plano si y solo si en espectros es epiyectivo.

2. Notación: Siempre que escribamos $\mathrm{Spec}B \to \mathrm{Spec}A$, será la aplicación inducida por un morfismo de anillos $A \to B$. Diremos que $\mathrm{Spec}B \to \mathrm{Spec}A$ es un revestimiento (resp. morfismo finito, plano), si el morfismo $A \to B$ es un revestimiento (resp. finito, plano). Dado otro morfismo $\mathrm{Spec}B' \to \mathrm{Spec}A$, denotaremos

$$\mathrm{Spec}B \underset{\mathrm{Spec}A}{\times} \mathrm{Spec}B' := \mathrm{Spec}(B \otimes_A B')$$

Denotaremos $\mathrm{Hom}_{\mathrm{Spec}A}(\mathrm{Spec}B, \mathrm{Spec}B') := \mathrm{Hom}_{A-alg}(B', B)$. Si $Y \to X$ e $Y' \to X$ son revestimientos, diremos que $f \in \mathrm{Hom}_X(Y, Y')$ es un morfismo de revestimientos.

3. Si un morfismo $\pi : Y = \mathrm{Spec}B \to \mathrm{Spec}A = X$ es epiyectivo, entonces por cambio de base también es epiyectivo: Dado un cambio de base $f : X' \to X$, el morfismo inducido $\pi' : Y \times_X X' \to X'$ y $x' \in X'$, entonces $\pi'^{-1}(x') = Y \times_X x'$. Sea $x = f(x')$ e $y \in Y$ tal que $\pi(y) = f(x')$, entonces, $y \times_x x' = \mathrm{Spec}(k(y) \otimes_{k(x)} k(y') \neq \emptyset$. Como tenemos un morfismo obvio $y \times_x x' \to Y \times_X x' = \pi'^{-1}(x')$ es no vacío.

4. Ejemplos: 1. Los revestimientos de un cuerpo k son las k-álgebras finitas. En particular, las extensiones finitas de cuerpos son revestimientos.

2. Sea $B = A \times \overset{n}{\ldots} \times A$. El morfismo de anillos obvio $A \to B$ es un revestimiento. Observemos que

$$\mathrm{Spec}B = \mathrm{Spec}A \coprod \overset{n}{\ldots} \coprod \mathrm{Spec}A$$

Se dice que $\mathrm{Spec}B$ es un **revestimiento trivial** de $\mathrm{Spec}A$. Supongamos que X es conexo, entonces $\#\mathrm{Hom}_X(\coprod^n X, \coprod^m X) = n \cdot m$. En efecto,

$$\mathrm{Hom}_X(\overset{n}{\coprod} X, \overset{m}{\coprod} X) = \prod_n \mathrm{Hom}_X(X, \overset{m}{\coprod} X) = \prod_n \coprod_m \mathrm{Hom}_X(X, X).$$

La categoría $C_{Trv/X}$ de los revestimientos triviales sobre X es equivalente a la categoría C_{Conj} de los conjuntos finitos. Los functores que dan la equivalencia

son $F: C_{Conj} \rightsquigarrow C_{Trv/X}$, $F(Z) := X \times Z$ y $F': C_{Trv/X} \rightsquigarrow C_{Conj}$, $F'(Y) = \mathrm{Hom}_X(X,Y)$: $F \circ F' = \mathrm{Id}$, pues el morfismo funtorial $X \times \mathrm{Hom}_X(X,Y) \to Y$, $(x,s) \mapsto s(x)$ es isomorfismo, como basta comprobar para $Y = X$, porque F y F' son aditivos. $F' \circ F = \mathrm{Id}$, pues el morfismo natural $Z \to \mathrm{Hom}_X(X, X \times Z)$, $z \mapsto \tilde{z}$, definida por $\tilde{z}(x) = (x,z)$, es un isomorfismo, como basta comprobar para $Z = \{z\}$.

3. Todo morfismo finito $\varphi: A \to B$ entre dominios de Dedekind es inyectivo y es un revestimiento:

   En efecto, $\mathrm{Ker}\,\varphi = 0$, porque si no $A/\mathrm{Ker}\,\varphi$ sería un cuerpo y B una $A/\mathrm{Ker}\,\varphi$-álgebra finita, luego $\dim B = 0$, contradicción . Sólo nos falta probar que B es un A-módulo plano. Podemos suponer que A es un anillo local, luego un anillo de ideales principales. Ahora bien, como B es íntegro, no tiene torsión, luego es plano.

   Por ejemplo, el morfismo $k[x] \to k[x,y]/(x^2+y^2-1)$, $x \mapsto \bar{x}$ es un revestimiento.

5. Proposición: *La noción de revestimiento es estable por cambio de base.*

Demostración. En efecto, pues lo son la finitud y la fiel platitud. □

6. Proposición: *La composición de revestimientos es un revestimiento.*

Demostración. En efecto, la composición de morfismos finitos es finito y la composición de morfismos de anillos fielmente planos es un morfismo de anillos fielmente plano, pues $(- \otimes_A B) \otimes_B C = - \otimes_A C$. □

7. Definición: Diremos que un revestimiento $\mathrm{Spec}\,B \to \mathrm{Spec}\,A$ es de grado n, si B_x es un A_x-módulo libre de rango n, para todo punto cerrado $x \in \mathrm{Spec}\,A$.

Sabemos que todo A-módulo finito generado y plano es localmente libre. Si M es un A-módulo finito generado plano, entonces $\mathrm{Spec}\,A$ es una unión finita disjunta de abiertos donde el A-módulo M es localmente libre de rango constante. Entonces $A = A_0 \times \cdots \times A_n$, donde $\mathrm{Spec}\,A_i = \{x \in \mathrm{Spec}\,A$ tales que M_x es un A_x-módulo libre de rango $i\}$.

Sea $A \to B$ es un morfismo finito plano y $f: Y := \mathrm{Spec}\,B \to \mathrm{Spec}\,A =: X$ el morfismo inducido en los espectros. Entonces, $\mathrm{Spec}\,A = \coprod_{i=0}^{n} \mathrm{Spec}\,A_i$ e $Y = \coprod_{i=1}^{n} f^{-1}(\mathrm{Spec}\,A_i)$ y cada $f^{-1}(\mathrm{Spec}\,A_i)$ es un revestimiento de grado i de $\mathrm{Spec}\,A_i$. Además, $f(Y) = \coprod_{i=1}^{n} \mathrm{Spec}\,A_i$.

8. Proposición: *Si $f: Y \to X$ es un morfismo finito plano, entonces $f(Y)$ es un abierto y cerrado de X.*

Supongamos X es conexo y $f : Y \to X$ un morfismo finito y plano. Entonces f es un revestimiento, y si $Y = Y_1 \coprod Y_2$ entonces $Y_1 \to X$ es un revestimiento, porque si M es un A-módulo finito generado plano y $M = M_1 \times M_2$, entonces M_1 es un A-módulo finito generado plano.

9. Corolario : *Si $Y' \to Y$ es un morfismo de revestimientos sobre X e Y es trivial, entonces $f(Y')$ es un revestimiento trivial y $Y' \to f(Y')$ es un revestimiento.*

Demostración. Podemos suponer que $Y = X$. El morfismo $Y' \to X$ es fielmente plano y $f(Y') = X$. □

10. Proposición : *Sea $f : Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ un revestimiento de grado n. Entonces,*

$$n = \textit{Número de puntos de } f^{-1}(x), \textit{ contando multiplicidades y grados sobre } x,$$

para todo punto $x \in \operatorname{Spec} A$.

Demostración. $B_x = A_x \oplus \overset{n}{\cdots} \oplus A_x$. Entonces,

$$B_x/\mathfrak{p}_x B_x = B_x \otimes_{A_x} (A_x/\mathfrak{p}_x A_x) = (A_x/\mathfrak{p}_x A_x) \oplus \overset{n}{\cdots} \oplus (A_x/\mathfrak{p}_x A_x)$$

y $\dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x = n$. □

11. Proposición: *Sea $f : Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ un morfismo finito (es decir, $A \to B$ es finito) y supongamos que X es reducido. Entonces, f es un revestimiento de grado n si y solo si el número de puntos de la fibra de x (contando multiplicidades y grados sobre x) es n, para todo punto $x \in X$.*

Demostración. Sólo nos falta probar que si $\dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x = n$ para todo punto $x \in \operatorname{Spec} A$, entonces B es un A-módulo localmente libre de rango n, lo cual es consecuencia de 0.9.9. □

12. Definición : Diremos que un revestimiento $A \to B$ es puro o no ramificado si $\Omega_{B/A} = 0$. Si $A \to B$ es un revestimiento puro, también diremos que $\operatorname{Spec} B \to \operatorname{Spec} A$ es un revestimiento puro.

13. Ejemplos : Los revestimientos triviales son puros.

El revestimiento $\mathbb{Q}[x] \to \mathbb{Q}[x,y]/(x^2+y^2-1)$ no es puro. En efecto,

$$\Omega_{[\mathbb{Q}[x,y]/(x^2+y^2-1)]/\mathbb{Q}[x]} = \mathbb{Q}[x,y]/(x^2+y^2-1, 2y)dy = \mathbb{Q}[x,y]/(x^2-1, y)dy$$

El revestimiento $\mathbb{Q}[x]_{x^2-1} \to (\mathbb{Q}[x,y]/(x^2+y^2-1))_{x^2-1}$ es puro.

Las k-álgebras finitas separables son revestimientos puros.

14. Ejercicio: Prueba que un revestimiento $\pi: Y \to X$ es puro si y solo si para cada punto cerrado $x \in X$, $\pi^{-1}(x) \to x$ es un revestimiento puro.

15. Proposición: *La noción de revestimiento puro es estable por cambio de base y por descenso fielmente plano (es decir, dado un morfismo $A \to B$ y un morfismo fielmente plano $A \to C$, si $C \to B \otimes_A C$ es un revestimiento puro, entonces $A \to B$ también).*

Demostración. La finitud, la fiel platitud y la anulación de las diferenciales son estables por cambio de base y por descenso fielmente plano. □

16. Proposición: *Sea $Y \to X$ un revestimiento puro y X conexo. Cada componente conexa de Y es un revestimiento puro de X.*

Demostración. Sabemos que es un revestimiento. Sólo queda ver que es no ramificado. Si $B = B' \times B''$, entonces $\Omega_{B'/A} = 0$ porque $0 = \Omega_{B/A} = \Omega_{B'/A} \oplus \Omega_{B''/A}$. □

17. Teorema: *Sea $\pi: Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ un revestimiento puro, X conexo. Cada sección de π tiene por imagen una componente conexa de Y (isomorfa a X). En particular, si Y es conexo, toda sección de π es un isomorfismo.*

Demostración. Sea $\sigma: B \to A$ la sección. Escribamos $I = \operatorname{Ker}\sigma$. Por el corolario 3.6.5, $I/I^2 = \Omega_{B/A} \otimes_B A = 0$. Por el lema de Nakayama, el conjunto de puntos $y \in \operatorname{Spec} B$ tales $I_y = 0$ es $(I)_0$. Por otra parte, el conjunto de los puntos $y \in \operatorname{Spec} B$, tales que $I_y = 0$ es un abierto, porque I es un B-módulo finito generado. En conclusión, $(I)_0$ es una componente conexa de $Y = \operatorname{Spec} B$ (isomorfa a X). □

18. Fórmula de las gráficas: *Sea Y un revestimiento puro de X de grado n. Sea $X' \to X$ un morfismo, y supongamos X' conexo. Entonces*

$$\operatorname{Hom}_X(X', Y) = \operatorname{Hom}_{X'}(X', Y \times_X X') = \left\{ \begin{array}{l} \text{comp. conexas de } Y \times_X X' \\ \text{isomorfas a } X' \end{array} \right\}.$$

En particular, $\#\operatorname{Hom}_X(X', Y) \leq n$ y se da la igualdad si y solo si $Y \times_X X' \to X'$ es un revestimiento trivial.

Demostración. Para la primera igualdad, véase la proposición 0.8.13. La segunda igualdad se deduce de la proposición anterior. Veamos ahora que $\#\operatorname{Hom}_X(X', Y) \leq n$. Sea $r = \#\operatorname{Hom}_X(X', Y) = \#\operatorname{Hom}_{X'}(X', Y \times_X X')$. Se tiene entonces un morfismo inyectivo $X' \coprod \overset{r}{\ldots} \coprod X' \hookrightarrow Y \times_X X'$ de revestimientos sobre X' y por grados, $r \leq n$. Además es una igualdad si y solo si $r = n$. □

19. Definición: Sea $X' \to X$ un morfismo. Se dice que X' trivializa al revestimiento $Y \to X$ si $Y \times_X X' \to X'$ es un revestimiento trivial.

Si X' trivializa a Y y tenemos un morfismo $X'' \to X'$, entonces X'' trivializa a Y:

$$\begin{aligned} Y \times_X X'' &= (Y \times_X X') \times_{X'} X'' = (X' \coprod \cdots \coprod X') \times_{X'} X'' \\ &= X'' \coprod \cdots \coprod X'' \end{aligned}$$

Obviamente, si X' trivializa a dos revestimientos trivializa a la unión disjunta de los revestimientos y viceversa.

20. Teorema: *Sea $Y \to X$ un revestimiento puro y X conexo. Entonces existe un revestimiento puro $X' \to X$ que trivializa a $Y \to X$.*

Demostración. Procedamos por inducción sobre el grado del revestimiento $Y \to X$. Obviamente, si el grado es uno entonces $X' = Y = X$.

Supongamos que el grado es n. Como la identidad es un automorfismo de Y sobre X, por la fórmula de las gráficas, $Y \times_X Y = Y \coprod Y_2 \coprod \cdots \coprod Y_r$, donde los Y_i son todos revestimientos puros de Y, conexos y de grado estrictamente menor que n. Por inducción, existe un revestimiento puro $X' \to Y$ que trivializa a todos los $Y_i \to Y$. Luego $X' \to X$ es un revestimiento puro de X, que trivializa a Y, pues

$$\begin{aligned} Y \times_X X' &= (Y \times_X Y) \times_Y X' = (Y \coprod Y_2 \coprod \cdots \coprod Y_r) \times_Y X' \\ &= X' \coprod \cdots \coprod X'. \end{aligned}$$

□

21. Proposición: *Sea $f : Y' \to Y$ un morfismo de revestimientos de X y supongamos que Y' e Y son revestimientos puros de X. Entonces, $f(Y')$ es un revestimiento puro e $Y' \to f(Y')$ es un revestimiento puro.*

Demostración. Por cambio de base fielmente plano, puede suponerse que Y' e Y son triviales. Puede suponerse que X e Y son conexos. Entonces, $Y = X$. □

22. Definición: Diremos que un revestimiento puro conexo $Y \to X$ es principal o de Galois, si $Y \times_X Y$ es un revestimiento trivial de Y.

23. Ejemplo: Los revestimientos principales de un cuerpo k son precisamente las extensiones de Galois de k.

24. Teorema: *Sea $Y \to X$ un revestimiento puro (X conexo). Existe un revestimiento $X' \to X$ puro y conexo mínimo que trivializa a Y. Además, es único salvo isomorfismos y es un revestimiento principal.*

Demostración. Sea n el grado del revestimiento $Y \to X$. Sea X'' un revestimiento puro conexo que trivializa a $Y \to X$. Por la fórmula de las gráficas, $\#\mathrm{Hom}_X(X'',Y) = n$. Entonces, $\mathrm{Hom}_X(X'',Y) = \{\phi_1,\dots,\phi_n\}$. Consideremos el morfismo

$$X'' \xrightarrow{\phi} Y \times \overset{n}{\cdots} \times Y, \qquad \phi = \phi_1 \times \cdots \times \phi_n$$

$X' := \phi(X'')$ es una componente conexa de $Y \times \overset{n}{\cdots} \times Y$. Por la proposición anterior, X'' es un revestimiento puro epiyectivo de X' y X' es un revestimiento puro de X.

X' trivializa a Y: La composición de la inclusión $X' \hookrightarrow Y \times \overset{n}{\cdots} \times Y$ con las n proyecciones en Y, definen n morfismos distintos, pues son distintos al componerlos con la proyección $X'' \to X'$. Por tanto, $\mathrm{Hom}_X(X',Y) \geq n$ y concluimos por la fórmula de las gráficas.

Si Z es un revestimiento que trivializa a Y, entonces trivializa a $Y \times \overset{n}{\cdots} \times Y$, luego trivializa a X'. De nuevo por 3.8.18, existen morfismos de revestimientos de Z en X', que ha de ser un revestimiento puro, luego concluimos la minimalidad de X' y unicidad salvo isomorfismos.

Finalmente, X' trivializa a Y, luego se trivializa a sí mismo, esto es, es un revestimiento principal de X. □

25. Proposición: *Sea $\pi : Y' \to Y$ un epimorfismo de revestimientos sobre X. Si $Y' \to X$ es principal, entonces $Y' \to Y$ es principal.*

Demostración. $Y' \times_Y Y'$ es un cerrado de $Y' \times_X Y'$, que es trivial luego $Y' \times_Y Y'$ también lo es.

□

26. Teorema de Artin: *Sea $Y \to X$ un revestimiento puro y G un subgrupo de $\mathrm{Aut}_X Y$. Entonces, $Y/G = X$ si y solo si $Y \to X$ es principal y $G = \mathrm{Aut}_X Y$.*

Demostración. Supongamos que $Y/G = X$. Escribamos

$$Y \times_X Y = Y \coprod \cdots \coprod Y \coprod Z_1 \coprod \cdots \coprod Z_n,$$

siendo los Z_i las componentes no isomorfas a Y. Entonces

$$Y = Y \times_X (Y/G) = (Y \times_X Y)/G = (Y \coprod \cdots \coprod Y)/G \coprod (Z_1 \coprod \cdots \coprod Z_n)/G$$

Como Y es conexo, las Z_i no existen, e $Y \times_X Y = Y \coprod \cdots \coprod Y$. Luego $Y \to X$ es principal y es claro que $G = \mathrm{Aut}_X Y$.

Recíprocamente, sea $Y \times_X Y = Y \coprod \cdots \coprod Y$ y $G = \mathrm{Aut}_X Y$. Por la fórmula de las gráficas se tiene que $Y \times_X Y = Y \coprod \overset{G}{\cdots} \coprod Y$. Luego $Y/G \times_X Y = (Y \times_X Y)/G = Y$. Como $Y \to X$ es un morfismo fielmente plano, esto implica que $Y/G = X$.

□

27. Teorema de Galois: *Sea $X' \to X$ un revestimiento principal de grupo G. Denotemos por $C_{X'/X}$ la categoría de revestimientos de X trivializados por X', y por C_G la categoría de G-conjuntos finitos. Los funtores*

$$\begin{array}{ll} P\colon C_G \rightsquigarrow C_{X'/X} & P(Z) = (X' \times Z)/G \\ P'\colon C_{X'/X} \rightsquigarrow C_G & P'(Y) = \mathrm{Hom}_X(X', Y) \end{array}$$

definen una equivalencia entre las categorías C_G y $C_{X'/X}$.

Demostración. 1. La categoría de conjuntos finitos C_{Conj} es equivalente a la categoría de revestimientos triviales $C_{Trv/X'}$ de X'. Los funtores que dan la equivalencia son $F\colon C_{Conj} \rightsquigarrow C_{Trv/X'}$, $F(Z) := X' \times Z$ y $F'\colon C_{Trv/X'} \rightsquigarrow C_{Conj}$, $F'(Y) = \mathrm{Hom}_{X'}(X', Y)$, como hemos probado en el ejemplo 3.8.4.2.

2. Diremos que un revestimiento $\pi\colon Y' \to X'$ es un G-revestimiento si G opera en Y' por isomorfismos (de revestimientos sobre X). La categoría de G-conjuntos finitos C_G es equivalente a la categoría de G-revestimientos triviales de X' $C_{Trv/X'}$: Por 1., los funtores covariantes $F\colon C_G \rightsquigarrow C_{Trv/X}$, $F(Z) := X' \times Z$ (G opera sobre los dos factores) y $F'\colon C_{Trv/X'} \rightsquigarrow C_G$, $F'(Y') := \mathrm{Hom}_{X'}(X', Y')$ (G opera en $\mathrm{Hom}_{X'}(X', Y')$, como sigue: $g * s = g \cdot \circ s \circ g^{-1}\cdot$), dan la equivalencia categorial.

3. La categoría de G-revestimientos triviales $C_{Trv/X'}$ de X' es equivalente a la categoría $C_{X'/X}$ de revestimientos de X trivializados por X'. Los funtores que dan la equivalencia son $S\colon C_{Trv/X'} \rightsquigarrow C_{X'/X}$, $S(Y') := Y'/G$ y $S'\colon C_{X'/X} \rightsquigarrow C_{Trv/X'}$, $S'(Y) := X' \times_X Y$. En efecto, $S \circ S' = \mathrm{Id}$, pues $(X' \times_X Y)/G = X'/G \times_X Y = X \times_X Y = Y$. $S' \circ S = \mathrm{Id}$, pues para cada G-revestimiento trivial $Y' = X' \times Z \to X'$, el morfismo funtorial $X' \times Z \to S' \circ S(Y') = (X' \times_X (X' \times Z))/G$, $(x', z) \mapsto (x', \overline{(x', z)})$ es isomorfismo, ya que

$$(X' \times_X (X' \times Z))/G = (X' \times_X X' \times Z)/G = (X' \times G \times Z)/G = X' \times (G \times Z)/G = X' \times Z$$

4. El teorema es consecuencia de las equivalencias categoriales de 2. y 3.

□

28. Corolario: *Sea $X' \to X$ un revestimiento principal, $X' \to Y$ un morfismo de revestimientos sobre X epiyectivo y $H := \mathrm{Aut}_Y X' \subset \mathrm{Aut}_X X' =: G$. Entonces, $Y = X'/H$ y $\mathrm{Hom}_X(X', Y) = G/H$.*

Demostración. Por 3.8.25, $X' \to Y$ es un revestimiento principal. Por el teorema de Artin, $X'/H = Y$. Como $(X' \times G/H)/G = X'/H = Y$, por el teorema de Galois, $\mathrm{Hom}_X(X', Y) = \mathrm{Hom}_G(G, G/H) = G/H$. □

29. Corolario: *Sea $X' \to X$ un revestimiento principal de grupo G y $H \subseteq G$ un subgrupo. Entonces, $X'/H \to X$ es un revestimiento principal si y solo si H es un subgrupo normal de G.*

Demostración. $X'/H \to X$ es de Galois si y solo si tiene tantos automorfismos como grado.

Por el teorema de Galois, $\mathrm{Aut}_X(X'/H) = \mathrm{Aut}_G(G/H) = N(H)/H$, donde $N(H)$ es el normalizador de H en G. Por otra parte, Como $X' \to X$ es un revestimiento de grado $|G|$ y $X' \to X'/H$ es un revestimiento de grado $|H|$, $X'/H \to X$ es un revestimiento de grado $|G/H|$. Con todo,

$$\begin{aligned} X'/H \text{ es de Galois} &\iff |N(H)/H| = |G/H| \iff |N(H)| = |G| \\ &\iff H \text{ es normal en } G. \end{aligned}$$

□

3.8.3. Revestimientos ramificados

En esta subsección supondremos que los anillos son noetherianos.

Sea $A \to B$ un morfismo de anillos finito tal que B es un A-módulo libre. Para cada $b \in B$, sea $h_b : B \to B$ la homotecia de razón b, que es un endomorfismo A-lineal cuya traza denotamos $\mathrm{tr}(h_b)$. Se define la métrica de la traza T_A en B por la fórmula

$$T_A(b, b') := \mathrm{tr}(h_{b \cdot b'})$$

Seguiremos denotando T_A a la polaridad $B \to B^*$ asociada a la métrica.

Como la matriz de una aplicación lineal es estable por cambio de anillo base, también lo es la métrica de la traza. Es decir, dado un morfismo de anillos $A \to C$, el diagrama siguiente es conmutativo

$$\begin{array}{ccc} B \otimes_A C & \xrightarrow{T_C} & B^* \otimes_A C = \mathrm{Hom}_C(B \otimes_A C, C) \\ \uparrow & & \uparrow \\ B & \xrightarrow{T_A} & B^* = \mathrm{Hom}_A(B, A) \end{array}$$

Si $A \to B$ es finito y plano, existe un recubrimiento de $\mathrm{Spec}\, A$ por abiertos básicos U_{a_i} tal que B_{a_i} es un A_{a_i}-módulo libre. Por tanto, tenemos definida una métrica $T_{A_{a_i}}$ para cada B_{a_i} y, como dicha métrica es invariante por cambio de base, resulta que $T_{A_{a_i}}$ y $T_{A_{a_j}}$ coinciden en $B_{a_i \cdot a_j}$. Existe[3] una única métrica $T_A : B \times B \to A$ de modo

[3] Es consecuencia de que el núcleo del morfismo $f : \prod_i A_{a_i} \to \prod_{ij} A_{a_i a_j}$, $f((a_i)) = (a_{ij})_{ij}$ con $a_{ij} := a_i - a_j$, es la imagen del morfismo inyectivo $A \to \prod_i A_{a_i}$, $a \mapsto (a, \ldots, a)$ (véase el problema 96 del capítulo 0). En el caso A íntegro, pruébelo el lector usando que $\bigcap_i A_{a_i} = A$.

que $T_A(b,b') = T_{A_{a_i}}(b,b')$ en A_{a_i}, para todo i, que llamaremos métrica de la traza y denotaremos T_A.

30. Definición: Sea $\varphi\colon A \to B$ un revestimiento. Llamaremos diferente de B sobre A, $\mathrm{dif}_{B/A}$, al módulo definido por la sucesión exacta

$$B \xrightarrow{T_A} B^* \to \mathrm{dif}_{B/A} \to 0$$

31. Definición: Sea $\varphi\colon A \to B$ un revestimiento de rango r. Llamaremos discriminante de B sobre A, que denotaremos $\mathrm{Disc}_{B/A}$, al A-módulo definido por la sucesión exacta

$$\Lambda^r_A B \xrightarrow{\Lambda^r T_A} \Lambda^r_A B^* \to \mathrm{Disc}_{B/A} \to 0$$

Tanto el discriminante como la diferente son estables por cambio de base. En particular, localizan.

32. Teorema: *Sea $A \to B$ un revestimiento de rango r y $x \in \mathrm{Spec}A$. Entonces,*

$$(\mathrm{dif}_{B/A})_x = 0 \Leftrightarrow (\Omega_{B/A})_x = 0 \Leftrightarrow (\mathrm{Disc}_{B/A})_x = 0$$

Demostración. Podemos suponer que A es local de ideal maximal $\mathfrak{m}_x$. Por el lema de Nakayama y por estabilidad por cambio de base, podemos suponer que A es un cuerpo sin más que hacer el cambio de anillo base $A \to k(x)$ (donde $k(x)$ es el cuerpo residual de x). Pero en este caso la equivalencia $\mathrm{dif}_{B/A} = 0 \Leftrightarrow \mathrm{Disc}_{B/A} = 0$ es inmediata y la equivalencia $\mathrm{dif}_{B/A} = 0 \Leftrightarrow \Omega_{B/A} = 0$ es la proposición 2.3.29. □

33. Definición: Llamaremos lugar de ramificación de un revestimiento $A \to B$ (o del revestimiento $\mathrm{Spec}B \to \mathrm{Spec}A$) al soporte del A-módulo $\Omega_{B/A}$. Por Nakayama, esto equivale al conjunto de puntos $x \in \mathrm{Spec}A$ tales que $\Omega_{(B/\mathfrak{m}_x B)/k(x)} \neq 0$, siendo $k(x)$ el cuerpo residual de x.

Por el teorema anterior, el lugar de ramificación coincide con el soporte del discriminate y con el soporte de la diferente.

34. Teorema de pureza de Zariski: *Sea $X \to Y$ un revestimiento entre variedades algebraicas afines íntegras. El lugar de ramificación, si no es vacío, es un divisor de Cartier (es decir, localmente son los ceros de una función).*

Demostración. Escribamos $X = \mathrm{Spec}B$ e $Y = \mathrm{Spec}A$. El lugar de ramificación es el soporte del A-módulo finito generado $\Omega_{B/A}$, luego es un cerrado.

Si A es local entonces B es libre. Por tanto, $\Lambda^r_A B \simeq A$ y el discriminante es un cociente de A por un ideal principal, digamos (f). Luego el soporte del discriminante, que es el lugar de ramificación, es $(f)_0$ (localmente). □

Sea $A \hookrightarrow B$ es un revestimiento y supongamos que A es íntegro y que el morfismo $\Sigma_A \hookrightarrow B \otimes_A \Sigma_A$ es separable. Consideremos el diagrama conmutativo definido por las polaridades de las métricas de la traza

$$\begin{array}{ccc} B & \xrightarrow{\quad T_A \quad} & B^* = \mathrm{Hom}_A(B,A) \\ \downarrow & & \downarrow \\ B \otimes_A \Sigma_A & \overset{T_{\Sigma_A}}{=\!=} & (B \otimes_A \Sigma_A)^* = \mathrm{Hom}_{\Sigma_A}(B \otimes_A \Sigma_A, \Sigma_A) = \mathrm{Hom}_A(B, \Sigma_A) \end{array}$$

El A-submódulo de $B \otimes_A \Sigma_A$ formado por las $f \in B \otimes_A \Sigma_A$ tales que $T_{\Sigma_A}(f,B) = \mathrm{tr}(fB) \subseteq A$, se identifica, vía T_{Σ_A}, con B^*.

35. Teorema : *Sea A un anillo íntegro, $p(x) \in \Sigma_A[x]$ un polinomio mónico separable, con coeficientes en A y $B = A[x]/(p(x))$. Consideremos el revestimiento obvio $A \hookrightarrow B$. Entonces,*

1. *Vía la métrica de la traza $\frac{1}{p'(x)} \cdot B \simeq B^*$, donde $p'(x)$ es la derivada de $p(x)$ respecto de x.*
2. $\mathrm{dif}_{B/A} \simeq \Omega_{B/A}$ *y* $\mathrm{Disc}_{B/A} = A/\Delta(p(x))$.

Demostración. 1. Denotemos $\xi = \bar{x} \in B$. B es un A-módulo libre de base $1, \xi, \ldots, \xi^{n-1}$. Sea $w_1, \ldots, w_n \in B^*$ la base dual de $1, \xi, \ldots, \xi^{n-1}$, que es base también del Σ_A-espacio vectorial $(B \otimes_A \Sigma_A)^*$. Escribamos

$$T_{\Sigma_A}\left(\frac{\xi^j}{p'(\xi)}\right) = \sum_i a_{ji} w_i = \sum_i \mathrm{tr}\left(\frac{\xi^j \xi^i}{p'(\xi)}\right) w_i, \text{ con } a_{ji} \in \Sigma_A$$

Para probar que $\frac{1}{p'(\xi)} \cdot B$ es isomorfo a B^*, vía T_{Σ_A}, tenemos que demostrar que la matriz (a_{ji}) es una matriz con coeficientes en A e invertible.

Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$. Se verifica que $\mathrm{tr}\left(\frac{\xi^j \xi^i}{p'(\xi)}\right) = \sum_s \frac{\alpha_s^{i+j}}{p'(\alpha_s)}$. Identificando los coeficientes de los desarrollos en serie de potencias en $\frac{1}{x}$ en la igualdad $\frac{1}{p(x)} = \sum_{s=1}^{n} \frac{1}{p'(\alpha_s)} \frac{1}{(x-\alpha_s)}$, obtenemos que $a_{ji} = \sum_s \frac{\alpha_s^{i+j}}{p'(\alpha_s)} \in A$ y que

$$\mathrm{tr}\left(\frac{\xi^i \xi^j}{p'(\xi)}\right) = \sum_s \frac{\alpha_s^{i+j}}{p'(\alpha_s)} = \begin{cases} 1 & \text{si } i+j = n-1 \\ 0 & \text{si } i+j \leq n-1 \end{cases}$$

Por tanto, $\det(a_{ji}) = \pm 1$ y hemos concluido.

2. $\mathrm{dif}_{B/A} = \frac{1}{p'(\xi)} \cdot B/B \simeq B/p'(\xi) \cdot B \simeq \Omega_{B/A}$. La matriz de la métrica de la traza en la base $1, \xi, \ldots, \xi^{n-1}$ es igual a (σ_{i+j}), donde $\sigma_r = \alpha_1^r + \cdots + \alpha_n^r$. Por el teorema 1.1.10, sabemos que el determinante de esta matriz es igual al discriminante de $p(x)$. Por tanto, $\mathrm{Disc}_{B/A} = A/\Delta(p(x))$.

□

3.8.4. El maravilloso automorfismo de Fröbenius

Dado un polinomio $p(x) \in \mathbb{Z}[x]$, queremos calcular el grupo de Galois de $p(x)$ relacionándolo con el grupo de Galois de $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$, variando el primo $p \in \mathbb{Z}$.

36. Teorema: *Sea B una R-álgebra de tipo finito y G un grupo finito de automorfismos de R-álgebras de B. Consideremos el morfismo finito*

$$\pi\colon \operatorname{Spec} B \to \operatorname{Spec} B^G \overset{3.3.38}{=} (\operatorname{Spec} B)/G.$$

Sea $x \in \operatorname{Spec} B$, $y := \pi(x)$, $D := \{g \in G\colon g(x) = x\}$ el grupo de descomposición de x e I el núcleo del morfismo natural $D \to \operatorname{Aut}_{k(y)-alg} k(x)$, que se denomina el grupo de inercia de x. Denotemos $k(x)$, $k(y)$ los cuerpos residuales de x e y.

Entonces, $k(x)$ es una $k(y)$-extensión normal de grupo D/I. Si B es íntegro, π es plano y $k(x)$ es una $k(y)$-extensión separable, entonces la multiplicidad de x en la fibra de y es igual a $|I|$. En este caso, si x no es un punto de ramificación, $k(x)$ es una $k(y)$-extensión de Galois de grupo D.

Demostración. Localizando en y, podemos suponer que y e x son puntos cerrados. Observemos que $\pi^{-1}(y) = \operatorname{Spec} B/\mathfrak{m}_y B = \{x_1, \dots, x_n\} = G \cdot x$. Por el teorema del elemento primitivo, $k(x) = k(y)(\theta)$. Sea $a \in B$ tal que $a(x) = \theta$ y $a(x_i) = 0$ para todo $x_i \neq x$. Tenemos que $P(X) := \prod_{g \in G}(X - g(a)) \in B^G[X] \subset B[X]$ y módulo $\mathfrak{m}_x$, tenemos que $\overline{P(X)} = \prod_{g \in D}(X - g(\theta)) \cdot X^{|G|-|D|} \in k(y)[X]$ es un polinomio que anula a θ y todas sus raíces están en $k(x)$. Por tanto, $k(x)$ es una $k(y)$-extensión normal de grupo un cociente de D, luego de grupo D/I. Si π es plano, entonces el número de puntos de las fibras de π es constante, e igual $|G|$. Como G actúa transitivamente sobre las fibras, el número de puntos distintos de la fibra de y coincide con el orden de G/D. Todos los puntos de una fibra aparecen con la misma multiplicidad y tienen los mismos grados residuales. Luego, si m_x es la multiplicidad con que aparece x en la fibra de y, tenemos que $|G| = m_x \cdot \operatorname{gr}_y x \cdot n = m_x \cdot |D/I| \cdot |G/D|$, luego $m_x = |I|$. □

Sea $\phi\colon A \to B$ un revestimiento entre dominios de Dedekind. Sean Σ_A y Σ_B los cuerpos de fracciones de A y B respectivamente. Supongamos que $\Sigma_A \hookrightarrow \Sigma_B$ es una extensión de Galois de grupo G. Por el teorema de Artin, $\Sigma_B^G = \Sigma_A$ y el grado de ϕ es el orden de G. Sea $x \in \operatorname{Spec} B$ un punto cerrado, e_x el índice de ramificación de x y D el grupo de descomposición de x. Entonces, $|G| = e_x \cdot \operatorname{gr}_y x \cdot |G/D|$ y

$$\boxed{|D| = e_x \cdot \operatorname{gr}_y x}$$

37. Teorema: *Sea A un anillo de enteros tal que su cuerpo de fracciones Σ_A sea una $\mathbb{Q}$-extensión de Galois de grupo G y tal que $G\cdot A = A$. Sea $\mathfrak{m}_x \subset A$ un ideal maximal y sea $(p) = \mathfrak{m}_x \cap \mathbb{Z}$. El automorfismo de Fröbenius, F, de $A/\mathfrak{m}_x$ está inducido por algún automorfismo $F_p \in G$ de A, y éste es único cuando A/pA es reducida (es decir, el morfismo* $\operatorname{Spec} A \to \operatorname{Spec}\mathbb{Z}$ *no ramifica en x), en este caso se dice que F_p es el automorfismo de Fröbenius de Σ_A en el primo p.*

Demostración. Observemos que $A^G = \mathbb{Z}$ porque está incluido en $\mathbb{Q}$ y es finito sobre $\mathbb{Z}$. A es un $\mathbb{Z}$-módulo plano, porque no tiene torsión, y $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo perfecto. Sea $D := \{g \in G : g(x) = x\}$, por el teorema 3.8.36, el morfismo $D \to \operatorname{Aut}_{\mathbb{Z}/p\mathbb{Z}-alg} A/\mathfrak{m}_x = \langle F\rangle$ es epiyectivo (de núcleo I), luego F está inducido por algún automorfismo $F_p \in D$. Además, si x no es un punto de ramificación, $D = \operatorname{Aut}_{\mathbb{Z}/p\mathbb{Z}-alg} A/\mathfrak{m}_x$ y F_p es único. □

38. Observaciones: 1. En el teorema, en la fibra de (p), si en vez de tomar x consideramos otro punto x', entonces como G opera transitivamente en las fibras, existe $g \in G$ de modo que $x' = gx$. Por tanto, el grupo de descomposición de x' es gDg^{-1} y el automorfismo que asociaríamos a F sería gF_pg^{-1}.

2. Si A/pA es reducida y $x_i \in \operatorname{Spec}(A/pA)$, entonces $(A/pA)_{x_i} = A/\mathfrak{m}_{x_i}$. Por tanto, $\mathfrak{m}_{x_i}\cdot A_{x_i} = p\cdot A_{x_i}$. Es decir, todos los puntos de la fibra del ideal primo (p) son no singulares. Si $\bar{A}$ es el cierre entero de A en Σ_A, entonces $A_{x_i} = \bar{A}_{x_i}$, $A/pA = \bar{A}/p\bar{A}$ y el automorfismo de Fröbenius de Σ_A en p no depende del anillo A considerado.

   Sea $\Sigma' \subset \Sigma_A$ una $\mathbb{Q}$-subextensión de Galois y A' el cierre entero de $\mathbb{Z}$ en Σ'. Si $\mathbb{Z} \to \bar{A}$ no ramifica en p, entonces $\mathbb{Z} \to A'$ tampoco, porque si $pA' = \mathfrak{m}_1^{e_1}\cdots\mathfrak{m}_r^{e_r}$, con $e_1 > 1$ entonces la descomposición de $p\bar{A}$ también tendrá algún factor repetido. Además, el automorfismo de Fröbenius, F_p de Σ_A en p, induce en Σ' un automorfismo, que sobre $A'/\mathfrak{m}_1 \subseteq A/\mathfrak{m}_{x_1}$ es el automorfismo de Fröbenius. Por tanto, el automorfismo de Fröbenius de Σ' en p es igual $F_{p\,|\Sigma'}$.

Sea $q(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in \mathbb{Z}[x]$ un polinomio separable y sea G el grupo de Galois de $p(x)$. Consideremos el anillo de enteros $A = \mathbb{Z}[\alpha_1,\dots,\alpha_n]$. Dado un ideal maximal $\mathfrak{m} \subset A$ en la fibra de p, $A/\mathfrak{m} = \mathbb{Z}/p\mathbb{Z}[\bar{\alpha}_1,\dots,\bar{\alpha}_n]$ es el cuerpo de descomposición del polinomio $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$. Como A es un cociente de $\mathbb{Z}[x]/(q(x))^{\otimes n}$, tenemos que A/pA es una $\mathbb{Z}/p\mathbb{Z}$-álgebra separable (es decir, reducida) si y solo si lo es $\mathbb{Z}/p\mathbb{Z}[x]/(\overline{q(x)})$ (es decir, $q(x)$ es separable módulo p). Al automorfismo de Fröbenius F_p asociado a $\mathbb{Q}[\alpha_1,\dots,\alpha_n]$ en p se le denomina también el automorfismo de Fröbenius de $q(x)$ en p.

39. El polinomio $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es separable precisamente en los primos que no dividan al discriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$.

40. Cualquier cuártica $q(x)$ cuyo grupo de Galois sea el grupo de Klein es irreducible, aunque no lo sea módulo cualquier primo p.

41. Si todo automorfismo $g \in G$ deja fija alguna raíz de $q(x)$, entonces $F(\bar{\alpha}_i) = \bar{\alpha}_i$, para algún i. Por tanto, $\overline{q(x)}$ tiene alguna raíz en $\mathbb{Z}/p\mathbb{Z}$.

Considerando $K = \mathbb{Q}[i, \sqrt{2}]$, vemos que el polinomio $(x^2+1)(x^2-2)(x^2+2)$ tiene raíz modular en todo primo p, aunque carece de raíces racionales.

42. El grupo de Galois de la extensión ciclotómica n-ésima, $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ es $(\mathbb{Z}/n\mathbb{Z})^*$: $x^n - 1$ es separable módulo p, cuando p no divide a n. $F(\overline{e^{\frac{2\pi i}{n}}}) = \overline{e^{\frac{2p\pi i}{n}}}$, luego $F_p(e^{\frac{2\pi i}{n}}) = e^{\frac{2p\pi i}{n}}$. Concluimos porque $((\mathbb{Z}/n\mathbb{Z})^*, \cdot) = \langle p \rangle_{\{p<n, \text{ primo y no divide a } n\}}$.

43. Para todo número natural n existen polinomios cuyo grupo de Galois sobre $\mathbb{Q}$ es S_n: Sea $q_2(x)$ un polinomio irreducible de grado n con coeficientes en $\mathbb{Z}/2\mathbb{Z}$, sea $q_3(x)$ un polinomio de grado n separable con coeficientes en $\mathbb{Z}/3\mathbb{Z}$ que contenga una raíz en $\mathbb{Z}/3\mathbb{Z}$ y un factor irreducible de grado $n-1$, y sea $q_5(x)$ un polinomio separable de grado n con coeficientes en $\mathbb{Z}/5\mathbb{Z}$ que admita $n-2$ raíces y tenga un factor irreducible de grado dos. Por el teorema chino de los restos existe un polinomio $q(x)$ de grado n con coeficientes en $\mathbb{Z}$ cuyas reducciones módulo 2, 3 y 5 son $q_2(x)$, $q_3(x)$ y $q_5(x)$, respectivamente. Entonces, F_2 opera transitivamente sobre las raíces de $q(x)$, es decir, es un n-ciclo, F_3 es un $n-1$-ciclo y F_5 es un 2-ciclo. Dejamos que el lector pruebe que $\langle F_2, F_3, F_5 \rangle = S_n$.

44. *Ley de reciprocidad cuadrática de Gauss.* Dado un número primo $q \neq 2$ y un entero $n \in \mathbb{Z}$, si n es un resto cuadrático módulo q (es decir, $\bar{n} = a^2$, para cierto $a \in \mathbb{F}_q$) escribiremos $(\frac{n}{q}) = 1$, en caso contrario escribiremos $(\frac{n}{q}) = -1$. Sea $\mathbb{F}_q^{*2} = \{a^2, a \in \mathbb{F}_q^*\}$, el núcleo del epimorfismo $\mathbb{F}_q^* \to \mathbb{F}_q^{*2}$, $a \mapsto a^2$ es $\{\pm 1\}$. Por tanto, $|\mathbb{F}_q^{*2}| = (q-1)/2$ Luego, $\mathbb{F}_q^{*2}$ es de índice 2 y coincide con el núcleo del epimorfismo $\mathbb{F}_q^* \to \{\pm 1\}$, $a \mapsto a^{\frac{q-1}{2}}$. Así pues, $(\frac{n}{q}) = \bar{n}^{\frac{q-1}{2}} \in \mathbb{F}_q$. Observemos que si $n' = n \mod q$, entonces $(\frac{n'}{q}) = (\frac{n}{q})$, luego podemos suponer $n \leq q$. Además, si $n = r \cdot s$, $(\frac{n}{q}) = (\frac{r}{q}) \cdot (\frac{s}{q})$. Demos un algoritmo de cálculo de $(\frac{n}{q})$, cuando n es primo.

Por una parte, el automorfismo de Fröbenius F_p de $\mathbb{Q}[e^{2\pi i/q}]$ en p, es la identidad en K, cuando F_p esté en el subgrupo de índice 2 de $\mathbb{F}_q^*$, es decir, cuando $\bar{p} \in \mathbb{F}_q^{*2}$.

Por otra parte, si $p \neq 2$, $x^2 - \tilde{q}$ módulo p es separable. Así pues, el automorfismo de Fröbenius de K en p es la identidad cuando $\tilde{q} \in \mathbb{F}_p^{*2}$. Por tanto,

$$(\frac{p}{q}) = (\frac{\tilde{q}}{p}) = (\frac{-1}{p})^{\frac{q-1}{2}} \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot (\frac{q}{p}).$$

Supongamos $p=2$. Desgraciadamente $\mathbb{Z}\hookrightarrow\mathbb{Z}[\sqrt{\tilde{q}}]$ ramifica 2, pero si consideramos el cierre entero de $\mathbb{Z}[\sqrt{\tilde{q}}]$, que es $\mathbb{Z}[\frac{\sqrt{\tilde{q}}+1}{2}]$ ya no ramifica. El polinomio anulador de $\frac{\sqrt{\tilde{q}}+1}{2}$ es $x^2-x-\frac{\tilde{q}-1}{4}\in\mathbb{Z}[x]$ (compruébese que $\tilde{q}=1 \mod 4$, es decir, $\frac{\tilde{q}+1}{2}=1 \mod 2$), que es separable módulo 2. El automorfismo de Fröbenius F_2 de K en 2 es la identidad cuando $\frac{\tilde{q}-1}{4}$ sea múltiplo de 2. Por tanto,

$$(\frac{2}{q})=(-1)^{\frac{\tilde{q}-1}{4}}=(-1)^{\frac{\tilde{q}+1}{2}\cdot\frac{\tilde{q}-1}{4}}=(-1)^{\frac{\tilde{q}^2-1}{8}}=(-1)^{\frac{q^2-1}{8}}.$$

45. Ejercicio: Prueba que un número primo p es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ si y solo si $p=2$ mód 3.

Resolución: p es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ si y solo si $\mathbb{Z}[e^{\frac{2\pi i}{3}}]/(p)=\mathbb{F}_p[x]/(x^2+x+1)$ es íntegro. Si $p=2$ entonces es íntegro, si $p=3$ no es íntegro. Supongamos $p\neq 2,3$. Tenemos que ver cuándo $x^2+x+1\in\mathbb{F}_p[x]$ es irreducible, que equivale a decir que $\sqrt{-3}\notin\mathbb{F}_p$, osea $(\frac{-3}{p})\neq 1$. Por la ley de reciprocidad cuadrática de Gauss

$$(\frac{-3}{p})=(-1)^{\frac{p-1}{2}}\cdot(\frac{3}{p})=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\cdot(\frac{p}{3})=(\frac{p}{3})=p \mod 3$$

que es distinto de $\bar{1}$ si y solo si $p=2 \mod 3$.

3.9. Apéndice: Cálculo tensorial diferencial valorado

Los objetivos de este apéndice son desarrollar el cálculo tensorial diferencial, el cálculo diferencial de orden superior y el cálculo diferencial valorado, desde un punto de vista puramente algebraico.

Para apuntar cómo los resultados de esta sección demuestran los correspondientes resultados de la Geometría Diferencial, digamos solo cómo se obtiene el módulo de diferenciales de una variedad diferenciable a partir del módulo de las diferenciales de Kähler.

Notación: *Sea A un k-álgebra y M un A-módulo. Dados $m,m'\in M$, diremos que $m\sim m'$ si y solo si $\bar{m}=\overline{m'}$ en $M/\mathfrak{m}_x^n M$, para todo $x\in\operatorname{Spec}_{rac}A$ y $n\in\mathbb{N}$.*

Teorema: *Sea $\mathscr{C}^\infty(\mathbb{R}^n)$ la $\mathbb{R}$-álgebra de funciones reales infinito diferenciables de $\mathbb{R}^n$. Se cumple que el morfismo*

$$\Omega_{\mathscr{C}^\infty(\mathbb{R}^n)/\mathbb{R}}/\sim\longrightarrow\mathscr{C}^\infty(\mathbb{R}^n)dx_1\oplus\cdots\oplus\mathscr{C}^\infty(\mathbb{R}^n)dx_n,\ \overline{df}\mapsto\sum_{i=1}^n\frac{\partial f}{\partial x_i}dx_i$$

es un isomorfismo de $\mathscr{C}^\infty(\mathbb{R}^n)$-módulos.

$\Omega_{\mathscr{C}^\infty(X)/\mathbb{R}}/\sim$ *es isomorfo al módulo de diferenciales de* X *de la Geometría Diferencial y*

$$\mathrm{Hom}_{\mathscr{C}^\infty(X)}(\Omega_{\mathscr{C}^\infty(X)/\mathbb{R}}/\sim, \mathscr{C}^\infty(X)) = \mathrm{Hom}_{\mathscr{C}^\infty(X)}(\Omega_{\mathscr{C}^\infty(X)/\mathbb{R}}, \mathscr{C}^\infty(X)) = \mathrm{Der}_{\mathbb{R}}(\mathscr{C}^\infty(X), \mathscr{C}^\infty(X))$$

Además, si X es una variedad diferenciable y $U \subseteq X$ es un abierto, entonces $\mathscr{C}^\infty(U) = \mathscr{C}^\infty(X)_S$, donde $S := \{f \in \mathscr{C}^\infty(X) \colon f(u) \neq 0, \text{ para todo } u \in U\}$.

3.9.1. Derivada de Lie. Fórmula de Cartan

1. Definición: Sea R un álgebra graduada anticonmutativa. Diremos que una aplicación R_0-lineal $D : R \to R$ es una antiderivación de grado r, si $D(R_n) \subseteq R_{n+r}$ para todo n y $D(r_n r_m) = D(r_n) r_m + (-1)^n r_n D(r_m)$.

2. Ejemplo: Sea M un A-módulo y $\Lambda^{\cdot} M = \oplus_{n=0}^{\infty} \Lambda^n M$. Dado $w \in M^* = \mathrm{Hom}_A(M, A)$, el morfismo $i_w : M \otimes_A \overset{n}{\cdots} \otimes_A M \to M \otimes_A \overset{n-1}{\cdots} \otimes_A M$ definido por

$$i_w(m_1 \otimes \cdots \otimes m_n) := \sum_{i=1}^{n} (-1)^{i+1} w(m_i) \cdot w_1 \otimes \cdots \otimes \widehat{m_i} \otimes \cdots \otimes m_n$$

induce por paso al cociente el morfismo

$$i_w : \Lambda^n M \to \Lambda^{n-1} M,\ i_w(m_1 \wedge \cdots \wedge m_n) := \sum_{i=1}^{n} (-1)^i w(m_i) \cdot w_1 \wedge \cdots \wedge \widehat{m_i} \wedge \cdots \wedge m_n$$

El morfismo inducido $i_w : \Lambda^{\cdot} M \to \Lambda^{\cdot} M$ es una antiderivación de grado -1, denominada *contracción interior* por w (sobrentendemos que i_w sobre A es nulo). Si M es un A-módulo libre de rango n, entonces $\Lambda^n M = \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*; A)$, donde $m_1 \wedge \cdots \wedge m_n$ se puede entender como aplicación multilineal hemisimétrica como sigue

$$(m_1 \wedge \cdots \wedge m_n)(w_1, \ldots, w_n) := \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) m_1(w_{\sigma(1)}) \cdots m_n(w_{\sigma(n)}).$$

Dada $w \in M^*$, sea

$$i_{\tilde{w}} : \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*; A) \to \mathrm{Hem}_A(M^*, \overset{n-1}{\ldots}, M^*; A),\ (i_{\tilde{w}} F)(w_2, \ldots, w_n) := F(w, w_2, \ldots, w_n).$$

El lector puede comprobar que via la igualdad $\Lambda^n M = \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*; A)$, $i_w = i_{\tilde{w}}$.

En el caso de que A es una k-álgebra conmutativa, $M = \Omega_{A/k}$ y $D \in M^* = \mathrm{Der}_k(A, A)$, tenemos que

$$i_D(f\, da_1 \wedge \cdots \wedge da_n) = \sum_i (-1)^i f D(a_i) \cdot da_1 \wedge \cdots \wedge \widehat{da_i} \wedge \cdots \wedge da_n$$

3. Lema: *Sea A una k-álgebra. Sean L el A-módulo libre de base (formal) $\{d\mathbf{a}\}_{a\in A}$ y el submódulo de L,*

$$N := \langle d(\mathbf{a}+\mathbf{b}) - d\mathbf{a} - d\mathbf{b}, d(\mathbf{ab}) - ad\mathbf{b} - bd\mathbf{a}, d(\lambda\mathbf{a}) - \lambda d\mathbf{a} \mid \forall a,b \in A, \lambda \in k\rangle.$$

Entonces, $\Omega_{A/k} \simeq L/N$, $adb \mapsto \overline{ad\mathbf{b}}$.

Demostración. Sea M un A-módulo. Entonces,

$$\begin{aligned}\mathrm{Hom}_A(L/N, M) = \{f \in \mathrm{Hom}_A(L,M) \colon f_{|N} = 0\} = \{f \in \mathrm{Aplic}(A,M) \colon f(a+b) = f(a)+f(b),\\ f(\lambda a) = \lambda f(a), f(ab) = af(b) + bf(a) \mid \forall a,b \in A, \lambda \in k\}\\ = \mathrm{Der}_k(A,M) = \mathrm{Hom}_A(\Omega_{A/k}, M)\end{aligned}$$

Luego, $\Omega_{A/k} \simeq L/N$. □

4. Teorema: *El morfismo natural $d \colon A \to \Omega_{A/k}$, $a \mapsto da$ extiende de modo único a una antiderivación de grado 1 del álgebra exterior de $\Omega_{A/k}$ de cuadrado nulo, es decir, existen morfismos únicos $d_i \colon \Lambda^i\Omega_{A/k} \to \Lambda^{i+1}\Omega_{A/k}$, de modo que $d_0 = d$, $d_{i+1} \circ d_i = 0$ y $d_{n+m}(\omega_n \wedge \omega_m) = (d_n\omega_n) \wedge \omega_m + (-1)^n \omega_n \wedge (d_m\omega_m)$, para toda $\omega_n \in \Lambda^n\Omega_{A/k}$ y $\omega_m \in \Lambda^m\Omega_{A/k}$.*

Demostración. Estamos obligados a definir $d_1 \colon \Omega_{A/k} \to \Lambda^2\Omega_{A/k}$, $adb \mapsto da \wedge db$ (que está bien definida por el lema anterior), y en general

$$d_n(w_1 \wedge \cdots \wedge w_n) := \sum_i (-1)^{i-1} \cdot w_1 \wedge \cdots \wedge d_1(w_i) \wedge \cdots \wedge w_n.$$

Obsérvese que $d_n(adb_1 \wedge \cdots \wedge db_n) = da \wedge db_1 \wedge \cdots \wedge db_n$, luego $d_{i+1} \circ d_i = 0$.

□

5. Notación: *Denotaremos $d_n = d$ (si no induce a equivocación), $\Omega^i = \Lambda^i\Omega_{A/k}$, siendo $\Omega^0 = A$. Denotaremos $\Omega^\cdot = \overset{\infty}{\underset{i=0}{\oplus}} \Omega^i$. $\Omega^\cdot$ es un álgebra anticonmutativa con el producto exterior. Diremos que $d \colon \Omega^\cdot \to \Omega^\cdot$ es la diferencial de Cartan.*

6. Proposición: *Sea $D \in \mathrm{Der}_k(A,A) = \mathrm{Hom}_A(\Omega_{A/k}, A)$. Entonces,*

$$\boxed{D^L := i_D \circ d + d \circ i_D}$$

es una derivación de grado cero de $\Omega^\cdot$, que sobre A es D. Diremos que D^L es la derivada de Lie respecto de D.

Demostración. Por ser i_D y d antiderivaciones de grado -1 y 1 respectivamente entonces D^L es una derivación de grado cero (compruébese). □

7. Proposición: $\boxed{D^L \circ d = d \circ D^L}$.

Demostración. $D^L \circ d = (i_D \circ d + d \circ i_D) \circ d = d \circ i_D \circ d$ y $d \circ D^L = d \circ (i_D \circ d + d \circ i_D) = d \circ i_D \circ d$. □

Por tanto, $D^L(a db_1 \wedge \cdots \wedge db_n) = Da \cdot db_1 \wedge \cdots \wedge db_n + \sum_i a db_1 \wedge \cdots \wedge d(Db_i) \wedge \cdots \wedge db_n$.

Dadas $D, D' \in \mathrm{Der}_k(A,A)$, definimos $[D,D'] := D \circ D' - D' \circ D$, que resulta ser una derivación de A. Por otra parte, la derivación D^L sobre $\Omega_{A/k}$ induce de modo natural una derivación, denotémosla también D^L, sobre $\mathrm{Der}_k(A,A) = \mathrm{Hom}_A(\Omega_{A/k}, A)$: dada D' definimos $D^L D$ como sigue, $(D^L D')(w) \overset{*}{:=} D(w(D')) - (D^L w)(D')$, para cada $w \in \Omega_{A/k}$. Se cumple que $D^L D' = [D,D']$: basta comprobar la igualdad para $w = db$,

$$[D,D'](db) = (D \circ D' - D' \circ D)(b)$$
$$(D^L D')(db) = D(db(D')) - (D^L(db))(D') = D(D'b) - (dDb)(D') = D(D'b) - D'(Db)$$

De hecho, podríamos haber definido $D^L D' := [D,D']$, después podríamos haber definido $D^L w$, para toda $w \in \Omega_{A/k}$ (suponiendo que $\Omega_{A/k} = \mathrm{Der}_k(A,A)^*$) y después extenderíamos (de modo único) D^L como derivación sobre el álgebra exterior de $\Omega_{A/k}$. Por último, tendríamos que $D^L = i_D \circ d + d \circ i_D$, porque coinciden sobre $\Omega_{A/k}$.

8. Proposición: *Sean $D, D' \in \mathrm{Der}_k(A,A)$ dos derivaciones. Entonces,*

$$\boxed{D^L \circ i_{D'} - i_{D'} \circ D^L = i_{[D,D']}}$$

sobre $\Omega^{\cdot}$.

Demostración. Por ser D^L una derivación de grado cero y $i_{D'}$ una antiderivación de grado -1. entonces $D^L \circ i_{D'} - i_{D'} \circ D^L$ es una antiderivación de grado -1, que estará determinada por lo que vale sobre $\Omega_{A/k}$, que es $i_{[D,D']}$, por $\overset{*}{=}$. □

9. Fórmula de Cartan: *Dada $w \in \Omega_{A/k}$, entonces*

$$\boxed{(dw)(D,D') = D(w(D')) - D'(w(D)) - w([D,D'])}$$

Demostración. $(dw)(D,D') = i_{D'}(i_D dw) = i_{D'}((D^L - d \circ i_D)(w)) = (D^L \circ i_{D'} - i_{[D,D']})w - D'w(D) = D(w(D')) - w([D,D']) - D'w(D)$. □

Sea E un k-módulo libre de base $\{e_1,\dots,e_n\}$ y sea $\{w_1,\dots,w_n\}$ la base dual. Sea $K := S^{\cdot}_k E^* \otimes_k \Lambda^{\cdot}_k E = \Lambda^{\cdot}_{S^{\cdot}_k E^*}(S^{\cdot}_k E^* \otimes_k E)$ y sea $\mathrm{Id}^\wedge : K \to K$ hacer producto exterior por "el vector general" $\mathrm{Id} = \sum_i w_i \otimes e_i$,

$$\mathrm{Id}^\wedge(s\otimes\Omega_r) = \mathrm{Id}\wedge(s\otimes\Omega_r) := \sum_j w_j\cdot s\otimes e_j\wedge\Omega_r, \quad \forall\, s\otimes\Omega_r \in S^m_k E^*\otimes_k \Lambda^r_k E.$$

Obviamente, $\mathrm{Id}^\wedge\circ\mathrm{Id}^\wedge = 0$.

Consideremos el morfismo

$$i_{\mathrm{Id}} : S^{\cdot}_k E^*\otimes_k \Lambda^{\cdot}_k E \to S^{\cdot}_k E^*\otimes_k \Lambda^{\cdot}_k E, \quad i_{\mathrm{Id}}(s\otimes\Omega_r) := \sum_i i_{e_i} s\otimes i_{w_i}\Omega_r.$$

Claramente, $i_{\mathrm{Id}}\circ i_{\mathrm{Id}} = 0$. Por otra parte, $i_{\mathrm{Id}} : S^r_k E^*\otimes_k \Lambda^s_k E \to S^{r-1}_k E^*\otimes_k \Lambda^{s-1}_k E$ es el morfismo dual del morfismo $\mathrm{Id}^\wedge : S^{r-1}_k E\otimes_k \Lambda^{s-1}_k E^* \to S^r_k E\otimes_k \Lambda^s_k E^*$.

10. Nota: A partir de aquí, en esta subsección, supondremos que k es un cuerpo de característica cero.

11. Teorema: *La sucesión*

$$0\to S^{\cdot}_k E^* \xrightarrow{\mathrm{Id}^\wedge} S^{\cdot}_k E^*\otimes E \xrightarrow{\mathrm{Id}^\wedge} S^{\cdot}_k E^*\otimes\Lambda^2 E \xrightarrow{\mathrm{Id}^\wedge} \cdots \xrightarrow{\mathrm{Id}^\wedge} S^{\cdot}_k E^*\otimes\Lambda^{n-1}E \xrightarrow{\mathrm{Id}^\wedge} S^{\cdot}_k E^*\otimes\Lambda^n E \xrightarrow{\pi} \Lambda^n E\to 0$$

es exacta (donde π es la proyección obvia sobre $S^0E^*\otimes\Lambda^n E = \Lambda^n E$).

Demostración. Dada $s_m\otimes\Omega_r \in S^m_k E^*\otimes_k\Lambda^r_k E$ se cumple que

$$\begin{aligned}(i_{\mathrm{Id}}\circ\mathrm{Id}^\wedge + \mathrm{Id}^\wedge\circ i_{\mathrm{Id}})(s_m\otimes\Omega_r) &= \sum_i i_{\mathrm{Id}}(w_i\cdot s_m\otimes e_i\wedge\Omega_r) + \mathrm{Id}^\wedge(i_{e_i}s_m\otimes i_{w_i}\Omega_r)\\ &= \sum_{ij}(\delta_{ij}s_m + w_i\cdot i_{e_j}s_m)\otimes(\delta_{ij}\Omega_r - e_i\wedge i_{w_j}\Omega_r) + w_j\cdot i_{e_i}s_m\otimes e_j\wedge i_{w_i}\Omega_r\\ &= \sum_{ij}\delta_{ij}s_m\otimes(\delta_{ij}\Omega_r - e_i\wedge i_{w_j}\Omega_r) + w_i\cdot i_{e_j}s_m\otimes\delta_{ij}\Omega_r\\ &= \sum_i (s_m\otimes\Omega_r - s_m\otimes(e_i\wedge i_{w_i}\Omega_r) + w_i\cdot i_{e_i}s_m\otimes\Omega_r) = (n-r+m)\cdot s_m\otimes\Omega_r\end{aligned}$$

Consideremos los morfismos

$$\mathrm{Id}^\wedge_{mr} : S^m_k E^*\otimes_k\Lambda^r_k E \to S^{m+1}_k E^*\otimes_k\Lambda^{r+1}_k E,\ s_m\otimes\Omega_r \mapsto \mathrm{Id}^\wedge(s_m\otimes\Omega_r).$$

Si $s_m\otimes\Omega_r \in \mathrm{Ker}\,\mathrm{Id}^\wedge_{mr}$, entonces

$$(n-r+m)\cdot s_m\otimes\Omega_r = (i_{\mathrm{Id}}\circ\mathrm{Id}^\wedge + \mathrm{Id}^\wedge\circ i_{\mathrm{Id}})(s_m\otimes\Omega_r) = \mathrm{Id}^\wedge\circ i_{\mathrm{Id}}(s_m\otimes\Omega_r) \in \mathrm{Im}\,\mathrm{Id}^\wedge_{m-1r-1}$$

Luego, si $r \neq n$ ó $m \neq 0$, $s_m \otimes \Omega_r \in \operatorname{Im} \mathrm{Id}^{\wedge}_{m-1r-1}$. En consecuencia, como $\mathrm{Id}^{\wedge}$ es cero sobre $S^{\cdot}_k E^* \otimes \Lambda^n E$ es fácil probar que $\mathrm{Id}^{\wedge}(S^{\cdot}_k E^* \otimes \Lambda^{n-1} E) = \underset{i>0}{\oplus} S^i_k E^* \otimes \Lambda^n E$. Con todo, concluimos la exactitud de la sucesión exacta.

□

12. Observación: Se cumple también que la sucesión

$$0 \to \Lambda^n E \to S^{\cdot}_k E^* \otimes \Lambda^n E \xrightarrow{i_{\mathrm{Id}}} S^{\cdot}_k E^* \otimes \Lambda^{n-1} E \xrightarrow{i_{\mathrm{Id}}} S^{\cdot}_k E^* \otimes \Lambda^{n-2} E \xrightarrow{i_{\mathrm{Id}}} \cdots \xrightarrow{i_{\mathrm{Id}}} S^{\cdot}_k E^* \otimes E \xrightarrow{i_{\mathrm{Id}}} S^{\cdot}_k E^* \to 0$$

es exacta.

Consideremos los isomorfismos canónicos $\Lambda^p E \otimes_k \Lambda^n E^* = \Lambda^{n-p} E^*$, luego tenemos el isomorfismo canónico $(S^{\cdot}_k E^* \otimes \Lambda^{\cdot} E) \otimes \Lambda^n E^* = S^{\cdot}_k E^* \otimes \Lambda^{\cdot} E^*$. Los morfismos $\mathrm{Id}^{\wedge}$ y i_{Id} inducen morfismos i_D y d en $S^{\cdot}_k E^* \otimes \Lambda^{\cdot} E^*$, que explícitamente son

$$\begin{aligned} i_D(s_m \otimes \Omega_r) &= \textstyle\sum_i w_i \cdot s_m \otimes i_{e_i} \Omega_r \\ d(s_m \otimes \Omega_r) &= \textstyle\sum_i i_{e_i} s_m \otimes w_i \wedge \Omega_r \end{aligned}$$

Observemos que $\mathrm{Der}_k(S^{\cdot} E^*, S^{\cdot} E^*) = \mathrm{Hom}_k(E^*, S^{\cdot} E^*) = E \otimes S^{\cdot} E^*$. Por tanto,

$$S^{\cdot} E^* \otimes_k E^* = \Omega_{S^{\cdot} E^*/k},\ 1 \otimes w \mapsto dw$$

y $S^{\cdot} E^* \otimes_k \Lambda^{\cdot} E^* = \Omega^{\cdot}_{S^{\cdot} E^*/k}$. En esta situación, el morfismo d de $S^{\cdot} E^* \otimes_k \Lambda^{\cdot} E^*$ se corresponde con la diferencial de Cartan de $\Omega^{\cdot}_{S^{\cdot} E^*/k}$ y el morfismo i_D de $S^{\cdot} E^* \otimes_k \Lambda^{\cdot} E^*$ con la contracción por "el campo de las homotecias", $D = \sum_i w_i \partial_{w_i}$. Además, $S^{\cdot} E^* = k[x_1, \ldots, x_n]$. Por 3.9.12, obtenemos el teorema de De Rham.

13. Teorema de De Rham: *La sucesión*

$$0 \to k \to k[x_1, \ldots, x_n] \xrightarrow{d} \Omega_{k[x_1,\ldots,x_n]/k} \xrightarrow{d} \Omega^2_{k[x_1,\ldots,x_n]/k} \xrightarrow{d} \cdots \xrightarrow{d} \Omega^{n-1}_{k[x_1,\ldots,x_n]/k} \xrightarrow{d} \Omega^n_{k[x_1,\ldots,x_n]/k} \xrightarrow{d} 0$$

es exacta

14. Ejercicio: Sea $A = k[x, 1/x]$. Prueba que $\frac{dx}{x} \in \Omega_{A/k}$ es cerrada (su diferencial es nula) pero no es exacta (es distinta de da, para todo $a \in A$).

3.9.2. Cálculo diferencial valorado. Identidades de Bianchi

15. Definición: Sea M un A-módulo. Una aplicación $d : M \to M \otimes_A \Omega_{A/k}$ diremos que es una diferencial en M, si

1. $d(m + m') = dm + dm'$, para todo $m, m' \in M$.

2. $d(am) = adm + m \otimes da$, para todo $a \in A$ y $m \in M$.

16. Ejemplo: La diferencial canónica $d: A \to \Omega_{A/k} = A \otimes_A \Omega_{A/k}, a \mapsto da$, es una diferencial en A.

17. Ejemplo: Sea M un A-módulo libre de base $\{m_1, \ldots, m_r\}$. La aplicación

$$d: M \to M \otimes \Omega,\ d(\sum_i a_i \cdot m_i) := \sum_i m_i \otimes da_i$$

es una diferencial.

18. Proposición: *Sea M un A-módulo y d una diferencial en M. Entonces,*

$$[\textit{Conjunto de diferenciales de } M] = d + \mathrm{Hom}_A(M, M \otimes_A \Omega), \quad d' \mapsto d + (d' - d).$$

Demostración. Es inmediata. □

Si M es un A-módulo libre de base $\{m_1, \ldots, m_r\}$, $\Omega_{A/k}$ es una A-módulo libre de base $da_1, \ldots, da_n$ y d es una diferencial entonces $d(m_i) = \sum_{jk} \Gamma_{ij}^k m_j \otimes da_k$ y los $\Gamma_{ij}^k \in A$ determinan la diferencial d.

Dadas $m \otimes \Omega_i \in M \otimes \Omega^i$ y $m' \otimes \Omega_j \in M' \otimes \Omega^j$ definamos

$$(m \otimes \Omega_i) \wedge (m' \otimes \Omega_j) := m \otimes m' \otimes \Omega_i \wedge \Omega_j \in M \otimes M' \otimes \Omega^{i+j}.$$

Tenemos un morfismo

$$\begin{array}{ccc} (M \otimes \Omega^\cdot) \otimes (M' \otimes \Omega^\cdot) & \stackrel{\wedge}{\to} & M \otimes M' \otimes \Omega^\cdot \\ w_i \otimes w_j & \mapsto & w_i \wedge w_j \end{array}$$

La diferencial $d: M \to M \otimes \Omega_{A/k}$ extiende a la aplicación

$$d: M \otimes \Omega^\cdot \to M \otimes \Omega^\cdot,\ d(m \otimes \Omega_i) := dm \wedge \Omega_i + m \otimes d\Omega_i.$$

Los elementos de $M \otimes \Omega^i$ los llamaremos i-formas valoradas en M.

Dada otra diferencial $d: M' \to M' \otimes \Omega$, podemos definir la diferencial en $M \otimes M'$,

$$d: M \otimes_A M' \to M \otimes_A M' \otimes_A \Omega,\ d(m \otimes m') := dm \wedge m' + m \wedge dm',$$

que extiende a un morfismo $d: M \otimes_A M' \otimes_A \Omega^\cdot \to M \otimes_A M' \otimes_A \Omega^\cdot$.

Se cumple que

$$\boxed{d(w_i \wedge w'_j) = dw_i \wedge w'_j + (-1)^i w_i \wedge dw'_j},$$

para toda $w_i \in M \otimes \Omega^i$ y $w'_j \in M' \otimes \Omega^j$. Dado $D \in \mathrm{Der}_k(A,A)$, sea $i_D : M \otimes \Omega^\cdot \to M \otimes \Omega^\cdot$, $i_D(m \otimes \Omega_i) = m \otimes i_D \Omega_i$. Obviamente,

$$\boxed{i_D(w_i \wedge w'_j) = i_D w_i \wedge w'_j + (-1)^i w_i \wedge i_D w'_j}$$

Definamos $\boxed{D^L := i_D \circ d + d \circ i_D}$, que es una derivación, es decir,

$$\boxed{D^L(w_i \wedge w'_j) = D^L w_i \wedge w'_j + w_i \wedge D^L w'_j}$$

Es sencillo comprobar que

$$\boxed{D^L \circ i_{D'} - i_{D'} \circ D^L = i_{[D,D']}}$$

19. Definición: Una conexión ∇ en un A-módulo M es una aplicación

$$\mathrm{Der}_k(A,A) \times M \to M, (D,m) \mapsto D^\nabla m,$$

que cumple para todo $a \in A$, $m, m' \in M$, $D, D' \in \mathrm{Der}_k(A,A)$,

1. $(D+D')^\nabla m = (D^\nabla m) + (D'^\nabla m)$.
2. $(aD)^\nabla m = a(D^\nabla m)$.
3. $D^\nabla(am) = (Da) \cdot m + aD^\nabla m$.
4. $D^\nabla(m+m') = D^\nabla m + D^\nabla m'$.

20. Notación: A partir de ahora, supondremos que $\Omega_{A/k}$ es un A-módulo finito generado proyectivo (como sucede cuando $X = \mathrm{Spec}\, A$ es una variedad lisa).

$\Omega_{A/k}$ y $\mathrm{Der}_k(A,A)$ son duales entre sí. Además,

$$\Omega^i = \mathrm{Hem}_A(\mathrm{Der}_k(A,A), \overset{i}{\ldots}, \mathrm{Der}_k(A,A); A),$$

luego $M \otimes_A \Omega^i = \mathrm{Hem}_A(\mathrm{Der}_k(A,A), \overset{i}{\ldots}, \mathrm{Der}_k(A,A); M)$: $m \otimes \Omega_i \in M \otimes_A \Omega^i$ es la aplicación multilineal hemisimétrica $(m \otimes \Omega_i)(D_1, \ldots, D_i) := \Omega_i(D_1, \ldots, D_i) \cdot m$.

21. Proposición: *Existe una correspondencia biunívoca entre conexiones en M y diferenciales de M.*

Demostración. Dada una diferencial $d\colon M \to M \otimes_A \Omega_{A/k}$, le asignamos la conexión ∇ definida por $D^\nabla m := i_D(dm)$, que cumple que

$$D^\nabla(am) = i_D(d(am)) = i_D(m \otimes da + adm) = (Da)m + a i_D dm = (Da)m + aD^\nabla m$$

y las demás propiedades exigidas a las conexiones.

Recíprocamente, dada la conexión ∇ sea $d(m)$, tal que $dm(D) = D^\nabla m$, para toda derivación D.

□

22. Dada una 1-forma valorada $w \in M \otimes \Omega$, tenemos que

$$(dw)(D_1,D_2) = i_{D_2}(i_{D_1}dw) = i_{D_2}(D_1^L w - d(w(D_1))) = D_1^\nabla(w(D_2)) - D_2^\nabla(w(D_1)) - w([D_1,D_2])$$

En particular,

$$d^2(m)(D_1,D_2) = D_1^\nabla D_2^\nabla m - D_2^\nabla D_1^\nabla m - [D_1,D_2]^\nabla m.$$

23. Definición: El morfismo A-lineal $d^2\colon M \to M \otimes \Omega^2$ diremos que es el tensor de curvatura.

Si tenemos dos módulos M,N con sendas diferenciales, podemos definir en el A-módulo $\mathrm{Hom}_A(M,N)$ una diferencial:

$$d\colon \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N) \otimes \Omega = \mathrm{Hom}_A(M, N \otimes \Omega)$$

$d(T)(m) := d(T(m)) - T(dm)$ ($T\colon M \otimes \Omega^\cdot \to N \otimes \Omega^\cdot$, $T(m \otimes \Omega_i) := T(m) \otimes \Omega_i$). Explicitemos la conexión: $(D^\nabla T)(m) = dT(D,m) = (d(T(m)) - (T(dm))(D) = D^\nabla(T(m)) - T((dm)(D)) = D^\nabla(T(m)) - T(D^\nabla m)$.

Un morfismo $T\colon M \to M'$ de A-módulos diremos que es diferencial si $dT = 0$, es decir, $d \circ T = T \circ d$. Si el morfismo T es diferencial, entonces $T\colon M \otimes \Omega^\cdot \to M' \otimes \Omega^\cdot$ conmuta con d, i_D y D^L. El morfismo $\mathrm{Hom}_A(M,N) \otimes M \to N$, $\phi \otimes m \mapsto \phi(m)$, resulta ser diferencial. Cuando tengamos una n-forma w_n valorada en $\mathrm{Hom}_A(M,N)$ y otra m-forma w_m valorada en N, entendemos vía este morfismo que $w_n \wedge w_m$ es una $n+m$-forma valorada en N.

Denotaré por $R \in \mathrm{End}_A(M) \otimes \Omega^2 = \mathrm{Hom}_A(M, M \otimes \Omega^2)$ a la 2-forma valorada en $\mathrm{End}_A(M)$ correspondiente a d^2, es decir, $\boxed{R \wedge m = d^2 m}$. Observemos que

$$R(D_1,D_2,m) = d^2(m)(D_1,D_2) = D_1^\nabla D_2^\nabla m - D_2^\nabla D_1^\nabla m - [D_1,D_2]^\nabla m.$$

24. Proposición: *Dada $w \in M \otimes \Omega^i$, entonces*

$$\boxed{d^2 w = R \wedge w}$$

Demostración. Escribamos $w = m \otimes \Omega_i$. Entonces, $d^2(m \otimes \Omega_i) = d(dm \wedge \Omega_i + m \otimes d\Omega_i) = d^2m \wedge \Omega_i - dm \wedge d\Omega_i + dm \wedge d\Omega_i + m \otimes d^2\Omega_i = d^2m \wedge \Omega_i = R \wedge w$. □

Dado $S \in \mathrm{Hom}_A(M, N \otimes \Omega^n)$, consideremos el diagrama

$$\begin{array}{ccc} M & \xrightarrow{S} & N \otimes \Omega^n \\ {\scriptstyle d}\downarrow & & \downarrow{\scriptstyle d} \\ M \otimes \Omega & \xrightarrow[S \wedge \mathrm{Id}]{} & N \otimes \Omega^{n+1} \end{array} \qquad (S \wedge \mathrm{Id})(m \otimes w) := S(m) \wedge w$$

Sea $dS := d \circ S - (S \wedge \mathrm{Id}) \circ d \in \mathrm{Hom}_A(M, N \otimes \Omega^{n+1})$. La diferencial dS coincide con la diferencial de S como elemento de $\mathrm{Hom}_A(M,N) \otimes \Omega^n \subset \mathrm{Hom}_A(M,N) \otimes \Omega^{\cdot}$.

25. Identidad diferencial de Bianchi: $dR = 0$.

Demostración. La diferencial del morfismo $M \xrightarrow{d^2} M \otimes \Omega^2$ es nula ya que el cuadrado

$$\begin{array}{ccc} M & \xrightarrow{d^2} & M \otimes \Omega^2 \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ M \otimes \Omega & \xrightarrow{d^2} & M \otimes \Omega^3 \end{array}$$

es conmutativo. □

26. Definición: Una conexión sobre $M = \mathrm{Der}_k(A,A)$ se llama conexión lineal.

27. Definición: Sea ∇ una conexión lineal. Pensemos el endomorfismo identidad

$$\mathrm{Id} \in \mathrm{Hom}_A(\mathrm{Der}_k(A,A), \mathrm{Der}_k(A,A)) = \mathrm{Der}_k(A,A) \otimes \Omega$$

como una 1-forma valorada. Definimos $\mathrm{Tor}_\nabla := d\,\mathrm{Id} \in \mathrm{Der}_k(A,A) \otimes \Omega^2$.

Explícitamente,

$$\begin{aligned} \mathrm{Tor}_\nabla(D_1, D_2) = (d\,\mathrm{Id})(D_1, D_2) &= D_1^\nabla(\mathrm{Id}(D_2)) - D_2^\nabla(\mathrm{Id}(D_1)) - \mathrm{Id}([D_1, D_2]) \\ &= D_1^\nabla D_2 - D_2^\nabla D_1 - [D_1, D_2] \end{aligned}$$

Observemos que la curvatura R pertenece a $\mathrm{End}_A(\mathrm{Der}_k(A,A)) \otimes_A \Omega^2$.

28. Definición: Se dice que una conexión lineal ∇ es simétrica si $\mathrm{Tor}_\nabla = 0$.

29. Identidad lineal de Bianchi: *Si ∇ es una conexión lineal simétrica, entonces*

$$R \wedge \mathrm{Id} = 0$$

Demostración. $0 = d(\mathrm{Tor}_\nabla) = d^2(\mathrm{Id}) = R \wedge \mathrm{Id}$. □

Interpretemos esta igualdad:

$$\begin{aligned} 0 &= R \wedge \mathrm{Id}(D_1,D_2,D_3) = (i_{D_1}(R \wedge \mathrm{Id}))(D_2,D_3) = (i_{D_1}R) \wedge \mathrm{Id} + R \wedge i_{D_1}\mathrm{Id})(D_2,D_3) \\ &= R(D_1,D_2)(\mathrm{Id}(D_3)) - R(D_1,D_3)(\mathrm{Id}(D_2)) + R(D_2,D_3)(\mathrm{Id}(D_1)). \end{aligned}$$

Luego,

$$\boxed{R(D_1,D_2)(D_3) + R(D_3,D_1)(D_2) + R(D_2,D_3)(D_1) = 0}$$

30. Proposición: *Sea ∇ una conexión lineal, $d^\nabla\colon \Omega \to \Omega\otimes\Omega$ la diferencial definida por ∇ y $\pi\colon \Omega\otimes\Omega \to \Omega^2$ el morfismo natural de paso al cociente. Sea d_C la diferencial de Cartan. Se cumple que*

$$\pi \circ d^\nabla + d_C = \mathrm{Tor}_\nabla \in \mathrm{Der}_k(A,A)\otimes\Omega^2$$

Por tanto, una conexión lineal es simétrica si y solo si $\pi \circ d^\nabla = -d_C$.

Demostración. Tenemos que

$$\begin{aligned} \pi(d^\nabla w)(D_1,D_2) &= (d^\nabla w)(D_1,D_2) - (d^\nabla w)(D_2,D_1) = (D_2^\nabla w)(D_1) - (D_1^\nabla w)(D_2) \\ &= D_2(w(D_1)) - w(D_2^\nabla D_1) - D_1(w(D_2)) + w(D_1^\nabla D_2). \end{aligned}$$

Por la fórmula de Cartan, $d_C(w)(D_1,D_2) = D_1(w(D_2)) - D_2(w(D_1)) - w([D_1,D_2])$. Por tanto, $(\pi\circ d^\nabla + d_C)(w,D_1,D_2) = \mathrm{Tor}_\nabla(w,D_1,D_2)$. □

Supongamos $\mathrm{car}\, k \neq 2$.

Si definimos $D^{\nabla_s}D' := D^\nabla D' - \frac{1}{2}\mathrm{Tor}_\nabla(D,D') = \frac{1}{2}(D^\nabla D' + D'^\nabla D + [D,D'])$, se tiene que ∇_s es simétrica.

31. Proposición: *Tenemos la correspondencia biunívoca*

$$\begin{array}{rcl} \{\textit{Conexiones lineales}\} & = & [\textit{Conexiones lineales simétricas}\} \times \mathrm{Der}_k(A,A)\otimes_A\Omega^2 \\ \nabla & \mapsto & (\nabla_s, \mathrm{Tor}_\nabla) \end{array}$$

Demostración. La aplicación inversa asigna a una conexión lineal simétrica ∇_s y una dos forma valorada $w_2 \in \mathrm{Der}_k(A,A)\otimes\Omega^2$, la conexión lineal definida por $D^\nabla D' := D^{\nabla_s}D' + \frac{1}{2}w_2(D,D')$. □

Consideremos el morfismo canónico $\pi_2\colon \Omega\otimes\Omega \to S^2\Omega$. Dada una conexión lineal simétrica y el morfismo diferencial $d^\nabla\colon \Omega \to \Omega\otimes\Omega$, sea $d_s^\nabla\colon \Omega \to S^2\Omega$ el morfismo $d_s^\nabla := \pi_2 \circ d^\nabla$. Explícitamente,

$$\begin{aligned} d_s^\nabla(w)(D_1,D_2) &= (D_1^\nabla w)(D_2) + (D_2^\nabla w)(D_1) = D_1(w(D_2)) - w(D_1^\nabla D_2) + D_2(w(D_1)) - (D_2^\nabla D_1) \\ &= D_1(w(D_2)) + D_2(w(D_1)) - w(D_1^\nabla D_2 + D_2^\nabla D_1). \end{aligned}$$

Se cumple que d_s^∇ es k-lineal y $d_s^\nabla(f\cdot w)=(df)\cdot w+f\cdot d_s^\nabla w$ y diremos que d_s^∇ es una diferencial simétrica.

32. Proposición: *Tenemos la correspondencia biunívoca*

$$\begin{array}{ccc}\{\textit{Conexiones lineales simétricas}\} & = & \{\textit{Diferenciales. simétricas } d_s\colon \Omega\to S^2\Omega\}\\ \nabla & \mapsto & d_s^\nabla\end{array}$$

Demostración. La aplicación inversa asigna a la diferencial simétrica d_s, la conexión lineal simétrica cuya diferencial es $d=\frac{1}{2}(d_s-d_C)\colon \Omega\to\Omega\otimes\Omega$ (donde $d_s(w)(D_1,D_2):=i_{D_1}(i_{D_2}d_s w)$). □

La diferencial simétrica d_s extiende a un morfismo k-lineal

$$d_s\colon S^\cdot\Omega\to S^\cdot\Omega,\ d_s(w_1\cdots w_m):=\sum_i w_1\cdot\cdots d_s w_i\cdots w_m,$$

(para $m=0$ definimos $d_s=d$), que cumple

1. $d_s(f\cdot s_n)=d_s(f)\cdot s_n+f\cdot d_s(s_n)$, para toda $f\in A$ y $s_n\in S^n\Omega$.
2. $d_s(s_n\cdot s_m)=d_s(s_n)\cdot s_m+s_n\cdot d_s(s_m)$, para toda $s_n\in S^n\Omega$ y $s_m\in S^m\Omega$.

Se dice que $\frac{d_s^2 f}{2}$ es el Hessiano de f.
Dada una conexión lineal ∇, $S^\cdot\Omega$ es un módulo diferencial:

$$D^\nabla(w_1\cdots w_r):=\sum_{i=1}^r w_1\cdots D^\nabla w_i\cdots w_r,\ \text{para todo } w_i\in\Omega \text{ y } D\in \mathrm{Der}_k(A,A).$$

33. Proposición: *Sean $s_m,s_{m'}\in S^m\Omega$ y $D,D_1,\ldots,D_m\in\mathrm{Der}_k(A,A)$. Se cumple que*

1. $D^\nabla(s_m\cdot s_{m'})=D^\nabla s_m\cdot s_{m'}+s_m\cdot D^\nabla s_{m'}$.
2. $(D^\nabla s_m)(D_1,\ldots,D_m)=D(s_m(D_1,\ldots,D_m))-\sum_{i=1}^m s_m(D_1,\ldots,D^\nabla D_i,\ldots,D_m)$.
3. $d_s s_m(D_1,\ldots,D_{m+1})=\sum_{i=1}^{m+1}(D_i^\nabla s_m)(D_1,\ldots,\widehat{D_i},\ldots,D_{m+1})$.

Demostración. Compruébese con $s_m=w_1\cdots w_m$, $s_{m'}=w'_1\cdots w'_{m'}$ y $w_i,w'_j\in\Omega$. □

3.9.3. Módulos de jets y operadores diferenciales

Sea A una k-álgebra y sean M y N dos A-módulos. Se dice que una aplicación k-lineal $F\colon N \to M$ es un operador diferencial de orden 0 si $F(an) = a \cdot F(n)$, para todo $a \in A$ y $n \in N$, es decir, si F es un morfismo de A-módulos.

34. Definición: Una aplicación k-lineal $F\colon N \to M$ se dice que es un operador diferencial de orden $n-1$ si

$$\sum_{\{i_1,\ldots,i_r\}\cup\{j_1,\ldots,j_{n-r}\}=\{1,\ldots,n\}} (-1)^r a_{i_1}\cdots a_{i_r}\cdot F(a_{j_1}\cdots a_{j_{n-r}}\cdot n) = 0$$

para todo $a_1,\ldots,a_n \in A$ y $n \in N$.

35. Ejemplo: Las derivaciones $D \in \mathrm{Der}_k(A,M)$ son operadores diferenciales de orden 1.

36. Proposición: *$F\colon N \to M$ es un operador diferencial de orden $n > 0$ si y solo si $[F,a] := F\circ a\cdot - a\cdot F$ es un operador diferencial de orden $n-1$ para todo $a \in A$.*

37. Proposición: *La composición de un operador diferencial de orden r con uno de orden s es un operador diferencial de orden $r+s$.*

Demostración. Sea $F\colon N \to M$ un operador diferencial de orden r y $G\colon M \to M'$ un operador diferencial de orden s. Procedamos por inducción sobre $r+s$. Por hipótesis de inducción

$$[a,G\circ F] = a\cdot G\circ F - G\circ F\circ a\cdot = (a\circ G\circ F - G\circ a\cdot\circ F) + (G\circ a\cdot\circ F - G\circ a\cdot\circ F) = [a,G]\circ F + G\circ[a,F]$$

es un operador diferencial de orden $r+s-1$, luego $G\circ F$ es un operador diferencial de orden $r+s$.

□

38. Notación: $\mathrm{Diff}^n_k(N,M)$ denota el conjunto de operadores diferenciales de N en M de orden n.

39. Proposición: *Sea $\mathfrak{m} \subset A$ un ideal tal que $A/\mathfrak{m} = k$. Supongamos que M es un $A/\mathfrak{m}$-módulo. Entonces,*

$$\mathrm{Diff}^n_k(N,M) = \mathrm{Hom}_k(N/\mathfrak{m}^{n+1}\cdot N, M)$$

Demostración. Todo operador diferencial $F\colon N \to M$ de orden n se anula en $\mathfrak{m}^{n+1}\cdot N$ (recordemos que $\mathfrak{m}\cdot M = 0$), por la definición de operador diferencial de orden n. Por tanto, F factoriza vía $N/\mathfrak{m}^{n+1}\cdot N$.

Para el recíproco procedamos por inducción sobre n. Sea $F\colon N \to M$ una aplicación lineal que factorice vía $N/\mathfrak{m}^{n+1}\cdot N$, es decir, que se anule en $\mathfrak{m}^{n+1}\cdot N$. $[F,a]$ se anula en $\mathfrak{m}^n\cdot N$: si $a\in\mathfrak{m}$ entonces $[F,a](\mathfrak{m}^n\cdot N)\subset F(\mathfrak{m}^{n+1}\cdot N)+\mathfrak{m}\cdot F(N)=0$, luego $[F,a]=0$; si $a\in k$, obviamente $[F,a]=0$. Por hipótesis de inducción, $[F,a]$ es un operador diferencial de orden $n-1$. Luego F es un operador diferencial de orden n.

□

40. Definición: Sea N un A-módulo. Diremos que

$$J^n_{N/k} := (A\otimes_k A/\Delta^{n+1})\otimes_A N$$

es el módulo de r-jets de N ($a\cdot(\overline{a_1\otimes a_2}\otimes n) = \overline{aa_1\otimes a_2}\otimes n$ y $\overline{a_1\otimes a_2 a}\otimes n = \overline{a_1\otimes a_2}\otimes an$, para todo $\overline{a_1\otimes a_2}\otimes n\in J^n_{N/k}$ y $a\in A$).

41. Proposición: *Sea $\mathfrak{m}\subset A$ un ideal tal que $A/\mathfrak{m}=k$ y sea M un A-módulo. Entonces,*

$$(J^n_{M/k})\otimes_A A/\mathfrak{m} = M/\mathfrak{m}^{n+1}\cdot M$$

Demostración. Recordemos que $\Delta\otimes_A A/\mathfrak{m}=\mathfrak{m}$, luego

$$(J^n_{M/k})\otimes_A A/\mathfrak{m} = (J^n_{A/k}\otimes_A A/\mathfrak{m})\otimes_A M = A/\mathfrak{m}^{n+1}\otimes_A M = M/\mathfrak{m}^{n+1}\cdot M$$

□

Sea $j^r_N\colon N\to J^r_{N/k}$, $j^r_N(n) := \overline{1\otimes n}$.

42. Proposición: *Se cumple que*

$$\mathrm{Hom}_A(J^n_{N/k},M) = \mathrm{Diff}^n_k(N,M),\ F\mapsto F\circ j^n_N$$

En particular, $\mathrm{Hom}_A(J^n_{A/k},A) = \mathrm{Diff}^n_k(A,A)$.

Demostración. $A\otimes_k A$ es una A-álgebra, $A\to A\otimes_k A$, $a\mapsto a\otimes 1$. Consideremos $A\otimes_k N$ como $A\otimes A$-módulo de modo natural. M es un $A\otimes_k A/\Delta = A$-módulo. Observemos que $\mathrm{Diff}^n_k(N,M) = \mathrm{Diff}^n_A(A\otimes_k N,M)$, $D\mapsto \mathrm{Id}\otimes D$, luego

$$\begin{aligned}\mathrm{Diff}^n_k(N,M) = \mathrm{Diff}^n_A(A\otimes_k N,M) &\overset{3.9.39}{=} \mathrm{Hom}_A((A\otimes_k N)/(\Delta^{n+1}\cdot(A\otimes_k N)),M)\\ &= \mathrm{Hom}_A((A\otimes_k A/\Delta^{n+1})\otimes_A N,M) = \mathrm{Hom}_A(J^n_{N/k},M).\end{aligned}$$

□

43. Tenemos que

$$\mathrm{Diff}^n_k(N,M) = \mathrm{Hom}_A(J^n_{N/k}, M) = \mathrm{Hom}_A(N, \mathrm{Hom}_A(J^n_{A/k}, M)) = \mathrm{Hom}_A(N, \mathrm{Diff}^n_k(A,M)).$$

Explícitamente, a $D \in \mathrm{Diff}^n_k(N,M)$ le asignamos $\tilde{D} \in \mathrm{Hom}_A(N, \mathrm{Diff}^n_k(A,M))$, definido por $\tilde{D}(n)(a) := D(an)$.

La composición,

$$N \xrightarrow{j^r_N} J^r_{N/k} \xrightarrow{j^s_{J^r_{N/k}}} J^s_{J^r_{N/k}/k} = J^s_{A/k} \otimes_A J^r_{N/k}$$

es un operador diferencial de orden $r+s$, que induce un morfismo $J^{r+s}_{N/k} \to J^s_{A/k} \otimes_A J^r_{N/k}$, que dualmente es el morfismo $\mathrm{Diff}^s_k(N, \mathrm{Diff}^r_k(A,M)) \to \mathrm{Diff}^{r+s}_k(N,M)$, $D \mapsto \tilde{D}$, $\tilde{D}(n) := D(n)(1)$.

Consideremos la cadena de inclusiones (en $\mathrm{Hom}_k(A,A)$)

$$\mathrm{Diff}^1_k(A,A) \hookrightarrow \mathrm{Diff}^2_k(A,A) \hookrightarrow \cdots \hookrightarrow \mathrm{Diff}^n_k(A,A) \hookrightarrow \cdots$$

44. Definición: $\mathrm{Diff}_k(A,A) = \bigcup_{i=0}^{\infty} \mathrm{Diff}^i_k(A,A)$.

45. Proposición: *Si $X = \mathrm{Spec}\, A$ es una variedad lisa, el epimorfismo natural*

$$S^n_A(\Delta/\Delta^2) \to \Delta^n/\Delta^{n+1}$$

es isomorfismo.

Demostración. Por cambio de cuerpo base podemos suponer que k es algebraicamente cerrado. Podemos suponer que X es conexa, luego íntegra. X es una variedad regular porque es lisa (4.3.14). Entonces, sabemos por 4.3.5 que $S^n_A(\Delta/\Delta^2) \otimes_A A/\mathfrak{m}_x = S^n_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = \mathfrak{m}_x^n/\mathfrak{m}_x^{n+1} = (\Delta^n/\Delta^{n+1}) \otimes_A A/\mathfrak{m}_x$, para todo punto cerrado $x \in X$. Por tanto, si $r = \dim X$, que es el rango del A-módulo localmente libre Δ/Δ^2, entonces

$$\dim_{A/\mathfrak{m}_x}((\Delta^n/\Delta^{n+1}) \otimes_A A/\mathfrak{m}_x) = \binom{n+r-1}{r-1},$$

que no depende del punto cerrado x. Luego, Δ^n/Δ^{n+1} es localmente libre de rango $\binom{n+r-1}{r-1}$ y el epimorfismo natural es isomorfismo.

□

46. Notación: A partir de ahora supondremos que $X = \mathrm{Spec}\, A$ es lisa y que $\mathrm{car}\, k = 0$.

47. Definición: El dual de la sucesión exacta

$$0 \to S^n\Omega \to (A\otimes A)/\Delta^{n+1} \to (A\otimes A)/\Delta^n \to 0$$

es la sucesión exacta

$$0 \to \mathrm{Diff}_k^{n-1}(A,A) \to \mathrm{Diff}_k^n(A,A) \overset{\mathrm{simb}_n}{\to} S^n \mathrm{Der}_k(A,A) \to 0$$

Se dice que $\mathrm{simb}_n(F)$ es el símbolo del operador $F \in \mathrm{Diff}_k^n(A,A)$.

Tenemos que $\mathrm{Diff}_k^n(A,A) \simeq \mathrm{Diff}_k^{n-1}(A,A) \oplus S^n \mathrm{Der}_k(A,A) \simeq \cdots \simeq \oplus_{i=0}^n S^i \mathrm{Der}_k(A,A)$.

48. Proposición: *Sean $D_1,\ldots,D_r \in \mathrm{Der}_k(A,A)$. Entonces,*

1. $\mathrm{simb}_r(D_1\circ\cdots\circ D_r) = D_1\cdots D_r$.
2. $\mathrm{simb}_r(D_1\circ\cdots\circ D_s) = 0$, *para $s<r$.*

Demostración. Para $s<r$, $D_1\circ\cdots\circ D_s \in \mathrm{Diff}_k^{r-1}(A,A)$, luego $\mathrm{simb}_r(D_1\circ\cdots\circ D_s)=0$. Para $s=r$,

$$\begin{aligned}\mathrm{simb}_r(D_1\circ\cdots\circ D_r)(da_1\cdots da_r) &= (D_1\circ\cdots\circ D_r)((a_1\otimes 1-1\otimes a_1)\cdots(a_r\otimes 1-1\otimes a_r))\\ &= (1\otimes(D_1\circ\cdots\circ D_r))((a_1\otimes 1-1\otimes a_1)\cdots(a_r\otimes 1-1\otimes a_r))\\ &= ((1\otimes D_1)\circ\cdots\circ(1\otimes D_r))((a_1\otimes 1-1\otimes a_1)\cdots(a_r\otimes 1-1\otimes a_r))\\ &= \sum_{\sigma\in S_n} D_{\sigma(1)}a_1\cdots D_{\sigma(n)}a_n = (D_1\cdots D_r)(da_1\cdots da_r).\end{aligned}$$

□

Sea $\{D_1,\ldots,D_n\}$ una base de $\mathrm{Der}_k(A,A)$. Dado $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n$, denotamos $|\alpha| = \alpha_1+\cdots+\alpha_n$ y $D^\alpha = D_1\circ\overset{\alpha_1}{\cdots}\circ D_1\circ\cdots\circ D_n\circ\overset{\alpha_n}{\cdots}\circ D_n$. El lector puede comprobar que dado $F\in\mathrm{Diff}_k^r(A,A)$, existen $a_\alpha\in A$ únicos de modo que

$$F = \sum_{|\alpha|\le r} a_\alpha\cdot D^\alpha$$

y $\mathrm{simb}_r(F) = \sum_{|\alpha|=r} a_\alpha D^{\alpha_1}\cdots D^{\alpha_r}$.

Sea $\mathrm{Diff}_+^r(A,A) := \{F\in\mathrm{Diff}_k^r(A,A)\colon F(1)=0\}$.

49. Proposición: *Tenemos una correspondencia biunívoca*

$$\{\textit{Conexiones lineales simétricas}\} = \{s\in\mathrm{Hom}_A(S^2\mathrm{Der}(A,A),\mathrm{Diff}_+^2(A,A))\colon \mathrm{simb}_2\circ s=\mathrm{Id}\}$$

Demostración. Dada una conexión ∇, sea $s\colon S^2\operatorname{Der}(A,A)\to \operatorname{Diff}^2_+(A,A)$, $s(D_1\cdot D_2):=D_1\circ D_2-D_1^{\nabla}D_2$. Recíprocamente, dado s definimos $D_1^{\nabla}D_2:=D_1\circ D_2-s(D_1\cdot D_2)$, que como pertenece al núcleo de simb_2, pertenece a $\operatorname{Der}_k(A,A)$.

□

50. Teorema: *Sea d_s la diferencial simétrica asociada a una conexión lineal simétrica. Los morfismos*

$$(A\otimes A)/\Delta^{n+1}\xrightarrow{\phi_n} A\oplus\Omega\oplus\cdots\oplus S^n\Omega,\quad \overline{a\otimes b}\mapsto a\cdot(b,db,d_s^2b/2,\dots,d_s^nb/n!)$$

son isomorfismos de A-álgebras y los diagramas conmutativos

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Delta^n/\Delta^{n+1} & \longrightarrow & (A\otimes A)/\Delta^{n+1} & \longrightarrow & (A\otimes A)/\Delta^n & \longrightarrow & 0\\
 & & \| & & \wr\downarrow\phi_n & & \wr\downarrow\phi_{n-1} & & \\
0 & \longrightarrow & S^n\Omega & \longrightarrow & A\oplus\Omega\oplus\cdots\oplus S^n\Omega & \longrightarrow & A\oplus\Omega\oplus\cdots\oplus S^{n-1}\Omega & \longrightarrow & 0
\end{array}$$

de flechas verticales isomorfismos.

Demostración. Es fácil comprobar que ϕ_n es un morfismo de A-álgebras. Obviamente $\phi_n(\overline{a\otimes 1-1\otimes a})=(0,da,-,\dots,-)$, luego $\phi_n(\overline{a\otimes 1-1\otimes a}\cdots\overline{a_n\otimes 1-1\otimes a_n})=da_1\cdots da_n$ y $\phi_{n\,|\Delta^n/\Delta^{n+1}}\colon \Delta^n/\Delta^{n+1}\to S^n\Omega$ es un isomorfismo (cuyo inverso es el morfismo natural $S^n\Omega\to\Delta^n/\Delta^{n+1}$). Ahora es fácil probar, por inducción sobre n, que los ϕ_n son isomorfismos. □

51. Corolario: *El morfismo $A/\mathfrak{m}_x^{n+1}\to k\oplus\mathfrak{m}_x/\mathfrak{m}_x^2\oplus\cdots\oplus\mathfrak{m}_x^n/\mathfrak{m}_x^{n+1}$, $\bar f\mapsto\sum_{i=0}^{n}\frac{d_s^if}{i!}(x)$, es un isomorfismo de k-álgebras.*

El enunciado dual del teorema 3.9.50 es el que sigue.

52. Teorema: *Sea d_s la diferencial simétrica asociada a una conexión lineal simétrica. Entonces,*

$$S^{\cdot}\operatorname{Der}_k(A,A)\overset{\varphi}{=}\operatorname{Diff}_k(A,A),\ \varphi(D_1\cdots D_n)(a):=\frac{d_s^na}{n!}(D_1,\dots,D_n)$$

y se tiene el diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overset{n-1}{\underset{i=0}{\oplus}}S^i\operatorname{Der}_k(A,A) & \hookrightarrow & \overset{n}{\underset{i=0}{\oplus}}S^i\operatorname{Der}_k(A,A) & \longrightarrow & S^n\operatorname{Der}_k(A,A) & \longrightarrow & 0\\
 & & \|\varphi & & \|\varphi & & \|\mathrm{Id} & & \\
0 & \longrightarrow & \operatorname{Diff}_k^{n-1}(A,A) & \hookrightarrow & \operatorname{Diff}_k^{n}(A,A) & \longrightarrow & S^n\operatorname{Der}_k(A,A) & \longrightarrow & 0
\end{array}$$

Además se cumple la "fórmula de Leibnitz"

$$\varphi(D_1\cdots D_n)(a\cdot b)=\sum_{\{i_1,\ldots,i_r\}\cup\{j_1,\ldots,j_{n-r}\}=\{1,\ldots,n\}}\varphi(D_{i_1}\cdots D_{i_r})(a)\cdot\varphi(D_{j_1}\cdots D_{j_{n-r}})(b)$$

Ahora, $\mathrm{Diff}_k(A,A)$ vía φ, tiene estructura de álgebra conmutativa graduada:

$$\varphi(D_1\cdots D_n)*\varphi(D'_1\cdots D'_m):=\varphi(D_1\cdots D_n\cdot D'_1\cdots D'_m)$$

En $\mathrm{Diff}_k(A,A)$ existe una conexión canónica: $D^{\nabla}F:=D\circ F$, para todo $F\in\mathrm{Diff}_k(A,A)$ y $D\in\mathrm{Der}_k(A,A)$. Por tanto, existe una diferencial canónica

$$d\colon \mathrm{Diff}_k(A,A)\otimes\Omega^{\cdot}\to\mathrm{Diff}_k(A,A)\otimes\Omega^{\cdot}.$$

Observemos que $R=d^2=0$, porque $R(D_1,D_2)=D_1\circ D_2\circ -D_2\circ D_1\circ -[D_1,D_2]\circ=0$.

53. Teorema de Takens: *La sucesión*

$$\begin{aligned}0\to\mathrm{Diff}_k(A,A)\xrightarrow{d}\mathrm{Diff}_k(A,A)\otimes_A\Omega\xrightarrow{d}\mathrm{Diff}_k(A,A)\otimes_A\Omega^2\xrightarrow{d}\cdots\\ \xrightarrow{d}\mathrm{Diff}_k(A,A)\otimes_A\Omega^{n-1}\xrightarrow{d}\mathrm{Diff}_k(A,A)\otimes_A\Omega^n\xrightarrow{\pi}\Omega^n\to 0\end{aligned}$$

es exacta (donde $\pi(F\otimes\omega_n):=F(1)\cdot\omega_n$, para todo $F\otimes\omega_n\in\mathrm{Diff}_k(A,A)\otimes\Omega^n$).

Demostración. El diagrama

$$\begin{array}{ccc}\mathrm{Diff}^r_k(A,A)\otimes\Omega^{\cdot} & \xrightarrow{\mathrm{simb}_r\otimes\mathrm{Id}} & S^r\,\mathrm{Der}_k(A,A)\otimes\Omega^{\cdot}\\ \downarrow d & & \downarrow \mathrm{Id}^{\wedge}\\ \mathrm{Diff}^{r+1}_k(A,A)\otimes\Omega^{\cdot} & \xrightarrow{\mathrm{simb}_{r+1}\otimes\mathrm{Id}} & S^{r+1}\,\mathrm{Der}_k(A,A)\otimes\Omega^{\cdot}\end{array}$$

es conmutativo: Denotemos los morfismos simb y simb$\otimes$Id con una barrita. Dado $F\in\mathrm{Diff}^r_k(A,A)$, $\mathrm{Id}^{\wedge}(\bar F)(D)=(\mathrm{Id}\wedge\bar F)(D)=D\cdot\bar F=\overline{D\circ F}=\overline{dF(D)}=\overline{dF}(D)$, luego

$$\begin{aligned}\mathrm{Id}^{\wedge}(\overline{F\otimes\Omega_s})&=\mathrm{Id}^{\wedge}(\bar F\otimes\Omega_s)=\mathrm{Id}\wedge\bar F\wedge\Omega_s=\overline{dF}\wedge\Omega_s=\overline{dF\wedge\Omega_s}=\overline{dF\wedge\Omega_s+F\otimes d\Omega_s}\\&=\overline{d(F\otimes\Omega_s)}.\end{aligned}$$

Sea $S\in\mathrm{Diff}_k(A,A)\otimes_A\Omega^m$ tal que $dS=0$ y sea r el número natural mínimo tal que $S\in\mathrm{Diff}^r_k(A,A)\otimes_A\Omega^m$, entonces $\mathrm{Id}^{\wedge}(\bar S)=\overline{dS}=0$. Si $(r,m)\neq(0,n)$, por el teorema 3.9.11, existe $S_{r-1}\in\mathrm{Diff}^{r-1}_k(A,A)\otimes_A\Omega^{m-1}$ tal que $\mathrm{Id}^{\wedge}(\bar S_{r-1})=\bar S$. Por tanto, $S-dS_{r-1}\in\mathrm{Diff}^{r-1}_k(A,A)\otimes_A\Omega^m$, porque $\overline{S_r-dS_{r-1}}=\bar S_r-\mathrm{Id}^{\wedge}\bar S_{r-1}=0$. Operando así

sucesivamente, tendremos o que S es un borde, o bien S es módulo bordes igual a un ciclo $S_0 \in \mathrm{Diff}_k^0(A,A)\otimes_A \Omega^n$.

Obviamente, $(\mathrm{Diff}_k(A,A)\otimes_A \Omega^n) \subset \mathrm{Ker}\, d$. Luego todo elemento de $\mathrm{Diff}_k(A,A)\otimes_A \Omega^n$ módulo $d(\mathrm{Diff}_k(A,A)\otimes_A \Omega^{n-1})$ es equivalente a un elemento de $\mathrm{Diff}_k^0(A,A)\otimes_A \Omega^n$. Dado $0 \neq \lambda\otimes\Omega_n \in \mathrm{Diff}_k^0(A,A)\otimes_A \Omega^n$ supongamos que $\lambda\otimes\Omega_n \in \mathrm{Im}\, d$. Sea r mínimo para el que existe $S \in \mathrm{Diff}_k^r(A,A)\otimes_A \Omega^{n-1}$ de modo que $dS = \lambda\otimes\Omega_n \in \mathrm{Diff}_k^{r+1}(A,A)\otimes_A \Omega^n$. $\mathrm{Id}^\wedge \bar{S} = \overline{dS} = 0$, luego existe $S_{r-1} \in \mathrm{Diff}_k^{r-1}(A,A)\otimes_A \Omega^{n-2}$ tal que $\mathrm{Id}^\wedge(\bar{S}_{r-1}) = \bar{S}$. Por tanto, $S' = S - dS_{r-1} \in \mathrm{Diff}_k^{r-1}(A,A)\otimes_A \Omega^{n-1}$ y $dS' = dS$. Hemos llegado a contradicción.

Con todo hemos concluido.

□

3.10. Problemas

1. Prueba que si A es un anillo íntegro entonces (0) es irreducible. Prueba que los ideales primos son irreducibles.

2. Sea A un anillo noetheriano e $I \subseteq A$ un ideal. Si I no es irreducible, sean I_1 e I_2 dos ideales que contienen estrictamente a I tales que $I = I_1 \cap I_2$. Repitiendo este proceso con I_1 e I_2 y así sucesivamente, prueba que este proceso termina en un número finito de pasos, obteniéndose I como intersección de un número finito de ideales irreducibles.

3. Sea I un ideal de un anillo noetheriano. Probar que $I = r(I)$ si y solo si I es intersección de un número finito de ideales primos.

4. Prueba que en $k[x,y]$ se cumple que $(x)\cap(x,y)^2 = (x)\cap(y,x^2)$. ¿Son las descomposiciones primarias únicas?

5. Sea $\mathfrak{m} \subset A$ un ideal maximal y $\mathfrak{p} \underset{\neq}{\subset} \mathfrak{m}$ un ideal primo tal que $\mathfrak{p} \not\subseteq \mathfrak{m}^2$. ¿Puede ser $\mathfrak{p}\cap\mathfrak{m}^2$ un ideal primario?

6. Prueba que los ideales primos asociados al ideal cero de un anillo noetheriano A, son los ideales primos de A que coinciden con el anulador de algún elemento de A.

7. Sea $\mathcal{O}$ un anillo noetheriano local de ideal maximal $\mathfrak{m}$. Sea $I \subset \mathcal{O}$ un ideal tal que $r(I) = \mathfrak{m}$. Prueba que $\mathfrak{m}^r \subseteq I$ precisamente cuando $\overline{\mathfrak{m}^r} \subseteq \bar{I}$ en $\mathcal{O}/\mathfrak{m}^{r+1}$.

8. Calcula la descomposición primaria de $I = (xy, -y + x^2 + y^2)$ en $\mathbb{C}[x,y]$.

9. Calcula una descomposición primaria reducida de los ideales

a) $I = (x,y)\cdot(x,y-1)$ en $\mathbb{C}[x,y]$.

b) $I = (x)\cdot(x,y)\cdot(x,y-1)$ en $\mathbb{C}[x,y]$.

10. Halla la descomposición primaria del ideal generado en $\mathbb{C}[x,y]$ por las ecuaciones de:

a) Un par de rectas y una recta.

b) Una recta doble y una recta.

c) Una cónica no singular y una recta.

d) Una cónica no singular y un par de rectas.

e) Una cónica no singular y una recta doble.

11. Calcula la multiplicidad de intersección en el origen de la curva $y^2 = x^2 + y^3$ con la curva $y^3 + x^2 = 0$. Es decir, calcula $\dim_{\mathbb{C}}(\mathbb{C}[x,y]/(y^2 - x^2 - y^3, y^3 + x^2))_x$, donde x es el origen.

12. Prueba que todo anillo de Dedekind semilocal es un anillo euclídeo.

Resolución: Sea $\mathrm{Spec}_{max} A = \{x_1,\dots,x_r\}$. Definamos $\mathrm{gr}\colon A\setminus\{0\} \to \mathbb{N}$ como sigue: dado $a \in A$ no nula tenemos que $(a) = \mathfrak{p}_{x_1}^{n_1}\cdots\mathfrak{p}_{x_r}^{n_r}$. Definimos $\mathrm{gr}(a) = n_1 + \cdots + n_r$. Obviamente, $\mathrm{gr}(ab) = \mathrm{gr}(a) + \mathrm{gr}(b) \geq \mathrm{gr}(a)$. Dados $a, b \in A$ no nulos, escribamos $(a) = \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r}$ y $(b) = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}$. Si $n_i \geq m_i$ para todo i, entonces a es múltiplo de b y existe $q \in A$ tal que $a = bq$. Supongamos que $n_1 < m_1,\dots,n_s < m_s$ y $n_{s+1} \geq m_{s+1},\dots,n_r \geq m_r$. Sea $r \in A$, tal que $r = a \mod \mathfrak{p}_i^{m_i}$, para $i \leq s$ y $r = b \mod \mathfrak{p}_j^{m_j+1}$, para $j \geq s$. Entonces, $a - r = 0 \mod (b)$ y $\mathrm{gr}\, r < \mathrm{gr}\, b$. Existe $q \in A$, de modo que $a - r = bq$, es decir, $a = bq + r$ con $\mathrm{gr}\, r < \mathrm{gr}\, b$.

13. Sea A un dominio de Dedekind e $0 \neq I \subset A$ un ideal. Prueba que A/I es un anillo de ideales principales.

Resolución: $\mathrm{Spec}(A/I) = (I)_0 = \{x_1,\dots,x_r\}$ y

$$A/I = \prod_i (A/I)_{x_i} = \prod_i A_{x_i}/I\cdot A_{x_i}$$

Dado un ideal $J \subset A/I$ se tiene que $J_{x_i} = (t_{x_i})$ es principal porque es un ideal de $(A/I)_{x_i} = A_{x_i}/I_{x_i}$ que es de ideales principales. Además, $J = \prod_i J_{x_i}$, porque así es localmente. Vía esta igualdad $J = \langle (t_{x_i})_i \rangle$ porque así es localmente.

14. Prueba que en un anillo de Dedekind todos los ideales están generados por dos elementos.

    Resolución: Sea $I \subset A$ un ideal y $f \in I$ no nulo. $A/(f)$ es un anillo de ideales principales, luego $\bar{I} = (\bar{g})$. Por tanto, $I = (f, g)$.

15. Sea A un anillo noetheriano íntegro de cuerpo de fracciones K e $I \subset K$ un ideal fraccionario. Se dice que I es invertible si existe otro ideal fraccionario $J \subset K$ tal que $I \cdot J = A$. Prueba que I es invertible si y solo si I_x es un A_x-módulo monógeno para todo $x \in \operatorname{Spec} A$. Si A es de dimensión de Krull 1 y $x \in \operatorname{Spec}_{max} A$, prueba que x es no singular si y solo si $\mathfrak{p}_x$ es invertible.

    Resolución: Observemos que I es invertible si y solo si $I \cdot [A : I] = A$, lo cual es una cuestión local. Podemos suponer que A es un anillo local de ideal maximal $\mathfrak{m}_x$. Evidentemente, si I es monógeno entonces es invertible. Supongamos que I es invertible, es decir, existe un ideal fraccionario tal que $I \cdot J = A$. Si $i \cdot j \in \mathfrak{m}_x$ para todo $i \in I$ y $j \in J$, entonces $I \cdot J \subset \mathfrak{m}_x \neq A$. Luego existen $i \in I$ y $j \in J$ de modo que $u = i \cdot j \notin \mathfrak{m}_x$, es decir, u es un invertible de A. Por tanto, $I \cdot j = A$, luego $I = j^{-1} \cdot A$ que es monógeno.

    Por último, $\mathfrak{p}_x$ es invertible si y solo si $\mathfrak{p}_x$ es localmente de ideales principales, que equivale a decir que x es no singular.

16. Define "el grupo multiplicativo G_m" de los elementos no nulos de k, como variedad algebraica sobre k, así como los morfismos $G_m \times G_m \to G_m$ y $G_m \to G_m$ correspondientes al producto y paso al inverso. Análogamente define "el grupo aditivo G_a" de los elementos de k con la operación de la suma de k.

17. Sea $\mu_6 = \operatorname{Spec} k[x]/(x^6 - 1)$ el grupo de las raíces sextas de la unidad sobre un cuerpo k. Determina si es una variedad íntegra o reducida, y calcula el número de componentes irreducibles cuando $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$.

    Define los morfismos $\mu_6 \times \mu_6 \to \mu_6$, $\mu_6 \to \mu_6$ correspondientes a la noción intuitiva de producto y paso al inverso en este grupo. Define el concepto de morfismo de grupos $\mu_6 \to \mu_6$ y del núcleo del mismo. Prueba entonces que $\psi \colon \mu_6 \to \mu_6, \alpha \mapsto \alpha^2$, es morfismo de grupos y calcula el núcleo.

18. Sea X una variedad algebraica afín íntegra. Si dos morfismos de X en otra variedad algebraica afín coinciden en un abierto no vacío de X, prueba que coinciden en X.

19. Pon un ejemplo de variedad algebraica que sea la unión de dos componentes no disjuntas, una de dimensión 2, la otra de dimensión 1.

20. Sean X, Y variedades algebraicas íntegras sobre un cuerpo k y sean Σ_X, Σ_Y sus respectivos cuerpos de funciones racionales. Si $\phi\colon Y \to X$ es un morfismo que transforma el punto genérico de Y en el punto genérico de X (lo que equivale a que tenga imagen densa), induce un morfismo de k-álgebras $\Sigma_X \to \Sigma_Y$. Diremos que ϕ es un morfismo de *grado* n cuando Σ_Y sea una extensión finita de grado n de Σ_X. Los morfismos de grado 1 se llaman morfismos birracionales. Diremos que X e Y son birracionalmente equivalentes si sus cuerpos de funciones racionales son extensiones de k isomorfas: $\Sigma_X \simeq \Sigma_Y$. Las variedades algebraicas birracionalmente equivalentes al espacio afín se llaman racionales. Es decir, una variedad algebraica sobre k es racional si su cuerpo de funciones racionales es isomorfo a un cuerpo de fracciones racionales $k(x_1,\dots,x_n)$ con coeficientes en k.

    a) Sea C la cúbica plana $y^2 = x^2 + x^3$. Prueba que el haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcula el área del "ojo del lazo" definido por la curva $y^2 = x^2 + x^3$.

    b) Sea C la cúbica plana $y^2 = x^3$. Prueba que el haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2$, $y = t^3$.

21. Recordemos el teorema del elemento primitivo: "Si $k \hookrightarrow K$ es una extensión finita de cuerpos de característica cero, entonces existe un $\xi \in K$ de modo que $K = k(\xi)$". Demuestra que toda variedad algebraica íntegra, sobre $\mathbb{C}$, es birracionalmente isomorfa a una hipersuperficie de un espacio afín.

22. Sea $k \hookrightarrow K$ una extensión finita de cuerpos y $X = \operatorname{Spec} A$ una k-variedad algebraica. Prueba que el morfismo natural $X_K = \operatorname{Spec} A \otimes_k K \to X = \operatorname{Spec} A$ de cambio de base es epiyectivo y cerrado.

23. Sea A un anillo íntegro y $a \in A$ no invertible, ni nula. Prueba que el morfismo de localización $A \to A_a$ no es finito.

24. Sea A un anillo íntegro de cuerpo de fracciones K, y sea $k = A/\mathfrak{m}$, donde $\mathfrak{m}$ es un maximal de A. Si $f(x) \in A[x] \subset K[x]$ es un polinomio mónico y separable, y su reducción $\overline{f(x)}$ módulo $\mathfrak{m}$ es separable, entonces el grupo de Galois de $\overline{f(x)}$ es un subgrupo del grupo de Galois de $f(x)$.

25. Sean $p(x,y)$ y $q(x,y)$ dos polinomios de $k[x,y]$ sin factores comunes. Demuestra que la k-álgebra $k[x,y]/(p(x,y),q(x,y))$ es una k-álgebra finita.

26. Sea $\mathfrak{m} \subset k[x_1,\dots,x_n]$ un ideal maximal. Prueba que $\mathfrak{m}$ está generado por n funciones. ¿Puede estar generado por $n-1$ funciones?

27. Sea $\pi\colon X = \operatorname{Spec} A \to \mathbb{A}^1 = \operatorname{Spec} k[x]$ un morfismo finito y supongamos que X es una variedad algebraica íntegra (de dimensión 1). Prueba que el número de puntos (contando multiplicidades) de las fibras de π es constante.

28. Calcula los ideales maximales de $\mathbb{C}[x_1,\dots,x_n]$. Calcula los ideales maximales de $\mathbb{C}[x_1,x_2,x_3]/(x_1^2+x_2^2+x_3^2-1)$.

29. Sea p un número primo, $A = \mathbb{Z}_{\mathbb{Z}\setminus(p)}$ y $\mathbb{P}^1_A = \operatorname{Proj} A[x_0,x_1]$. Sea $\mathfrak{p}_y = (px_0 - x_1) \subset A[x_0,x_1]$. Prueba que y no es un punto cerrado de $\mathbb{P}^1_A$, pero que si es un punto cerrado en $\mathbb{P}^1_A \setminus (x_1)_0$.

30. Sea $X = \operatorname{Spec} A$ una variedad íntegra sobre un cuerpo k algebraicamente cerrado. Prueba que para toda extensión $k \to K$, la variedad $X_K = \operatorname{Spec}(A \otimes_k K)$ es íntegra. (Póngase K como límite inductivo de álgebras finito generadas).

31. Sea k un cuerpo algebraicamente cerrado y K,K' dos k-extensiones de cuerpos. Prueba que $K \otimes_k K'$ es íntegro.

32. Prueba que el morfismo $k[x] \hookrightarrow k[x,y]/(p(x,y))$ es finito si y solo si la curva $p(x,y) = 0$ no tiene asíntotas verticales.

33. Calcula las asíntotas imaginarias de la circunferencia $x^2 + y^2 = 1$.

34. Prueba que el conjunto de rectas que pasan por un punto ("haz de rectas") del plano afín se corresponde con el conjunto de puntos racionales de una recta proyectiva.

35. Prueba que el conjunto de cónicas que pasan por cuatro puntos no alineados del plano afín se corresponden con los puntos racionales de una recta proyectiva.

36. Prueba que el conjunto de cónicas que pasan tres puntos no alineados del plano afín y es tangente en uno de ellos a una recta fijada que pasa por el punto se corresponden con los puntos racionales de una recta proyectiva.

37. Prueba que el conjunto de curvas de grado n de $\mathbb{P}^2$ se corresponden con los puntos racionales de un espacio proyectivo.

38. Prueba que el conjunto de curvas afines de grado menor o igual que n de $\mathbb{A}^2$ se corresponden con los puntos racionales de un abierto de un espacio proyectivo.

39. Se dice que los puntos de una variedad algebraica irreducible cumplen una propiedad en general si existe un abierto de la variedad cuyos puntos cumplen la propiedad. Prueba que en general las curvas planas afines de grado n son irreducibles.

40. Demuestra que en general las matrices cuadradas son invertibles. Sean A y B dos matrices cuadradas de orden n, prueba que el polinomio característico de $A \cdot B$ es igual al de $B \cdot A$.

41. Define un isomorfismo natural $R_0[\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}] \simeq R_0[\xi_0, \ldots, \xi_n]/(\xi_i - 1)$ y prueba que $U^h_{\xi_i} \simeq (\xi_i - 1)_0$. Prueba que $U^h_{\xi_i} \times (\mathbb{A}^1 \setminus \{0\}) = U_{\xi_i}$. Dar una interpretación geométrica de estos resultados.

42. Demuestra que el conjunto de puntos cerrados de $\mathbb{P}^n(\mathbb{C}) = \operatorname{Proj} \mathbb{C}[x_0, \ldots, x_{n+1}]$ es biyectivo con el conjunto $\mathbb{C}^{n+1} \setminus \{0\}/\sim$, donde $\alpha \sim \alpha'$ si existe $\lambda \in \mathbb{C}*$ tal que $\alpha' = \lambda \cdot \alpha$.

43. *a*) Escribe las ecuaciones de la curva proyectiva plana $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2)$ en cada uno de los abiertos "afines", complementario del cerrado $(x_i)^h_0$ ("deshomogeneizar").

    b) Demuestra que el epimorfismo $\mathbb{C}[x_0, x_1, x_2] \to \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2)$ define una inmersión cerrada $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2) \hookrightarrow \mathbb{P}^2$

    c) Define una curva proyectiva plana que en uno de los abiertos afines sea la curva plana "afín" $y + x^2 = 0$. ¿Corta la recta $x = 0$, a la curva $y + x^2 = 0$, en algún punto del "infinito"?

44. Si X e Y son dos subvariedades proyectivas irreducibles de $\mathbb{P}^n$, que cumplen que $\operatorname{codim} X + \operatorname{codim} Y \leq n$, prueba que $X \cap Y \neq \emptyset$ y que

$$\operatorname{codim} X + \operatorname{codim} Y \geq \operatorname{codim} X \cap Y.$$

45. Sea $f \in k[\xi_0, \ldots, \xi_n]$ una función homogénea que se anula en algún punto de $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$. Demuestra que

$$\dim(f)^h_0 \geq \dim X - 1.$$

46. Sea $x^n + a_1 x^{n-1} + \cdots + a_n$ la ecuación general de grado n sobre k, y sea $k(\alpha_1, \ldots, \alpha_n)$ su cuerpo de descomposición. Se dice que $c \in K$ pertenece al subgrupo $G \subset S_n$, cuando $K^G = k(c)$.

    Sea $p(x)$ un polinomio irreducible y separable sobre k, de raíces $\alpha_1, \ldots, \alpha_n$. Sea $\phi(x_1, \ldots, x_n)$ una función racional que pertenece a $G \subset S_n$ y $\phi_1, \ldots, \phi_s$ sus diferentes transformados por S_n. Supongamos que $\phi_i(\alpha) \neq \phi_j(\alpha)$, $i \neq j$. Prueba: el grupo de Galois de $p(x)$ es un subgrupo de $G \Leftrightarrow \prod_i (x - \phi_i(\alpha)) \in k[x]$ tiene una raíz en k.

47. Sea p un número primo y $m > 0$ un número natural no divisible por p. Sea $K = \mathbb{F}_p[w]$, donde w es una raíz m-ésima primitiva de la unidad. Demuestra que $\dim_{\mathbb{F}_p} K$ es igual al orden de p en $(\mathbb{Z}/m\mathbb{Z})^*$.

    Resolución: El automorfismo de Fröbrenius en p de $\mathbb{Q}[e^{2\pi i/m}]$ es $F_p = \bar{p} \in (\mathbb{Z}/m\mathbb{Z})^*$. El grupo de Galois de K es isomorfo a $\langle \bar{p} \rangle$. El orden de $\langle \bar{p} \rangle$, que es igual al orden de p en $(\mathbb{Z}/m\mathbb{Z})^*$, es igual a $\dim_{\mathbb{F}_p} K$.

48. Prueba que el grupo de Galois de $x^3 + 2x^2 + 4x + 1$ es igual a S_3, argumentando con los morfismos de Fröbenius en 2 y 3.

    Resolución: Módulo 2, $x^3+2x^2+4x+1 = x^3+1 = (x+1)(x^2+x+1)$. Por tanto, F deja fija una raíz y permuta dos. Luego, F_2 es un dos ciclo. Módulo 3, $x^3+2x^2+4x+1 = x^3 - x^2 + x + 1$ y es irreducible, luego $\langle F \rangle$ opera transitivamente y F ha de ser un tres ciclo. Luego, F_3 es un tres ciclo. Como $\langle F_2, F_3 \rangle = S_3$ concluimos que el grupo de Galois es S_3.

Capítulo 4

Álgebra local

4.1. Introducción

Vamos a iniciar el estudio local, en un entorno de un punto, de las variedades algebraicas. Es decir, el estudio del anillo de los gérmenes de las funciones algebraicas de una variedad en un punto.

Comenzaremos con la teoría de la dimensión para anillos locales noetherianos, que incluye tanto a los anillos locales de las funciones de variedades algebraicas, como sus compleciones (por ejemplo los anillos de series formales). El concepto de dimensión es esencialmente local. Parte de la teoría desarrollada en el capítulo 3, para variedades algebraicas (por ejemplo, el teorema del ideal principal de Krull) es un caso particular de lo expuesto en este capítulo.

Caracterizaremos los anillos de gérmenes de las variedades algebraicas regulares en un punto. Veremos que una variedad es regular en un punto si y solo si el espacio tangente en el punto es un espacio afín. Probaremos que las k-variedades algebraicas lisas son regulares y que sobre cuerpos algebraicamente cerrados se cumple el recíproco.

Estudiaremos la compleción de un anillo en un punto. Esta técnica consiste en tomar los desarrollos de Taylor de las funciones en el punto. Así, el proceso de compleción puede entenderse como una aproximación algebraico-analítica al estudio de las variedades. El completado del anillo de funciones algebraicas de una variedad en un punto reflejará las propiedades locales de la variedad en el punto. Si bien el proceso de compleción es más drástico que el de localización. Por ejemplo, los anillos locales de una recta afín y los de una cúbica plana sin puntos singulares no son isomorfos pues no lo son sus cuerpos de funciones, sin embargo los completados de sus anillos locales si son isomorfos (sobre un cuerpo algebraicamente cerrado).

Demostraremos las propiedades de exactitud de la compleción, que la compleción

de un anillo noetheriano es noetheriano, que el morfismo de compleción $A \to \widehat{A}$ es plano y el teorema de Cohen. El teorema de Cohen es un teorema de estructura de los anillos completos. Afirma que la compleción de una k-álgebra local noetheriana es un cociente de un anillo de series formales. Como consecuencia obtendremos que una k-álgebra noetheriana completa es regular si y solo es un anillo de series formales. Debido a la platitud del morfismo de compleción, muchos problemas en A se pueden simplificar estudiándolos en $\widehat{A}$.

4.2. Teoría de la dimensión local

En esta sección vamos a desarrollar la teoría de la dimensión para anillos locales noetherianos. En variedades algebraicas vimos que el supremo de las longitudes de las cadenas de ideales primos coincidía con el número mínimo de parámetros necesarios para determinar localmente un punto cerrado. Para la demostración de ello fue fundamental el teorema del ideal principal de Krull.

Abordaremos la teoría de la dimensión en anillos locales noetherianos $\mathscr{O}$ considerando el espacio tangente a $\mathrm{Spec}\mathscr{O}$ en su punto cerrado. Éste será una variedad algebraica (de la misma dimensión que el anillo). A partir de él definiremos el polinomio de Samuel, que nos permitirá demostrar el teorema del ideal principal de Krull. Además, los coeficientes del polinomio de Samuel son invariantes asociados canónicamente al anillo local, importantes para su clasificación. Por ejemplo, caracterizan si el anillo local es regular o no y permiten definir la multiplicidad del anillo en el punto.

4.2.1. Cono tangente y espacio tangente en un punto

El espacio tangente a una variedad diferenciable en un punto es un concepto intrínseco, que no depende de la inmersión de la variedad diferenciable en un $\mathbb{R}^n$. El espacio tangente a una variedad en un punto se define en términos de su anillo de funciones diferenciables. Ya sabemos que la diferencial de una función en un punto y los módulos de diferenciales de Kähler son conceptos algebraicos. En esta sección, dado un anillo local, definiremos el espacio tangente en el punto cerrado.

Comencemos con un ejemplo sencillo. Consideremos el nodo en el plano afín

$$y^2 - x^2 + x^3 = 0.$$

El espacio tangente en el origen del nodo es aquella variedad homogénea que mejor se aproxima al nodo. "El nodo infinitesimalmente en el origen es igual al par de rectas $y^2 - x^2 = 0$." Diremos que el cono tangente a $y^2 - x^2 + x^3 = 0$ en el origen es $y^2 - x^2 = 0$. En general, si una subvariedad $X \subset \mathbb{A}_n$ que pasa por el origen, viene definida por los ceros

de un ideal $I \subset k[x_1,\dots,x_n]$, entonces el cono tangente C_0X en el origen es la variedad definida por el ideal $I_h = (f_r)_{f\in I}$, donde f_r es la parte homogénea de grado más pequeño de f. Es decir, si pensamos que X es la intersección de las variedades $f = 0$, con $f \in I$, entonces el cono tangente es la intersección de las variedades homogéneas $f_r = 0$.[1]

Veamos cómo construir I_h. Sea $\mathfrak{m}_0 = (x_1,\dots,x_n) \subset k[x_1,\dots,x_n]$ y $\bar{\mathfrak{m}}_0 \subset k[x_1,\dots,x_n]/I$ el ideal maximal de las funciones de X que se anulan en el origen. Se tiene la sucesión exacta $I \cap \mathfrak{m}_0^r \to \mathfrak{m}_0^r \to \bar{\mathfrak{m}}_0^r \to 0$ y por tanto la sucesión exacta

$$I \cap \mathfrak{m}_0^r \to \mathfrak{m}_0^r/\mathfrak{m}_0^{r+1} \to \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} \to 0$$

En conclusión,

$$\bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} = \{\text{Polinomios } p(x_1,\dots,x_n) \text{ homogéneos de grado } r\}/\{f_r\}_{f=f_r+\dots+f_n\in I}$$

Por tanto, $\oplus_r \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} = k[x_1,\dots,x_n]/I_h$. Entonces, $\operatorname{Spec}(\overset{\infty}{\underset{r=0}{\oplus}} \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1})$ es el cono tangente de X en el origen y $\operatorname{Proj}(\overset{\infty}{\underset{r=0}{\oplus}} \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1})$ es el espacio tangente de X en el origen.

Demos ahora las definiciones con toda precisión y mayor generalidad.

1. Definición: Una filtración de un A-módulo M es una cadena de submódulos

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \dots$$

2. Definición: Llamaremos graduado de M por la filtración $\{M_n\}$ al módulo $GM = \overset{\infty}{\underset{i=0}{\oplus}} M_i/M_{i+1}$. Si I es un ideal de A, denotaremos G_IM al graduado de M por la filtración $\{M_n := I^nM\}$.

Si $I \subset A$ es un ideal, entonces $G_IA = \overset{\infty}{\underset{i=0}{\oplus}} I^n/I^{n+1}$ es de modo natural un álgebra graduada, donde el subgrupo de elementos homogéneos de grado n es I^n/I^{n+1}.

3. Definición: Sea $X = \operatorname{Spec} A$ y $x \in X$ un punto cerrado de ideal $\mathfrak{m}$. Llamaremos cono tangente de X en x a

$$C_xX = \operatorname{Spec} G_{\mathfrak{m}}A := \operatorname{Spec} \overset{\infty}{\underset{i=0}{\oplus}} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

Llamaremos vértice del cono al punto de C_xX definido por el ideal (maximal) irrelevante $\underset{r>0}{\oplus} \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Llamaremos espacio tangente de X en x a

$$T_xX := \operatorname{Proj} G_{\mathfrak{m}}A$$

[1] Advertamos que debemos tomar todas las $f \in I$ y que no basta con tomar cualquier sistema generador de I.

En general, dado un cerrado $Y = (I)_0 \subset X = \mathrm{Spec} A$, llamaremos cono normal de X a lo largo de Y, que denotamos $C_{X/Y}$, a $C_{X/Y} := \mathrm{Spec} G_I A$; y espacio normal a Y en X, que denotamos $N_{X/Y}$, a $N_{X/Y} := \mathrm{Proj} G_I A$.

4. Ejemplo: El cono tangente de un espacio afín en el origen es isomorfo al espacio afín. Es decir, si $A = k[x_1, \ldots, x_n]$ y $\mathfrak{m} = (x_1, \ldots, x_n)$, entonces $G_{\mathfrak{m}} A \simeq A$.

5. Proposición: *Sea $I \subset A$ un ideal y $f \in I^r \backslash I^{r+1}$. Denotemos f_r la clase de f en $I^r/I^{r+1} \subset G_I A$. Si f_r es no divisor de cero en $G_I A$, entonces*

1. *$(f) \cap I^n = f \cdot I^{n-r}$, para $n \geq r$.*

2. *$G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$, donde $\bar{I}$ es el ideal I en $A/(f)$.*

Demostración. 1. Es claro que $f \cdot I^{n-r} \subseteq (f) \cap I^n$. Probemos la inclusión inversa. Si $h \in (f) \cap I^n$, entonces $h = f \cdot g$, con $g \in A$. Sea $s \geq 0$ el máximo tal que $g \in I^s$. Tenemos que ver que $s \geq n - r$. Escribamos $0 \neq g_s = \bar{g} \in I^s/I^{s+1}$. Por hipótesis, $0 \neq f_r \cdot g_s \in I^{r+s}/I^{r+s+1}$, luego $h = f \cdot g \notin I^{r+s+1}$. Por tanto, $n < r + s + 1$, es decir, $s \geq n - r$.

2. El núcleo del epimorfismo $I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1}$ es igual a $(I^n \cap (I^{n+1} + (f))/I^{n+1} = (I^{n+1} + I^n \cap (f))/I^{n+1}$. Por 1., la sucesión

$$0 \to I^{n-r}/I^{n-r+1} \xrightarrow{f_r \cdot} I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1} \to 0$$

es exacta, luego $G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$.

□

6. Ejercicio: Escribamos el polinomio $p(x,y) = p_n(x,y) + p_{n+1}(x,y) + \ldots + p_m(x,y)$ como suma de polinomios homogéneos. Sea $\mathcal{O} = (k[x,y]/p(x,y))_{x_0}$, con $\mathfrak{m}_{x_0} = (x,y)$. Demuestra que $G_{\mathfrak{m}_{x_0}} \mathcal{O} = k[x,y]/(p_n(x,y))$.

7. Ejercicio: Prueba que el espacio tangente de la intersección de dos hipersuperficies transversales es la intersección de los espacios tangentes. Es decir, considérese el espacio afín $\mathbb{A}_3 = \mathrm{Spec} k[x_1, x_2, x_3]$ y las superficies $f_1(x_1, x_2, x_3) = 0$, $f_2(x_1, x_2, x_3) = 0$. Sea $\mathfrak{m} = (x_1, x_2, x_3)$, y $f_{1,n}$, $f_{2,m}$ las componentes homogéneas de grado mínimo de f_1, f_2. Supongamos que no existen polinomios irreducibles que dividan a $f_{1,n}$ y $f_{2,m}$ (es decir, $f_{2,m}$ no es divisor de cero en $G_{\mathfrak{m}}(k[x_1, x_2, x_3]/(f_1)) = k[x_1, x_2, x_3]/(f_{1,n})$). Prueba que

$$G_{\mathfrak{m}}(k[x_1, x_2, x_3]/(f_1, f_2)) \simeq k[x_1, x_2, x_3]/(f_{1,n}, f_{2,m}).$$

4.2.2. Función de Hilbert

8. Definición: Sea $R = \oplus_{n\in\mathbb{Z}} R_n$ un anillo graduado. Diremos que un R-módulo M es un módulo graduado si es suma directa de R_0-módulos $\{M_n\}_{n\in\mathbb{Z}}$, de modo que $f_r \cdot m_s \in M_{r+s}$ para todo $r,s \in \mathbb{Z}$, $f_r \in R_r$ y $m_s \in M_s$.

Sea $A = R_0[\xi_1,\ldots,\xi_r]$ un anillo graduado, con R_0 un anillo de longitud finita (de grado cero) y ξ_i de grado 1, para todo i. R_0 es noetheriano y por tanto A también.

Sea $M = \oplus_{n\in\mathbb{N}} M_n$ un A-módulo finito generado graduado. Obsérvese que M_n son R_0-módulos finito generados, porque el A-submódulo de M generado por M_n es finito generado, ya que M es noetheriano. Por tanto, M_n es un R_0-módulo de longitud finita.

9. Definición: Llamaremos función de Hilbert de M a $H_M(n) := l(M_n)$.

10. Definición: Llamaremos función de Samuel de M a $S_M(n) := \sum_{i=0}^{n-1} l(M_i)$.

Dada una función $f : \mathbb{N} \to \mathbb{Q}$ denotemos por $\Delta f(n)$ la función $\Delta f(n) := f(n+1) - f(n)$. Observemos que $\Delta S_M(n) = S_M(n+1) - S_M(n) = H_M(n)$.

Las funciones $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}$ forman una base de los polinomios en n de grado menor o igual que r y $\Delta\binom{n}{i} = \binom{n}{i-1}$. Si una función $f : \mathbb{N} \to \mathbb{Q}$ cumple que $\Delta f(n) = \binom{n}{i}$ entonces $f(n) = \binom{n}{i+1} +$ cte.

11. Proposición: *Sea $A = R_0[x_1,\ldots,x_r]$, con R_0 de longitud finita. Se cumple que*

$$S_A(n) = l(R_0)\cdot\binom{n+r-1}{r} \quad y \quad H_A(n) = l(R_0)\cdot\binom{n+r-1}{r-1}$$

Demostración. Sea $\bar{A} = A/(x_r) = R_0[x_1,\ldots,x_{r-1}]$. De la sucesión exacta

$$0 \to A_n \xrightarrow{\cdot x_r} A_{n+1} \to \bar{A}_{n+1} \to 0$$

y por inducción sobre r, se obtiene que $\Delta H_A(n) = H_{\bar{A}}(n+1) = l(R_0)\cdot\binom{n+r-1}{r-2}$, luego $S_A(n) = l(R_0)\cdot\binom{n+r-1}{r} +$ cte. Tomando $n = 1$ se obtiene que cte $= 0$ y se concluye. □

12. Definición: Decimos que una función $f : \mathbb{N} \to \mathbb{Q}$ es un polinomio para $n > n_0$ si existe un polinomio $q(x) \in \mathbb{Q}[x]$ de modo que $f(n) = q(n)$, para todo $n > n_0$.

13. Lema: *Sea $f : \mathbb{N} \to \mathbb{Q}$ una aplicación. La función $\Delta f(n)$ es un polinomio para $n > n_0 \iff f(n)$ es un polinomio para $n > n_0$.*

Demostración. Es inmediato. □

14. Teorema: *Para n suficientemente grande, la función de Hilbert $H_M(n)$ es un polinomio en n (polinomio que llamaremos polinomio de Hilbert).*

Demostración. Vamos a proceder por inducción sobre el número de generadores de $A = R_0[\xi_1, \ldots, \xi_r]$.

Si $r = 0$, como M es finito generado $M_n = 0$ para $n > n_0$, con $n_0 >> 0$. Por tanto, $H_M(n) = 0$ para $n > n_0$ y concluimos.

Supongamos cierto el teorema para $A = R_0[\xi_1, \ldots, \xi_{r-1}]$ y consideremos las sucesiones exactas

$$0 \to \mathrm{Ker}_n \to M_n \xrightarrow{\xi_r \cdot} M_{n+1} \to \mathrm{Coker}_{n+1} \to 0$$

$$0 \to \mathrm{Ker} := \bigoplus_n \mathrm{Ker}_n \to M \xrightarrow{\xi_r \cdot} M \to \mathrm{Coker} := \bigoplus_n \mathrm{Coker}_n \to 0$$

Como ξ_r anula a Ker y Coker, ambos son $R_0[\xi_1, \ldots, \xi_{r-1}]$-módulos finito generados graduados. Por hipótesis de inducción

$$\Delta H_M(n) = H_M(n+1) - H_M(n) = H_{\mathrm{Coker}}(n+1) - H_{\mathrm{Ker}}(n)$$

es un polinomio para $n > n_0$, luego $H_M(n)$ es un polinomio para $n > n_0$, por el lema anterior.

□

La función de Samuel es un polinomio para $n >> 0$, ya que $\Delta S_M(n) = H_M(n)$. Dicho polinomio lo denominaremos polinomio de Samuel.

4.2.3. Teorema de Artin-Rees

Necesitamos el teorema de Artin-Rees para demostrar, mediante el polinomio de Samuel, el teorema del ideal principal de Krull en anillos locales noetherianos. El teorema de Artin-Rees será fundamental para demostrar, más adelante, que la compleción I-ádica es exacta (para módulos finito generados) y que el morfismo de compleción es plano.

15. Definición: Sea I un ideal de un anillo A y $\{M_n\}$ una filtración de un A-módulo M. Diremos que $\{M_n\}$ es una I-filtración si se verifica $IM_n \subseteq M_{n+1}$ para todo $n \in \mathbb{N}$. Diremos que la I-filtración es I-estable si existe un $h \in \mathbb{N}$ tal que $IM_n = M_{n+1}$ para todo $n > h$.

16. Proposición: *Sean $\{M_n\}$, $\{M'_n\}$ dos filtraciones I-estables de M. Existe un entero h tal que $M_{n+h} \subseteq M'_n$ y $M'_{n+h} \subseteq M_n$ para todo n.*

Demostración. Sea $h \in \mathbb{N}$ tal que $IM_n = M_{n+1}$ e $IM'_n = M'_{n+1}$ para todo $n \geq h$. Entonces, $M_{n+h} = I^n M_h \subseteq I^n M \subseteq M'_n$ y $M'_{n+h} = I^n M'_h \subseteq I^n M \subseteq M_n$. □

17. Definición: Sea I un ideal de A. Llamaremos dilatado de A por I a

$$D_I A = A \oplus I \oplus I^2 \oplus \cdots \oplus I^n \oplus \cdots$$

En general, dado un A-módulo M y una I-filtración $\{M_n\}$, llamaremos dilatado de M por la I-filtración a $DM = M \oplus M_1 \oplus M_2 \oplus \cdots \oplus M_n \oplus \cdots$.

Observemos que $D_I A$ es un anillo graduado y que DM es un $D_I A$-módulo graduado. Si A es noetheriano, entonces $I = (\xi_1, \ldots, \xi_r)$ es finito generado. El morfismo

$$\begin{array}{ccc} A[x_1, \ldots, x_r] & \to & D_I A = A \oplus I \oplus \cdots \oplus I^n \oplus \ldots \\ x_i & \mapsto & \xi_i \end{array}$$

es epiyectivo, luego $D_I A$ es noetheriano.

18. Lema: *Sea A noetheriano, M un A-módulo finito generado y $\{M_n\}$ una I-filtración. La filtración es I-estable $\iff$ DM es un $D_I A$-módulo finito generado.*

Demostración. El $D_I A$-submódulo de DM generado por $M \oplus M_1 \oplus \cdots \oplus M_h$ es igual

$$M \oplus M_1 \oplus \cdots \oplus M_h \oplus IM_h \oplus I^2 M_h \oplus \cdots$$

Si $\{M_n\}$ es I-estable, existe $h \in \mathbb{N}$ tal que $IM_n = M_{n+1}$ para todo $n \geq h$. Por tanto $M \oplus M_1 \oplus \cdots \oplus M_h$ genera DM como $D_I A$-módulo, luego es un $D_I A$-módulo finito generado. Recíprocamente, supongamos que $DM =< n_1, \ldots, n_s >$ es finito generado. Podemos suponer que los n_i son homogéneos. Sea h el máximo de los grados de los n_i. Entonces,

$$DM =< n_1, \ldots, n_s >= D_I A \cdot (M \oplus M_1 \oplus \cdots \oplus M_h)$$

luego $M_{n+h} = I^n M_h$ para todo n y la filtración es I-estable.

□

19. Teorema de Artin-Rees: *Sea A noetheriano, M un A-módulo finito generado y $M' \subset M$ un submódulo. Se verifica que la filtración $\{M' \cap I^n M\}$ es I-estable.*

Demostración. Consideremos en M la filtración I-ádica y consideremos en M' la I-filtración $\{M' \cap I^n M\}$. DM' es un $D_I A$-submódulo de DM. $D_I A$ es noetheriano y, por el lema anterior, DM es finito generado. Por tanto, DM' es finito generado, luego por el lema anterior $\{M' \cap I^n M\}$ es I-estable.

□

20. Corolario de Krull: *Sea A un anillo noetheriano, $I \subset A$ un ideal incluido en el radical de Jacobson de A y M un A-módulo finito generado. Entonces, $\bigcap_{n \in \mathbb{N}} I^n M = 0$.*

Demostración. Sea $N = \bigcap_{n \in \mathbb{N}} I^n M$. Por Artin-Rees, la filtración $\{N \cap I^n M = N\}$ es I-estable. Por tanto, $IN = N$ y por el lema de Nakayama $N = 0$. □

4.2.4. Dimensión en anillos locales noetherianos

De ahora en adelante, supondremos que $\mathscr{O}$ es un anillo local noetheriano de ideal maximal $\mathfrak{m}$, I un ideal $\mathfrak{m}$-primario (es decir, $\operatorname{Spec}\mathscr{O}/I = (I)_0 = \{\mathfrak{m}\}$) y M un $\mathscr{O}$-módulo finito generado.

$\mathscr{O}/I$ es de longitud finita, por 0.6.61. Escribamos $I = (\xi_1, \dots, \xi_r)$. El graduado de $\mathscr{O}$ por I es $G_I\mathscr{O} = \mathscr{O}/I[\bar{\xi}_1, \dots, \bar{\xi}_r]$, que es un anillo graduado con $\mathscr{O}/I$ de longitud finita y $\bar{\xi}_i$ de grado 1.

Consideremos en M una filtración I-estable, $\{M_n\}$. Sabemos que el dilatado DM es un $D_I\mathscr{O}$-módulo finito generado. Por tanto, el graduado de M por la filtración, GM, es un $D_I\mathscr{O}$-módulo finito generado, luego es un $G_I\mathscr{O}$-módulo finito generado.

Denotaremos $S_M(n)$ a la función de Samuel de GM, es decir

$$S_M(n) = l(M/M_1) + l(M_1/M_2) + \cdots + l(M_{n-1}/M_n) = l(M/M_n).$$

21. Teorema: *El grado y el primer coeficiente de $S_M(n)$ no dependen de la filtración I-estable considerada en M.*

Demostración. Sean $\{M_n\}$ y $\{\bar{M}_n\}$ dos filtraciones I-estables de M. Denotemos por $S_M(n) = l(M/M_n)$ y $S_{\bar{M}}(n) = l(M/\bar{M}_n)$. Por 4.2.16, existe un h tal que $M_{n+h} \subseteq \bar{M}_n$ y $\bar{M}_{n+h} \subseteq M_n$, para todo $n \in \mathbb{N}$, luego $S_M(n+h) \geq S_{\bar{M}}(n)$ y $S_{\bar{M}}(n+h) \geq S_M(n)$, con lo que se concluye. □

22. Proposición: *El grado de $S_M(n)$ no depende del ideal $\mathfrak{m}$-primario I.*

Demostración. Consideremos las filtraciones $\{I^n M\}$ y $\{\mathfrak{m}^n M\}$. Por el teorema anterior, basta probar que $S_{M,I}(n) = l(M/I^n M)$ y $S_{M,\mathfrak{m}}(n) = l(M/\mathfrak{m}^n M)$ tienen el mismo grado. Existe un k, tal que $\mathfrak{m}^k \subseteq I$. Por tanto,

$$S_{M,\mathfrak{m}}(kn) = l(M/\mathfrak{m}^{kn}M) \geq l(M/I^n M) = S_{M,I}(n)$$
$$S_{M,I}(n) = l(M/I^n M) \geq l(M/\mathfrak{m}^n M) = S_{M,\mathfrak{m}}(n)$$

de donde se deduce que $S_{M,I}(n)$ y $S_{M,\mathfrak{m}}(n)$ son dos polinomios del mismo grado.

□

La siguiente proposición hará las veces del teorema del ideal principal de Krull.

23. Teorema: *Si $a \in \mathscr{O}$ no es divisor de cero en M, entonces* $\operatorname{gr} S_{M/aM}(n) < \operatorname{gr} S_M(n)$.

Demostración. Consideremos la sucesión exacta

$$0 \to aM \to M \xrightarrow{\pi} M/aM \to 0$$

La filtraciones $\{aM \cap M_n\}$, $\{\pi(M_n)\}$ inducidas en aM y M/aM por la filtración I-estable $\{M_n\}$ de M, son I-estables por el teorema de Artin-Rees. De la sucesión exacta

$$0 \to aM/aM \cap M_n \to M/M_n \to (M/aM)/\pi(M_n) \to 0$$

se deduce que $S_{M/aM}(n) = S_M(n) - S_{aM}(n)$. Ahora bien, $M \overset{a\cdot}{\simeq} aM$ es un isomorfismo porque a no es divisor de cero, luego el grado y el primer coeficiente de $S_M(n)$ es igual al de $S_{aM}(n)$, por 4.2.21. Por tanto, $\operatorname{gr} S_{M/aM}(n) < \operatorname{gr} S_M(n)$.

□

24. Definición: Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Diremos que $f_1, \ldots, f_n \in \mathcal{O}$ es un sistema de parámetros en $\mathcal{O}$ si $(f_1, \ldots, f_n)_0 = \{\mathfrak{m}\}$.

25. Definición: Diremos que $S_{\mathcal{O}}(n) := l(\mathcal{O}/\mathfrak{m}^n)$ es la función de Samuel de $\mathcal{O}$, diremos que su polinomio asociado es el polinomio de Samuel de $\mathcal{O}$.

Seguiremos la siguiente convención: si $(0)_0 = \{\mathfrak{m}\}$ entonces diremos 0 parámetros es un sistema de parámetros de $\mathcal{O}$. Denotaremos $S_{\mathcal{O},I}(n) = l(\mathcal{O}/I^n)$.

26. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Los siguientes números son iguales*

1. *Dimensión de Krull de $\mathcal{O}$.*
2. *Número mínimo de parámetros de los sistemas de parámetros de $\mathcal{O}$.*
3. *Grado del polinomio de Samuel de $\mathcal{O}$.*

Demostración.

a) Dimensión de Krull de $\mathcal{O} \geq$ Número mínimo de parámetros de los sistemas de parámetros de $\mathcal{O}$:

Si $\dim \mathcal{O} \neq 0$, sea $f_1 \in \mathfrak{m}$ que no se anule en ningún ideal primo minimal (existe: si $\{\mathfrak{p}_j\}$ son los ideales primos minimales de $\mathcal{O}$ y $g_i \in \mathfrak{m}$ se anula en todos los $\mathfrak{p}_j$ salvo en $\mathfrak{p}_i$, entonces $f_1 = \sum_i g_i$). Por tanto, $\dim \mathcal{O} > \dim \mathcal{O}/(f_1)$. Sea ahora f_2 otro elemento que no se anula en ningún ideal primo minimal de $\mathcal{O}/(f_1)$, entonces $\dim \mathcal{O} > \dim \mathcal{O}/(f_1) > \dim \mathcal{O}/(f_1, f_2)$. Así sucesivamente, hasta llegar a dimensión cero, de donde se deduce

$$\dim \mathcal{O} \geq \text{ número mínimo de parámetros de los sist. de param..}$$

b) Número mínimo de parámetros de los sistemas de parámetros de $\mathcal{O} \geq$ grado del polinomio de Samuel de $\mathcal{O}$:

Sea $(f_1,\dots,f_r) = I$ un sistema de parámetros. Sea $A = (\mathcal{O}/I)[x_1,\dots,x_r]$, $J = (x_1,\dots,x_r)$. El morfismo

$$\begin{aligned} A &\longrightarrow G_I\mathcal{O} \\ x_i &\longmapsto \bar{f}_i \in I/I^2 \end{aligned}$$

es un epimorfismo, luego $S_{\mathcal{O},I}(n) \leq l(A/J^n) \overset{4.2.11}{=} l(\mathcal{O}/I)\cdot\binom{n+r-1}{r}$. Por tanto, $\operatorname{gr} S_{\mathcal{O},\mathfrak{m}}(n) = \operatorname{gr} S_{\mathcal{O},I}(n) \leq r$.

c) Grado del polinomio de Samuel de $\mathcal{O} \geq$ dimensión de Krull de $\mathcal{O}$:

Procedamos por inducción sobre el grado de $S_{\mathcal{O}}(n)$. Si $\operatorname{gr} S_{\mathcal{O}}(n) = 0$, entonces $l(\mathcal{O}/\mathfrak{m}^n)$ es constante (para todo $n >> 0$). Por tanto, $l(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$, es decir $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ (para $n >> 0$). Por el lema de Nakayama $\mathfrak{m}^n = 0$, luego $\dim\mathcal{O} = 0$.

Supongamos ya que $\operatorname{gr} S_{\mathcal{O}}(n) > 0$ y sea $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_m$ una cadena de ideales primos de $\mathcal{O}$. Tomemos $f \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$. Entonces

$$\operatorname{gr} S_{\mathcal{O}}(n) \geq \operatorname{gr} S_{\mathcal{O}/\mathfrak{p}_1}(n) \overset{4.2.23}{>} \operatorname{gr} S_{\mathcal{O}/(\mathfrak{p}_1,f)}(n) \geq m-1$$

donde la última desigualdad se debe a la hipótesis de inducción y a que $\bar{\mathfrak{p}}_2 \subset \cdots \subset \bar{\mathfrak{p}}_m$ es una cadena de ideales primos de $\mathcal{O}/(\mathfrak{p}_1, f)$. Por tanto, $\operatorname{gr} S_{\mathcal{O}}(n) \geq m$ y $\operatorname{gr} S_{\mathcal{O}}(n) \geq \dim\mathcal{O}$.

□

27. Corolario: *La dimensión de Krull de un anillo local noetheriano es finita y coincide con el grado del polinomio de Samuel.*

No es cierto, en general, que si un anillo es noetheriano, pero no local, su dimensión de Krull sea finita: véase el problema 7.

28. Corolario: *La dimensión de $\mathcal{O}$ coincide con la dimensión del anillo local en el vértice del cono tangente.*

Demostración. El vértice del cono viene definido por el ideal maximal irrelevante de $G_{\mathfrak{m}}\mathcal{O}$, esto es, por $I = \bigoplus_{r>0} \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Como el polinomio de Samuel de $\mathcal{O}$ coincide con el polinomio de Samuel de $G_{\mathfrak{m}}\mathcal{O}$ respecto a I, se concluye. □

Por el problema 8, la dimensión del anillo local en el vértice del cono tangente coincide con la dimensión del cono tangente, luego la dimensión de Krull de $\mathcal{O}$ coincide con la dimensión de su cono tangente.

29. Teorema del ideal principal de Krull: *Sea $f \in \mathcal{O}$ no invertible. Entonces,*

$$\dim \mathcal{O}/(f) \geq \dim \mathcal{O} - 1.$$

Además, si f no es divisor de cero, entonces

$$\dim \mathcal{O}/(f) = \dim \mathcal{O} - 1.$$

Demostración. Sea $(f_1, \ldots, f_m)$ un sistema de parámetros de $\mathcal{O}/(f)$, con el número mínimo de parámetros. Por el teorema anterior $\dim \mathcal{O}/(f) = m$. Por otra parte, $(f, f_1, \ldots, f_m)$ es un sistema de parámetros de $\mathcal{O}$, luego $\dim \mathcal{O} \leq m + 1$, es decir, $\dim \mathcal{O}/(f) \geq \dim \mathcal{O} - 1$.

Si f no es divisor de cero, entonces $\dim \mathcal{O}/(f) = \operatorname{gr} S_{\mathcal{O}/(f)}(n) \overset{4.2.23}{<} \operatorname{gr} S_{\mathcal{O}}(n) = \dim \mathcal{O}$ y se concluye.

□

4.3. Anillos locales regulares

El objetivo de esta sección es caracterizar localmente los anillos de funciones de las variedades algebraicas sin singularidades, es decir, regulares. Diremos que una variedad algebraica de dimensión n es regular en un punto si y solo si existen n hipersuperficies que se cortan (transversalmente) en el punto con multiplicidad de corte 1. Está definición equivaldrá a que el cono tangente a la variedad en el punto sea un espacio afín. Probaremos que un punto racional de una variedad algebraica es regular si y solo si es liso y daremos criterios diferenciales que caractericen la regularidad.

1. Notación: En esta sección supondremos que $\mathcal{O}$ es un anillo local y noetheriano de ideal maximal $\mathfrak{m}$.

2. Definición: Diremos que $\mathcal{O}$ es regular, si $\dim \mathcal{O} = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. El espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ se denomina espacio cotangente de Zariski.

Si $\mathcal{O}$ es local y noetheriano, entonces $\dim \mathcal{O} \leq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$: Sea $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = n$ y $\{f_1, \ldots, f_n\}$ un sistema de generadores de $\mathfrak{m}$, entonces $\dim \mathcal{O} \leq n$, por 4.2.26. Por tanto,

$$\mathcal{O} \text{ es regular} \Leftrightarrow \dim \mathcal{O} \geq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2..$$

3. Proposición: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión n. $\mathcal{O}$ es regular si y solo si existe un sistema de n parámetros $f_1, \ldots, f_n$ que generan el ideal maximal.*

Demostración. Si $\mathscr{O}$ es un anillo regular entonces $n = \dim \mathscr{O} = \dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. Si $f_1,\dots,f_n$ es un sistema generador de $\mathfrak{m}$ obtenido por Nakayama, éste será el sistema de parámetros buscado. Recíprocamente, si $f_1,\dots,f_n$ es un sistema de parámetros que generan $\mathfrak{m}$ entonces $\dim \mathscr{O} = n \geq \dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathscr{O}$ es regular. □

Aunque no hayamos definido la multiplicidad de intersección, digamos que esta proposición se interpreta geométricamente del siguiente modo: "Una variedad algebraica irreducible $X = \operatorname{Spec} A$ de dimensión n, es regular en un punto cerrado $x \in X$ si y solo si existen n hipersuperficies, $(f_i)_0$, que se cortan con multiplicidad 1 en x".

4. Proposición : *El anillo local de $k[x_1,\dots,x_n]$ en el origen es un anillo regular de dimensión n.*

Demostración. Denotemos $\mathfrak{m}_{or} = (x_1,\dots,x_n)$. Sabemos que $k[x_1,\dots,x_n]_{or}$ es un anillo local de dimensión n. Como $\dim_k \mathfrak{m}_{or}/\mathfrak{m}_{or}^2 = n$ se concluye. □

El morfismo de $\mathscr{O}/\mathfrak{m}$-módulos $\mathfrak{m}/\mathfrak{m}^2 \hookrightarrow G_{\mathfrak{m}}\mathscr{O}$ induce el epimorfismo graduado de anillos graduados $S^{\cdot}_{\mathscr{O}/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2 \to G_{\mathfrak{m}}\mathscr{O}$, $\bar{f}_1 \cdots \bar{f}_n \mapsto \overline{f_1 \cdots f_n}$.

5. Teorema : *$\mathscr{O}$ es regular si y solo si $G_{\mathfrak{m}}\mathscr{O} = S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. Es decir, $\mathscr{O}$ es regular si y solo si el cono tangente en el punto cerrado es un espacio afín.*

Demostración. En primer lugar, obsérvese que el polinomio de Samuel de $\mathscr{O}$ coincide con el polinomio de Samuel de $G_{\mathfrak{m}}\mathscr{O}$ respecto del ideal irrelevante.

Si $\mathscr{O}$ es un anillo regular de dimensión r, entonces $\dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = r$ y $S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \simeq \mathscr{O}/\mathfrak{m}[x_1,\dots,x_r]$. El epimorfismo

$$\begin{array}{rl} S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) & \xrightarrow{\pi} G_{\mathfrak{m}}\mathscr{O} \\ \bar{f}_1 \cdots \bar{f}_i & \longmapsto \overline{f_1 \cdots f_i} \end{array}$$

es además es inyectivo: porque si $\operatorname{Ker}\pi \neq 0$,

$$r = \operatorname{gr} S_{G_{\mathfrak{m}}\mathscr{O}}(n) = \operatorname{gr} S_{S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)/\operatorname{Ker}\pi}(n) \underset{4.2.23}{<} \operatorname{gr} S_{S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)}(n) \underset{4.3.4}{=} r$$

Recíprocamente, si $G_{\mathfrak{m}}\mathscr{O} = S^{\cdot}_{\mathscr{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$, entonces por 4.3.4, el polinomio de Samuel de $\mathscr{O}$ tiene grado $\dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathscr{O}$ es regular. □

6. Corolario : *Sea $\mathscr{O}$ un anillo local noetheriano. Entonces, $\mathscr{O}$ es un anillo regular de dimensión r si y solo si $S_{\mathscr{O}}(n) = \binom{n+r-1}{r}$.*

Demostración. Si $S_{\mathcal{O}}(n) = \binom{n+r-1}{r}$ entonces es $\mathcal{O}$ tiene dimensión de Krull r y $l(\mathcal{O}/\mathfrak{m}^2) = \binom{r+1}{r} = r+1$, luego $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = r$ y $\mathcal{O}$ es regular. Si $\mathcal{O}$ es regular de dimensión de Krull r, entonces $G_{\mathfrak{m}}\mathcal{O} = \mathcal{O}/\mathfrak{m}[x_1,\dots,x_r]$ y la función de Samuel es igual a $\binom{n+r-1}{r}$.

□

7. Lema: *Si $G_{\mathfrak{m}}\mathcal{O}$ es íntegro entonces $\mathcal{O}$ es íntegro.*

Demostración. Sean $f, g \in \mathcal{O}$, no nulas. Por el Lema de Krull, $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$. Por tanto, existen $r,s \in \mathbb{N}$ de modo que $f \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}$, $g \in \mathfrak{m}^s \setminus \mathfrak{m}^{s+1}$. Es decir, $\bar{f} \in \mathfrak{m}^r/\mathfrak{m}^{r+1}$ y $\bar{g} \in \mathfrak{m}^s/\mathfrak{m}^{s+1}$ son no nulas. Por tanto, $0 \neq \bar{f}\cdot\bar{g} = \overline{f\cdot g} \in \mathfrak{m}^{r+s}/\mathfrak{m}^{r+s+1}$ y $f\cdot g \neq 0$.

□

8. Proposición: *Si $\mathcal{O}$ es regular, entonces es íntegro.*

Demostración. $G_{\mathfrak{m}}\mathcal{O} = k[x_1,\dots,x_n]$ es un anillo íntegro, luego $\mathcal{O}$ es íntegro por el lema anterior. □

9. Proposición: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión 1. $\mathcal{O}$ es regular si y solo si es de ideales principales.*

Demostración. Sea $\mathfrak{m}$ el maximal de $\mathcal{O}$. Si $\mathcal{O}$ es regular de dimensión 1, entonces $\mathfrak{m}$ está generado por un parámetro, $\mathfrak{m} = (t)$ y $\mathcal{O}$ es íntegro. Luego $\mathcal{O}$ es d.i.p. Recíprocamente, si $\mathfrak{m}$ es principal, $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \leq 1$, luego $\dim \mathcal{O} \geq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ y $\mathcal{O}$ es regular.

□

Sea x el punto cerrado de $\operatorname{Spec}\mathcal{O}$. Si $f \in \mathfrak{m}_x$, denotaremos $d_x f$ la clase de f en $\mathfrak{m}_x/\mathfrak{m}_x^2$ y la denominaremos diferencial de f en x. En el caso de que $\mathcal{O}$ sea una k-álgebra y $\mathcal{O}/\mathfrak{m}_x = k$, estas definiciones coinciden con las del capítulo 3.

10. Teorema: *Sea $\mathcal{O}$ un anillo local regular de ideal maximal $\mathfrak{m}_x$ y sea $I \subset \mathcal{O}$ un ideal. Entonces $\mathcal{O}/I$ es regular $\Leftrightarrow$ I está generado por un sistema de parámetros cuyas diferenciales en x son linealmente independientes.*

Demostración. Denotemos $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en $\mathcal{O}/I$.

$\Leftarrow$) Si $I = (f_1,\dots,f_r)$ y $\{d_x f_1,\dots,d_x f_r\}$ son linealmente independientes en $\mathfrak{m}_x/\mathfrak{m}_x^2$, entonces la sucesión

$$0 \to I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

es exacta, porque $\bar{f}_1,\dots,\bar{f}_r$ es un sistema generador de $I/\mathfrak{m}_x I$ linealmente independiente en $\mathfrak{m}_x/\mathfrak{m}_x^2$. Por tanto,

$$\dim_{\mathcal{O}/\mathfrak{m}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim_{\mathcal{O}/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 - r = \dim \mathcal{O} - r \leq \dim \mathcal{O}/I$$

luego $\mathcal{O}/I$ es regular (y de dimensión $\dim\mathcal{O}-r$).

$\Rightarrow$) Supongamos que $\mathcal{O}/I$ es regular. Escribamos $\dim\mathcal{O}=n$ y $\dim\mathcal{O}/I=n-r$. Consideremos la sucesión exacta

$$I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Sean $f_1,\dots,f_r \in I$ tales que $\bar{f}_1,\dots,\bar{f}_r$ formen una base del núcleo del epimorfismo $\mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2$. Se tiene un epimorfismo $\mathcal{O}/(f_1,\dots,f_r)\to\mathcal{O}/I$, que es isomorfismo: en efecto, por la implicación anterior, $\mathcal{O}/(f_1,\dots,f_r)$ es regular y de dimensión $n-r$; si hubiese núcleo, la dimensión de $\mathcal{O}/I$ sería menor que $n-r$, por 4.2.29, ya que $\mathcal{O}/(f_1,\dots,f_r)$ es íntegro por ser regular.

En conclusión, $I=(f_1,\dots,f_r)$ y $d_x f_1,\dots,d_x f_r$ son linealmente independientes. □

11. Corolario: *Sea $\mathcal{O}$ un anillo local regular de dimensión de Krull n, de ideal maximal $\mathfrak{m}_x$ y sea $I=(f_1,\cdots,f_r)\subset\mathfrak{m}_x$ un ideal tal que la dimensión de Krull de $\mathcal{O}/I$ es $n-r$. Entonces $\mathcal{O}/I$ es regular $\Leftrightarrow$ $d_x f_1,\dots,d_x f_r$ son linealmente independientes.*

Demostración. $\Leftarrow$) Es consecuencia inmediata del Teorema 4.3.10.

$\Rightarrow$) $I/\mathfrak{m}_x I=(\bar{f}_1,\dots,\bar{f}_r)$, luego $\dim_{\mathcal{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I\le r$. De la sucesión exacta

$$I/\mathfrak{m}_x I \xrightarrow{i} \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

$\dim_{\mathcal{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I \ge \dim_{\mathcal{O}/\mathfrak{m}_x}\mathfrak{m}_x/\mathfrak{m}_x^2 - \dim_{\mathcal{O}/\mathfrak{m}}\bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = r$. Luego, $\dim_{\mathcal{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I = r$ e i es inyectivo. Por tanto, $d_x f_1,\dots,d_x f_r$ son linealmente independientes.

□

12. Definición: Sea A un anillo noetheriano y $X=\operatorname{Spec}A$. Diremos que X es regular en un punto cerrado x, si A_x es un anillo regular. Diremos que X es regular si lo es en todo punto cerrado.

13. Ejercicio: Sea $X=\operatorname{Spec}k[x_1,\dots,x_n]/(p(x_1,\dots,x_n))$. Demostrar que X es regular en un punto $\alpha=(\alpha_1,\dots,\alpha_n)$ si y solo si $\sum_i \frac{\partial p}{\partial x_i}(\alpha)d_\alpha x_i \neq 0$

14. Teorema: *Sea $x\in\operatorname{Spec}A$ un punto racional de una k-variedad algebraica. Entonces, x es regular $\Leftrightarrow$ es liso. Por tanto, una variedad algebraica sobre un cuerpo algebraicamente cerrado es regular si y solo si es lisa.*

Demostración. $\Rightarrow$) Sea Σ el cuerpo de fracciones de A. Como A_x es regular $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x = \operatorname{gr}\operatorname{tr}\Sigma = n$. Sea $\omega_1,\dots,\omega_n$ un sistema generador de $\Omega_{A_x/k}$ obtenido por el lema

de Nakayama (recordemos que $\Omega_{A_x/k} \otimes_{A_x} A_x/\mathfrak{m}_x = \mathfrak{m}_x/\mathfrak{m}_x^2$). Consideremos la sucesión exacta

$$0 \to \operatorname{Ker}\phi \to A_x \oplus \overset{n}{\cdots} \oplus A_x \xrightarrow{\phi} \Omega_{A_x/k} \to 0$$
$$(0,\ldots,\underset{i}{1},\ldots,0) \longmapsto \omega_i$$

Los anillos regulares son íntegros. Localizando en el punto genérico, g, tenemos

$$0 \to (\operatorname{Ker}\phi)_g \longrightarrow \Sigma \oplus \overset{n}{\cdots} \oplus \Sigma \longrightarrow \Omega_{\Sigma/k} \to 0$$

Ahora bien, por la proposición 3.6.35, $\dim_\Sigma \Omega_{\Sigma/k} = \operatorname{gr}\operatorname{tr}\Sigma = n$. Por tanto, $(\operatorname{Ker}\phi)_g = 0$. Pero $\operatorname{Ker}\phi$ está incluido en un A_x-módulo libre, que no tiene torsión, luego $\operatorname{Ker}\phi = 0$ y $\Omega_{A_x/k} = A_x \oplus \overset{n}{\cdots} \oplus A_x$.

$\Leftarrow$) Si $\Omega_{A_x/k}$ es un A_x-módulo libre de rango $\dim A_x$, entonces

$$\dim A_x = \dim_{A_x/\mathfrak{m}_x}(\Omega_{A_x/k} \otimes_{A_x} A_x/\mathfrak{m}_x) = \dim_{A_x/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2,$$

luego A_x es regular.

□

En 4.4.26 veremos que las variedades lisas son regulares. Una k-variedad es lisa si y solo si lo es por cambio de base al cierre algebraico de k. El ejercicio siguiente muestra que el concepto de regularidad no es estable por cambio de base, pues la curva del ejercicio no es lisa pero sí regular y por cambio de base al cierre algebraico no es lisa, luego tampoco regular.

15. Ejercicio: Sea $k = \mathbb{Z}/3\mathbb{Z}(t)$ y $A = \operatorname{Spec} k[x,y]/(y^2 + x^3 - t)$. Demuestra que la curva plana $\operatorname{Spec} A$ es regular en todo punto cerrado pero $\Omega_{A_x/k}$ no es un A_x-módulo libre de rango 1 para $\mathfrak{m}_x = (x^3 - t, y)$.

4.4. Compleción

Dada una filtración $\{M_i\}$ de un módulo M podemos definir una topología en M: Una base de entornos de cada $m \in M$ es $\{m + M_i\}$. Esta topología viene definida por la seudométrica

$$d(m_1,m_2) := \begin{cases} 2^{-n} & \text{si } m_1 - m_2 \in M_n, \text{ y } m_1 - m_2 \notin M_{n+1} \\ 0 & \text{si } m_1 - m_2 \in M_n \text{ para todo } n \end{cases}$$

Una vez que hemos definido d, podemos hablar de sucesiones convergentes, de sucesiones de Cauchy y la compleción de M por d.

1. Definición: Una sucesión $\{m_i\}$ se dice de Cauchy cuando para cada $\epsilon > 0$ existe un k tal que $d(m_n, m_{n'}) < \epsilon$, para cualesquiera $n, n' > k$. Se dice que la sucesión es convergente a cero si para cada $\epsilon > 0$ existe un k tal que $d(m_n, 0) < \epsilon$, para todo $n > k$.

2. Definición: Llamaremos compleción de M respecto de la topología definida por una filtración, al A-módulo

$$\widehat{M} := \{\text{Sucesiones de Cauchy}\}/\{\text{Sucesiones convergentes a cero}\}$$

3. Proposición: $\widehat{M} = \varprojlim_{j\in\mathbb{N}} M/M_j$.

Demostración. Si $(\bar{m}_j) \in \varprojlim_j M/M_j$, entonces $\bar{m}_{i+r} = \bar{m}_i$ en M/M_i. La sucesión (m_i) es de Cauchy, porque dado 2^{-j}, $d(m_r, m_s) < 2^{-j}$, para todo $r, s \geq j$. Así pues, tenemos definido el morfismo

$$\varprojlim_j M/M_j \to \widehat{M},\ (\bar{m}_i) \mapsto [(m_i)]$$

Dejamos como ejercicio la comprobación de que está bien definido.

Definamos la asignación inversa. Sea (m_i) una sucesión de Cauchy. Dado 2^{-j}, existe $n_j \in \mathbb{N}$ tal que $d(m_r, m_s) < 2^{-j}$, para todo $r, s \geq n_j$. Es decir, $m_r - m_s \in M_j$ para todo $r, s \geq n_j$, luego $\bar{m}_r = \bar{m}_s$ en M/M_j para todo $r, s \geq n_j$.

El morfismo

$$\{\text{Sucesiones de Cauchy}\} \to M/M_j,\ (m_i) \mapsto \bar{m}_{n_j}$$

no depende del $n_j >> 0$ escogido. En particular, dada una sucesión (m_i) convergente a cero, se tiene que $\bar{m}_{n_j} = 0$. Por tanto, los morfismos

$$\widehat{M} \to M/M_j,\ [(m_i)] \mapsto \bar{m}_{n_j}$$

están bien definidos y definen un morfismo

$$\widehat{M} \to \varprojlim_j M/M_j,\ [(m_i)] \mapsto (\bar{m}_{n_j})$$

Dejamos como ejercicio la comprobación de que estas asignaciones son inversas entre sí.

□

4. Observación: Un ejemplo de sucesión de Cauchy lo constituyen las series $\sum_{i=0}^{\infty} m_i$ ($m_i \in M_i$). Es más, toda sucesión de Cauchy es equivalente a una serie de esta forma. En efecto, por la proposición anterior, basta verlo para la sucesión de Cauchy (n_i), con $(\bar{n}_i) \in \varprojlim_i M/M_i$. Tenemos que $n_{i+1} - n_i = m_i \in M_i$, luego $n_1 = m_0$, $n_2 = m_1 + n_1 = m_1 + m_0$, $n_3 = m_2 + n_2 = m_2 + m_1 + m_0$, etc. Así pues,

$$\widehat{M} = \{\sum_{i=0}^{\infty} m_i,\ m_i \in M_i\}/\{\text{Series convergentes a cero}\}$$

Consideremos cada elemento $m \in M$ como la sucesión constante (m), tenemos definido un morfismo $M \to \hat{M}$; de otro modo, los morfismos de paso al cociente $M \to M/M_i$ definen un morfismo $M \to \hat{M} = \varprojlim_j M/M_j$; o de otro modo, cada $m \in M$, puede considerarse como la serie $m + 0 + \cdots + 0 + \cdots \in \hat{M}$.

5. Proposición: *M con la filtración $\{M_n\}$ es separado $\iff \bigcap_{n\in\mathbb{N}} M_n = 0 \iff M \to \widehat{M}$ es inyectivo.*

Demostración. El núcleo del morfismo $M \to \widehat{M} = \varprojlim_i M/M_i$ es $\bigcap_{n\in\mathbb{N}} M_n$, luego se obtiene el segundo $\iff$.

Si M es separado, para cada $m \in M$ existe un entorno M_n del cero que no contiene a m, es decir, $m \notin M_n$. Luego $\bigcap_{n\in\mathbb{N}} M_n = 0$. Recíprocamente, si $\bigcap_{n\in\mathbb{N}} M_n = 0$, entonces d es una distancia, porque si $d(m,m') = 0$, entonces $m - m' \in M_n$ para todo n, es decir que $m - m' \in \bigcap_{n\in\mathbb{N}} M_n = 0$, luego $m = m'$. Por tanto, M es separado. □

Sean M, N dos A-módulos con filtraciones respectivas $\{M_i\}$ y $\{N_i\}$. Un morfismo de A-módulos $f : M \to N$ se dice compatible si $f(M_n) \subseteq N_n$. Evidentemente un morfismo compatible $f : M \to N$ induce un morfismo entre los completados

$$\widehat{f} : \widehat{M} \to \widehat{N}.$$

6. Teorema: *Sea $0 \to M' \to M \xrightarrow{\pi} M'' \to 0$ una sucesión exacta de A-módulos y $\{M_i\}$ una filtración de M. Si se consideran en M' y M'' las filtraciones inducidas $\{M' \cap M_i\}$, $\{\pi(M_i)\}$, la sucesión de completados*

$$0 \to \widehat{M'} \to \widehat{M} \xrightarrow{\widehat{\pi}} \widehat{M''} \to 0$$

es exacta. Es decir, "completar conserva sucesiones exactas".

Demostración. Tenemos las sucesiones exactas de sistemas proyectivos

$$0 \to M'/M' \cap M_i \to M/M_i \xrightarrow{\pi} M''/\pi(M_i) \to 0$$

Por tanto, como el límite proyectivo es exacto por la izquierda tenemos la sucesión exacta

$$0 \to \widehat{M'} \to \widehat{M} \xrightarrow{\widehat{\pi}} \widehat{M''}$$

Sólo nos falta ver la epiyectividad de $\widehat{\pi}$: Dada una serie $\sum_{i=0}^{\infty} m_i''$, con $m_i'' \in \pi(M_i)$, sean $m_i \in M_i$ tales que $\pi(m_i) = m_i''$. Es obvio que $\widehat{\pi}(\sum_{i=0}^{\infty} m_i) = \sum_{i=0}^{\infty} m_i''$, luego por la observación anterior hemos concluido. □

7. Corolario: *$\widehat{M}_n$ es un submódulo de $\widehat{M}$ y $\widehat{M}/\widehat{M}_n = M/M_n$, para todo $n \in \mathbb{N}$.*

Demostración. Por el teorema anterior $\widehat{M}_n \hookrightarrow \widehat{M}$ y $\widehat{M}/\widehat{M}_n = \widehat{(M/M_n)}$. Ahora bien,

$$\widehat{(M/M_n)} = \varprojlim_i (M/M_n + M_i) = \varprojlim_{i>n} (M/M_n + M_i) = \varprojlim_{i>n} M/M_n = M/M_n$$

con lo que concluimos. □

8. Corolario: *$\widehat{M}$ es completo y separado, respecto de la topología definida por la filtración $\{\widehat{M}_n\}$. Es decir, $\widehat{\widehat{M}} = \widehat{M}$.*

Demostración. Es una consecuencia directa del corolario anterior y 4.4.5. □

9. Corolario: *Si consideramos en M una filtración $\{M_n\}$ y en $\widehat{M}$ la filtración $\{\widehat{M}_n\}$, entonces $G\widehat{M} = G\widehat{M}$.*

Demostración. Observemos que $M_n/M_{n+1} = \widehat{M_n/M_{n+1}} = \widehat{M}_n/\widehat{M}_{n+1}$. □

4.4.1. Topología I-ádica. Compleción I-ádica

Por la proposición 4.2.16, todas las filtraciones I-estables de un A-módulo M definen la misma topología y la misma compleción.

10. Definición: Sea $I \subset A$ un ideal y M un A-módulo. La filtración

$$M \supseteq IM \supseteq I^2M \supseteq \cdots \supseteq I^nM \supseteq \ldots$$

se denomina filtración I-ádica. Obviamente es una filtración I-estable. La topología definida por cualquier filtración I-estable se denomina la topología I-ádica.

De ahora en adelante, completar se entenderá que es completar respecto de la topología I-ádica.

11. Ejemplos: 1. $\varprojlim_{n\in\mathbb{N}} \mathscr{C}^\infty(\mathbb{R})/\mathfrak{m}_\alpha^n = \mathbb{R}[[x-\alpha]] \simeq \mathbb{R}[[t]]$ (con $t = x-\alpha$), donde el $\mathfrak{m}_\alpha$ es el ideal de funciones diferenciables que se anulan en α. El morfismo natural $\mathscr{C}^\infty(\mathbb{R}) \to \varprojlim_{n\in\mathbb{N}} \mathscr{C}^\infty(\mathbb{R})/\mathfrak{m}_\alpha^n = \mathbb{R}[[x-\alpha]]$ asigna a cada función su desarrollo de Taylor en α. El cuerpo de fracciones $k((t))$ de $k[[t]]$ es

$$k((t)) = k[[t]]_t = \{\frac{\lambda_{-n}}{t^n} + \cdots + \frac{\lambda_{-1}}{t} + \lambda_0 + \lambda_1 t + \cdots + \lambda_m t^m + \cdots \mid \lambda_i \in k, n \in \mathbb{N}\}.$$

2. $\varprojlim_{n\in\mathbb{N}} k[x]/(x)^n = k[[x]]$. El morfismo $k[x] \to \varprojlim_{n\in\mathbb{N}} k[x]/(x)^n = k[[x]]$, es el morfismo que considera cada polinomio como una serie.

3. Números p-ádicos $\underset{\text{Not}}{=} \hat{\mathbb{Z}}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{\sum_{n\in\mathbb{N}} a_n p^n,\ 0 \le a_i < p\}$. El morfismo natural

$$\mathbb{N} \to \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{\sum_{n\in\mathbb{N}} a_n p^n,\ 0 \le a_i < p\}$$

asigna a cada número natural su desarrollo como suma de potencias de p. El cuerpo de fracciones $\widehat{\mathbb{Q}}_p$ de $\widehat{\mathbb{Z}}_p$ es

$$\widehat{\mathbb{Q}}_p = \{\frac{a_{-n}}{p^n} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + \cdots + a_m p^m + \cdots \mid 0 \le a_i < p, n \in \mathbb{N}\}.$$

12. Proposición: *Sea $I \subset A$ un ideal. Entonces,*

1. $\hat{A}/\hat{I} = A/I$.
2. *$s \in \hat{A}$ es invertible si y solo si $\bar{s} \in \hat{A}/\hat{I}$ es invertible.*
3. $\mathrm{Spec}_{max}\,\hat{A} = \mathrm{Spec}_{max}\,A/I$.

Demostración. 1. La compleción I-ádica de la sucesión exacta $0 \to I \to A \to A/I \to 0$ es, por el teorema 4.4.6, la sucesión exacta

$$0 \to \hat{I} \to \hat{A} \to A/I \to 0$$

2. $\Leftarrow$) Sea $s' \in \hat{A}$ tal que $ss' = 1 \mod \hat{I}$. Basta ver que $t = ss'$ es invertible. Tenemos que $t = 1 + \sum_{n>0} i_n$, con $i_n \in I^n$. Calculando $\frac{1}{t}$ obtenemos que t es invertible.

3. Si $\mathfrak{m}$ es un ideal maximal de $\hat{A}$ que no contiene a $\hat{I}$, entonces $\mathfrak{m}+\hat{I}=\hat{A}$ y existe $m\in\mathfrak{m}$ tal que $m=1 \mod \hat{I}$, luego m es invertible y hemos llegado a contradicción. En conclusión, todo ideal maximal de $\hat{A}$ contiene a $\hat{I}$ y

$$\operatorname{Spec}_{max}\hat{A}=\operatorname{Spec}_{max}\hat{A}/\hat{I}=\operatorname{Spec}_{max}A/I.$$

□

13. Proposición: *Sea A noetheriano. Si*

$$0\to M'\to M\to M''\to 0$$

es una sucesión exacta de A-módulos finito generados, entonces

$$0\to \widehat{M'}\to \widehat{M}\to \widehat{M''}\to 0$$

es exacta.

Demostración. Sabemos que si completamos M' por la filtración $\{M'\cap I^nM\}$, M por la filtración $\{I^nM\}$ y M'' por la filtración $\{I^nM''\}$, entonces la sucesión completada es exacta. Ahora bien, por Artin-Rees la filtración $\{M'\cap I^nM\}$ es I-estable, luego completar por esta filtración es equivalente a completar por la topología I-ádica. Hemos terminado. □

14. Corolario: *Si A es noetheriano y M es un A-módulo finito generado, entonces*

$$M\otimes_A\widehat{A}=\widehat{M}$$

Demostración. Si M es libre es inmediato. Como A es noetheriano y M es finito, M es de presentación finita, luego se tiene una sucesión exacta

$$L_2\to L_1\to M\to 0$$

con L_1, L_2 libres finito generados. Tensando por $\widehat{A}$ y completando, se obtiene el diagrama de filas exactas

$$\begin{array}{ccccccc} L_2\otimes_A\widehat{A} & \longrightarrow & L_1\otimes_A\widehat{A} & \longrightarrow & M\otimes_A\widehat{A} & \longrightarrow & 0 \\ \| & & \| & & \downarrow & & \\ \widehat{L_2} & \longrightarrow & \widehat{L_1} & \longrightarrow & \widehat{M} & \longrightarrow & 0 \end{array}$$

Luego, $M\otimes_A\widehat{A}=\widehat{M}$. □

15. Corolario: *Si A es noetheriano, el morfismo $A \to \widehat{A}$ es plano.*

Demostración. Sea $M' \to M$ un morfismo inyectivo de A-módulos. Pongamos M como límite inductivo de módulos finito generados $M = \varinjlim M_i$ y sea $M'_i = M' \cap M_i$, que también es finito generado. Por la proposición anterior y su corolario

$$M'_i \otimes_A \widehat{A} \to M_i \otimes_A \widehat{A}$$

es inyectivo. Tomando límite inductivo y teniendo en cuenta que el producto tensorial conmuta con límites inductivos, se obtiene que

$$M' \otimes_A \widehat{A} \to M \otimes_A \widehat{A}$$

es inyectivo. Por tanto, $A \to \widehat{A}$ es plano. □

Dada una filtración $\{M_n\}$ de un módulo M, en $\widehat{M}$ considerábamos, en la sección anterior, la filtración $\{\widehat{M}_n\}$. Veamos que si en M consideramos la filtración I-ádica, entonces la filtración $\{\widehat{I^n M}\}$ es justamente la I-ádica de $\widehat{M}$, cuando I es un ideal finito generado. La igualdad $\widehat{I^n M} = I^n \widehat{M}$ puede interpretarse intuitivamente como la igualdad: $\sum_{i \geq n} a_i x^i = x^n \cdot \sum_{i \geq 0} a_{n+i} x^i$. Con precisión:

16. Proposición: *Si I es un ideal finito generado (por ejemplo, si A es un anillo noetheriano), entonces $\widehat{I^n M} = I^n \widehat{M}$. Además, $\widehat{M}$ es completo y separado con la topología I-ádica, $\widehat{M}/I^n \widehat{M} = M/I^n M$ y $G_I \widehat{M} = G_I M$.*

Demostración. Consideremos la inyección $I^n M \hookrightarrow M$. Completando tenemos la inyección $\widehat{I^n M} \hookrightarrow \widehat{M}$.

Sea $i_1, \ldots, i_r$ un sistema generador de I^n. Consideremos el epimorfismo

$$M \oplus \overset{r}{\cdots} \oplus M \to I^n M, (m_1, \ldots, m_r) \mapsto \sum_j i_j m_j.$$

Completando I-ádicamente tenemos un epimorfismo $\widehat{M} \oplus \overset{r}{\cdots} \oplus \widehat{M} \to \widehat{I^n M}$ y recordemos la inyección $\widehat{I^n M} \hookrightarrow \widehat{M}$. Hemos obtenido que $\widehat{I^n M} = I^n \widehat{M}$.

Todo lo demás es consecuencia de 4.4.7, 4.4.8 y 4.4.9.

□

4.4.2. Compleción y noetherianidad

Queremos probar que el completado de un anillo noetheriano es noetheriano. Un anillo noetheriano y su completado tienen el mismo graduado y éste es noetheriano. Probaremos que si el graduado de un anillo completo y separado es noetheriano el anillo es noetheriano y así obtendremos que el completado de un anillo noetheriano es noetheriano.

Un teorema básico en Análisis y Geometría Diferencial, es el teorema de la función inversa. Toda aplicación diferenciable $f: X \to Y$, entre variedades diferenciales, induce una aplicación entre los anillos $C^\infty(Y) \to C^\infty(X)$ y los espacios cotangentes $f^*: \mathfrak{m}_{f(x)}/\mathfrak{m}_{f(x)}^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$. El teorema de la función inversa afirma que si f^* es un isomorfismo entonces f es un isomorfismo en un entorno de x. Ahora bien, f^* es un isomorfismo si y solo si el morfismo graduado $G_{\mathfrak{m}_{f(x)}}C^\infty(Y) \to G_{\mathfrak{m}_x}C^\infty(X)$ lo es. Analíticamente, si el morfismo $G_{\mathfrak{m}_{f(x)}}C^\infty(Y) \to G_{\mathfrak{m}_x}C^\infty(X)$ es un isomorfismo entonces el morfismo $\widehat{C^\infty(Y)} \to \widehat{C^\infty(X)}$ es un isomorfismo. Hablemos ahora en Álgebra y con toda precisión.

17. Teorema formal de la función inversa: *Sean $\{M_n\}$ y $\{M'_n\}$ filtraciones de los A-módulos M y M' respectivamente. Supongamos que M y M' son completos y separados. Sea $f: M \to M'$ un morfismo de A-módulos compatible con las filtraciones y consideremos el morfismo $G(f): GM \to GM'$ inducido. Si $G(f)$ es isomorfismo (resp. epiyectivo, inyectivo), entonces $f: M \to M'$ es isomorfismo (resp. epiyectivo, inyectivo).*

Demostración. Supongamos que el morfismo $G(f)$ es epiyectivo. Sea $m' \in M'$. Como el morfismo $M/M_1 \to M'/M'_1$ es epiyectivo, existe $m_0 \in M$, tal que $m' = f(m_0) + m'_1$, con $m'_1 \in M'_1$. Como el morfismo $M_1/M_2 \to M'_1/M'_2$ es epiyectivo, existe $m_1 \in M_1$, tal que $m'_1 = f(m_1) + m'_2$, con $m'_2 \in M'_2$. Es decir, $m' = f(m_0) + f(m_1) + m'_2$. Así sucesivamente, obtenemos una serie $m = \sum_{i=0}^{\infty} m_i$, con $m_i \in M_i$, tal que $f(m) = f(\sum_{i=0}^{\infty} m_i) = \sum_{i=0}^{\infty} f(m_i) = m'$.

Supongamos ahora que $G(f)$ es inyectivo. Sea $m \in M$. Como M es separado existe $r \in \mathbb{N}$ tal que $m \in M_r$ y $m \notin M_{r+1}$. Entonces, $\bar{m}$ es no nulo en M_r/M_{r+1}, luego $G(f)(\bar{m}) = \overline{f(m)}$ es no nulo, porque $G(f)$ es inyectivo. Por tanto, $f(m) \neq 0$ y f es inyectivo.

En particular, si $G(f)$ es isomorfismo, f es isomorfismo.

□

18. Lema: *Sea A un anillo completo y separado para la topología I-ádica. Si $G_I A$ es noetheriano, entonces A es noetheriano.*

Demostración. Dado un ideal $\mathfrak{q} \subset A$ tenemos que ver que $\mathfrak{q}$ es finito generado. Consideremos en $\mathfrak{q}$ la filtración $\{\mathfrak{q}_n = \mathfrak{q} \cap I^n\}$. Se tiene una inclusión natural

$$G\mathfrak{q} \hookrightarrow G_I A$$

Además $G\mathfrak{q}$ es un ideal de $G_I A$ de modo natural. Como GA es noetheriano, $G\mathfrak{q}$ está generado por un número finito de elementos, que podemos suponer que son homogéneos. Sea $\bar{x} \in \mathfrak{q}_n/\mathfrak{q}_{n+1}$ una de los generadores y $x \in \mathfrak{q}_n$ un representante de la clase de $\bar{x}$. Consideremos en A la siguiente filtración: $A_0 = A, \dots, A_n = A, A_{n+1} = I, A_{n+2} = I^2, \dots$. El morfismo $A \to \mathfrak{q}$ dado por $1 \mapsto x$ es compatible con las filtraciones. Haciendo lo mismo con todos los generadores de $G\mathfrak{q}$ y tomando la suma directa de todas las A, tendremos un morfismo $L = A^m \to \mathfrak{q}$. Por construcción, el morfismo inducido en los graduados $GL \to G\mathfrak{q}$ es epiyectivo, luego $L = \widehat{L} \to \widehat{\mathfrak{q}}$ es epiyectivo, por el teorema anterior. El ideal $\mathfrak{q}$ es separado porque es un submódulo de A, que es separado, luego el morfismo $i\colon \mathfrak{q} \hookrightarrow \widehat{\mathfrak{q}}$ es inyectivo. Por tanto, $L \to \mathfrak{q}$ ha de ser epiyectivo, porque lo es la composición $L \to \mathfrak{q} \hookrightarrow \widehat{\mathfrak{q}}$. En conclusión, $\mathfrak{q}$ es finito generado. □

19. Teorema: *Si A es noetheriano entonces $\widehat{A}$ es noetheriano.*

Demostración. Si A es noetheriano e $I \subset A$ es un ideal, entonces $I = (\xi_1, \dots, \xi_r)$ es finito generado. El morfismo

$$\begin{aligned}(A/I)[x_1, \dots, x_r] &\longrightarrow G_I A \\ x_i &\longmapsto \bar{\xi}_i \in I/I^2\end{aligned}$$

es epiyectivo, luego $G_I A$ es noetheriano.

Por 4.4.16, $G_I \widehat{A} = G_I A$. Por el lema anterior, $\widehat{A}$ es noetheriano. □

20. Proposición: *Sea $\mathscr{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Sea $\widehat{\mathscr{O}}$ la compleción $\mathfrak{m}$-ádica de $\mathscr{O}$. Entonces,*

$$\dim \mathscr{O} = \dim \widehat{\mathscr{O}}$$

Demostración. $\mathscr{O}/\mathfrak{m}^n = \widehat{\mathscr{O}}/\widehat{\mathfrak{m}}^n$, luego $S_{\mathscr{O}}(n) = S_{\widehat{\mathscr{O}}}(n)$ y $\dim \mathscr{O} = \dim \widehat{\mathscr{O}}$. □

21. Proposición: *Sea $\mathscr{O}$ un anillo local noetheriano de maximal $\mathfrak{m}$ y $\widehat{\mathscr{O}}$ el completado $\mathfrak{m}$-ádico de $\mathscr{O}$. Entonces, $\mathscr{O}$ es regular si y solo si $\widehat{\mathscr{O}}$ es regular.*

Demostración. Se deduce de la igualdad $G_{\mathfrak{m}} \mathscr{O} = G_{\widehat{\mathfrak{m}}} \widehat{\mathscr{O}}$ y del teorema 4.3.5. □

22. Proposición: *Si A es noetheriano, entonces $A[[x_1, \dots, x_n]]$ es noetheriano.*

Demostración. Por el teorema de la base de Hilbert, si A es noetheriano entonces $A[x_1, \dots, x_r]$ es noetheriano. Como $A[[x_1, \dots, x_n]]$ es el completado de $A[x_1, \dots, x_r]$ por el ideal $(x_1, \dots, x_r)$, se concluye por el teorema anterior. □

4.4.3. Teorema de Cohen

Como hemos dicho en la introducción, el teorema de Cohen es un teorema de estructura de los anillos completos. Sin precisar, afirma que la compleción de un anillo local noetheriano es un cociente de un anillo de series formales. En el caso de que el anillo completo sea regular, probaremos que es isomorfo a un anillo de series formales.

23. Teorema de Cohen: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, completo y separado por la topología $\mathfrak{m}$-ádica. Si $\mathcal{O}$ contiene un cuerpo, entonces existe una sección del morfismo natural $\mathcal{O} \to \mathcal{O}/\mathfrak{m}$.*

Demostración. Denotemos $K = \mathcal{O}/\mathfrak{m}$. En general hay muchas secciones de $\mathcal{O} \to K$. Para construir una, bastará definir secciones $K \to \mathcal{O}/\mathfrak{m}^n$ que conmuten con los epimorfismos naturales $\pi_n \colon \mathcal{O}/\mathfrak{m}^n \to \mathcal{O}/\mathfrak{m}^{n-1}$, pues $\mathcal{O} = \widehat{\mathcal{O}} = \varprojlim \mathcal{O}/\mathfrak{m}^n$. Supongamos construido $K \subseteq \mathcal{O}/\mathfrak{m}^{n-1}$ y construyamos $K \to \mathcal{O}/\mathfrak{m}^n$ compatible con el anterior.

a) Supongamos que $\mathcal{O}$ contiene un cuerpo de característica cero. Por tanto, $\mathbb{Q} \subset \mathcal{O}$.

Sea K_1 una $\mathbb{Q}$-subextensión de cuerpos de K maximal con la condición de que el morfismo $K_1 \subseteq \mathcal{O}/\mathfrak{m}^{n-1}$ extienda a $\mathcal{O}/\mathfrak{m}^n$. Tenemos que ver que $K_1 = K$. Sea $\bar{a} \in K \subseteq \mathcal{O}/\mathfrak{m}^{n-1}$. Si $\bar{a}$ es un elemento K_1-trascendente, sea $a \in \mathcal{O}/\mathfrak{m}^n$ tal que $\pi_n(a) = \bar{a}$. El morfismo $K_1(\bar{a}) \to \mathcal{O}/\mathfrak{m}^n, \bar{a} \mapsto a$ está bien definido. Por la maximalidad de K_1, $\bar{a} \in K_1$. Si $\bar{a}$ es algebraico sobre K_1, sea $p(x) \in K_1[x]$ su polinomio mínimo anulador. Sea $a \in \mathcal{O}/\mathfrak{m}^n$ tal que $\pi_n(a) = \bar{a}$. Para que el morfismo $K_1(\bar{a}) \to \mathcal{O}/\mathfrak{m}^n, \bar{a} \mapsto a$, esté bien definido es necesario que $p(a) = 0$. Para ello, vamos a modificar a convenientemente. Sea $h \in \mathfrak{m}^{n-1}/\mathfrak{m}^n \subset \mathcal{O}/\mathfrak{m}^n$. Desarrollando por Taylor obtenemos

$$p(a+h) = p(a) + p'(a)h$$

pues $h^2 = 0$. Observemos que $\pi_n(p(a)) = p(\bar{a}) = 0$, luego $p(a) \in \mathfrak{m}^{n-1}/\mathfrak{m}^n$. Además $p'(a)$ es invertible, porque $(p(x), p'(x)) = (1)$ luego $(p(a), p'(a)) = (1)$ y como $p(a)$ es nilpotente, $p'(a)$ es invertible. En conclusión, si tomamos $h = -p(a)/p'(a)$, entonces $h \in \mathfrak{m}^{n-1}/\mathfrak{m}^n$, $\pi_n(a+h) = \bar{a}$ y $p(a+h) = 0$. Así pues, el morfismo $K_1(\bar{a}) \to \mathcal{O}/\mathfrak{m}^n, \bar{a} \mapsto a+h$ está bien definido. Por la maximalidad de K_1, $\bar{a} \in K_1$.

En conclusión, $K_1 = K$.

b) Supongamos que $\mathcal{O}$ contiene un cuerpo de característica $p > 0$.

Observemos que $\pi_n^{-1}(K) = \pi_n^{-1}(K \backslash 0) \cup \pi_n^{-1}(0)$, donde los elementos de $\pi_n^{-1}(K \backslash 0)$ son invertibles porque no son nilpotentes, y $\pi_n^{-1}(0) = \mathfrak{m}^{n-1}/\mathfrak{m}^n$. Por tanto, se cumple que $(\pi_n^{-1}(K))^p = \pi_n^{-1}(K \backslash 0)^p \cup 0$ es un cuerpo y el epimorfismo $\pi_n \colon (\pi_n^{-1}(K))^p \to K^p$ es un isomorfismo.

Sea L un subcuerpo máximo de $\pi_n^{-1}(K)$ que contenga a $(\pi_n^{-1}(K))^p := \{\lambda^p, \lambda \in \pi_n^{-1}(K)\}$. Si probamos que $\pi_n \colon L \hookrightarrow K$ es un isomorfismo concluimos. Dado $\bar{a} \in K \subseteq \mathcal{O}/\mathfrak{m}^{n-1}$,

sea $a \in \pi_n^{-1}(K)$ tal que $\pi_n(a) = \bar{a}$. Obviamente, $a^p \in (\pi_n^{-1}(K))^p \subset L$. Consideremos el epimorfismo

$$L[x]/(x^p - a^p) \to L[a],\ x \mapsto a$$

Si $\sqrt[p]{a^p} \notin L$, entonces $x^p - a^p$ es irreducible en $L[x]$, luego $L[x]/(x^p - a^p)$ es cuerpo y $L[x]/(x^p - a^p) \simeq L[a]$, lo cual contradice la maximalidad de L. Por tanto, $\sqrt[p]{a^p} \in L$ y $\pi_n(\sqrt[p]{a^p}) = a$. Luego $\pi_n : L \hookrightarrow K$ es un isomorfismo. □

24. Corolario : *Sea $\mathcal{O}$ un anillo local noetheriano de maximal $\mathfrak{m}$ y completo por la topología $\mathfrak{m}$-ádica. Si $\mathcal{O}$ contiene un cuerpo, entonces*

$$\mathcal{O} \simeq \mathcal{O}/\mathfrak{m}[[\xi_1, \ldots, \xi_n]]$$

Demostración. Por el teorema de Cohen, existe una sección $\mathcal{O}/\mathfrak{m} \hookrightarrow \mathcal{O}$ del cuerpo residual de $\mathfrak{m}$. Sea $\xi_1, \ldots, \xi_n$ un sistema generador de $\mathfrak{m}$. El morfismo

$$\begin{aligned} \mathcal{O}/\mathfrak{m}[[x_1, \ldots, x_n]] &\to \mathcal{O} \\ s(x_1, \ldots, x_n) &\mapsto s(\xi_1, \ldots, \xi_n) \end{aligned}$$

es un epimorfismo porque lo es entre los graduados. Por tanto, $\mathcal{O} \simeq \mathcal{O}/\mathfrak{m}[[\xi_1, \ldots, \xi_n]]$. □

25. Proposición: *Sea $\mathcal{O}$ un anillo local regular de maximal $\mathfrak{m}$ y completo por la topología $\mathfrak{m}$-ádica. Si $\mathcal{O}$ contiene un cuerpo, entonces*

$$\mathcal{O} \simeq \mathcal{O}/\mathfrak{m}[[x_1, \ldots, x_n]]$$

Demostración. Por el teorema de Cohen, existe una sección $\mathcal{O}/\mathfrak{m} \hookrightarrow \mathcal{O}$ del cuerpo residual de $\mathfrak{m}$. Sea $\xi_1, \ldots, \xi_n$ un sistema mínimo de generadores de $\mathfrak{m}$. El morfismo

$$\begin{aligned} \mathcal{O}/\mathfrak{m}[[x_1, \ldots, x_n]] &\to \mathcal{O} \\ s(x_1, \ldots, x_n) &\mapsto s(\xi_1, \ldots, \xi_n) \end{aligned}$$

es un isomorfismo porque lo es entre los graduados (recuérdese 4.3.5). □

26. Proposición: *Si $X = \operatorname{Spec} A$ es una variedad lisa entonces es regular.*

Demostración. Sea $x \in X$ un punto cerrado. Si el morfismo $\mathfrak{m}_x/\mathfrak{m}_x^2 \to \Omega_{A_x/k} \otimes_{A_x} A_x/\mathfrak{m}_x$, $\bar{a} \mapsto \overline{da}$ es inyectivo entonces $\dim_{k(x)} \mathfrak{m}_x/\mathfrak{m}_x^2 \leq \dim A_x$, donde $k(x) := A_x/\mathfrak{m}_x$, y por tanto A_x es regular.

Tenemos que ver que el morfismo $\mathfrak{m}_x/\mathfrak{m}_x^2 \to \Omega_{A_x/k} \otimes_{A_x} A_x/\mathfrak{m}_x$ es inyectivo: Por el teorema de Cohen tenemos un morfismo $k(x) \hookrightarrow A_x/\mathfrak{m}_x^2$, luego x es un punto $k(x)$-racional de $\operatorname{Spec} A_x/\mathfrak{m}_x^2$. El epimorfismo natural $\Omega_{A_x/k} \otimes_{A_x} A_x/\mathfrak{m}_x \to \Omega_{(A_x/\mathfrak{m}_x^2)/k(x)} \otimes_{A_x} A_x/\mathfrak{m}_x = \mathfrak{m}_x/\mathfrak{m}_x^2$ es un retracto del morfismo que queremos ver que es inyectivo. □

27. Lema: *Sean A y B d.i.p. locales (de ideales maximales $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente) y supongamos que $A/\mathfrak{m}$ es un cuerpo perfecto. Si $A \hookrightarrow B$ es un morfismo finito, entonces $B = A[\xi]$.*

Demostración. Denotemos $k = A/\mathfrak{m}$, $k' = B/\mathfrak{m}'$ y escribamos $\mathfrak{m}'/\mathfrak{m}'^2 = (\bar{f})$. $B/\mathfrak{m}B = B/\mathfrak{m}'^r$ y es una k-álgebra completa, luego por el teorema de Cohen 4.4.23, podemos suponer que es una k'-álgebra. Ahora es sencillo demostrar que el morfismo de k'-álgebras $k'[x]/(x^r) \to B/\mathfrak{m}B, x \mapsto f$ es un isomorfismo.

k es un cuerpo perfecto, luego $k' = k[\alpha]$, donde α es raíz de un polinomio $p(x)$ irreducible y separable con coeficientes en k. Así pues, $B/\mathfrak{m}B = k[\alpha, f]$. Ahora bien, $k[\alpha + f]$ es una k-subálgebra, luego es local; por tanto, el polinomio anulador de $\alpha + f$ es una potencia de un polinomio irreducible. Observemos que $p(\alpha+f) = p(\alpha)+p'(\alpha)f + f^2 \cdot h = 0 + f \cdot \text{invert.}$, luego el polinomio anulador de $\alpha + f$ es $p(x)^r$. Por dimensiones sobre k obtenemos que $k[\alpha + f] = B/\mathfrak{m}B$. Si $\xi \in B$ es un representante de $\alpha + f \in B/\mathfrak{m}'B$, por el lema Nakayama concluimos que $B = A[\xi]$. □

28. Teorema: *Sea $\varphi\colon A \to B$ un morfismo finito entre dominios de Dedekind, tal que el morfismo inducido entre los cuerpos de funciones sea separable. Supongamos que $A/\mathfrak{m}$ es un cuerpo perfecto, para todo ideal maximal $\mathfrak{m}$ de A. Entonces, $\mathrm{dif}_{B/A}$ es isomorfo a $\Omega_{B/A}$.*

Demostración. Si A y B fuesen locales entonces $B = A[\xi]$, por el lema 4.4.27. Si n es el rango del A-módulo libre B, entonces $1, \xi, \ldots, \xi^{n-1}$ es una base por el lema de Nakayama. Por lo tanto, $B = A[\xi] = A[x]/(p(x))$, donde $p(x)$ es un polinomio mónico de grado n. Por 3.8.35, concluimos.

Veamos que completando podemos suponer que A y B son locales y concluimos.

La localización de $\Omega_{B/A}$ y $\mathrm{dif}_{B/A}$ en el punto genérico de A es nula. Por tanto, el soporte de ambos A-módulo es un número finito de puntos cerrados y ambos son isomorfos a la suma directa de sus localizaciones en los puntos cerrados de $\operatorname{Spec} A$. Podemos suponer que A es local.

Tanto $\Omega_{B/A}$ como $\mathrm{dif}_{B/A}$ son A-módulos finito generados concentrados en el punto cerrado de A, luego son completos para la topología $\mathfrak{m}$-ádica. Por tanto,

$$\Omega_{B/A} = \widehat{\Omega}_{B/A} = \Omega_{B/A} \otimes_A \widehat{A} = \Omega_{\widehat{B}/\widehat{A}}$$

y

$$\mathrm{dif}_{B/A} = \widehat{\mathrm{dif}}_{B/A} = \mathrm{dif}_{B/A} \otimes_A \widehat{A} = \mathrm{dif}_{\widehat{B}/\widehat{A}}$$

$\widehat{A} \to \widehat{B}$ es un morfismo finito y $\widehat{A}$ es un anillo regular de dimensión 1, luego un dominio local de Dedekind. Veamos la estructura de $\widehat{B}$. Observemos que $\mathfrak{m}B = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, donde $x_1, \ldots, x_r$ son puntos cerrados de B. Por tanto,

$$\widehat{B} = \varprojlim_n B/\mathfrak{m}^n B = \varprojlim_n \prod_{i=1}^r (B/\mathfrak{m}^n B)_{x_i} = \prod_{i=1}^r \varprojlim_n (B/\mathfrak{m}^n B)_{x_i} = \prod_{i=1}^r \varprojlim_n B/\mathfrak{m}_{x_i}^n = \prod_{i=1}^r \widehat{B}_{x_i}$$

donde hemos denotado $\widehat{B}_{x_i} = \varprojlim_n B/\mathfrak{m}_{x_i}^n$. Por tanto, $\widehat{A} \to \widehat{B}_{x_i}$ es un morfismo finito entre dominios locales de Dedekind. Además, como $\Omega_{\widehat{B}/\widehat{A}} = \Omega_{B/A}$ está concentrado en el punto cerrado de $\widehat{A}$, el morfismo inducido por $\widehat{A} \to \widehat{B}_{x_i}$ en los cuerpos de fracciones es separable.

La descomposición $\widehat{B} = \prod_{i=1}^r \widehat{B}_{x_i}$ es ortogonal para la métrica de la traza, luego $\mathrm{dif}_{\widehat{B}/\widehat{A}} = \prod \mathrm{dif}_{\widehat{B}_{x_i}/\widehat{A}}$ y por tanto

$$\mathrm{dif}_{B/A} = \mathrm{dif}_{\widehat{B}/\widehat{A}} = \prod \mathrm{dif}_{\widehat{B}_{x_i}/\widehat{A}} = \prod \Omega_{\widehat{B}_{x_i}/\widehat{A}} = \Omega_{\widehat{B}/\widehat{A}} = \Omega_{B/A}.$$

□

4.4.4. Lema de Hensel

29. Teorema: *Sea $\mathscr{O}$ un anillo local de ideal maximal $\mathfrak{m}_x$ y sea $\mathscr{O}'$ una $\mathscr{O}$-álgebra finita, completa y separada por la topología $\mathfrak{m}_x$-ádica. Entonces $\mathscr{O}'$ descompone en producto directo de $\mathscr{O}$-álgebras finitas, locales, completas y separadas.*

Demostración. $\mathscr{O}'/\mathfrak{m}_x\mathscr{O}'$ es una $\mathscr{O}/\mathfrak{m}_x$-álgebra finita. Consideremos el morfismo natural $f\colon \mathrm{Spec}\mathscr{O}' \to \mathrm{Spec}\mathscr{O}$ y sea $f^{-1}(x) = \mathrm{Spec}\mathscr{O}'/\mathfrak{m}_x\mathscr{O}' = \{y_1, \dots, y_n\}$, que son los puntos cerrados de $\mathscr{O}'$. Obviamente, se cumple que $\mathrm{Spec}\mathscr{O}'/\mathfrak{m}_x^r\mathscr{O}' = \{y_1, \dots, y_n\}$ y por tanto,

$$\mathscr{O}'/\mathfrak{m}_x^r\mathscr{O}' = (\mathscr{O}'/\mathfrak{m}_x^r\mathscr{O}')_{y_1} \times \cdots \times (\mathscr{O}'/\mathfrak{m}_x^r\mathscr{O}')_{y_n}.$$

Además $\mathfrak{m}_{y_i}^{n_i}\mathscr{O}'_{y_i} \subseteq \mathfrak{m}_x\mathscr{O}'_{y_i}$, para ciertos $n_i \in \mathbb{N}$, pues $\mathfrak{m}_{y_i}$ es nilpotente en $(\mathscr{O}'/\mathfrak{m}_x\mathscr{O}')_{y_i}$, ya que es una $\mathscr{O}/\mathfrak{m}_x$-álgebra finita. Completando por el ideal $\mathfrak{m}_x$ obtenemos que

$$\mathscr{O}' = \widehat{\mathscr{O}'_{y_1}} \times \cdots \times \widehat{\mathscr{O}'_{y_n}}$$

Esta igualdad muestra que $\widehat{\mathscr{O}'_{y_i}}$ son completos y separados por la topología $\mathfrak{m}_x$-ádica, y son locales de ideal maximal $\mathfrak{m}_{y_i}$. Por tanto, $\widehat{\mathscr{O}'_{y_i}} = \mathscr{O}'_{y_i}$ es completo y separado por la topología $\mathfrak{m}_{y_i}$-ádica. □

30. Definición: Un anillo $\mathscr{O}$ se dice henseliano si toda $\mathscr{O}$-álgebra finita descompone en producto directo de $\mathscr{O}$-álgebras locales.

Los anillos noetherianos locales y completos son henselianos, por el teorema anterior.

31. Lema de Hensel: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, completo y separado por la topología $\mathfrak{m}$-ádica. Sea $p(x) \in \mathcal{O}[x]$ un polinomio mónico. Si $\overline{p(x)} \in (\mathcal{O}/\mathfrak{m})[x]$ descompone $\overline{p(x)} = f'(x) \cdot g'(x)$, siendo $f'(x), g'(x) \in (\mathcal{O}/\mathfrak{m})[x]$ polinomios mónicos primos entre sí, entonces existen polinomios mónicos $f(x), g(x) \in \mathcal{O}[x]$ tales que $p(x) = f(x) \cdot g(x)$ y $f'(x) = \overline{f(x)}$, $g'(x) = \overline{g(x)}$.*

Demostración. Consideremos la $\mathcal{O}$-álgebra finita libre $\mathcal{O}' = \mathcal{O}[x]/(p(x))$. Por el teorema anterior $\mathcal{O}'$ descompone en producto de álgebras locales, $\mathcal{O}' = \mathcal{O}'_1 \times \cdots \times \mathcal{O}'_r$. Haciendo cociente por $\mathfrak{m}$ resulta $\bar{\mathcal{O}}' = \bar{\mathcal{O}}'_1 \times \cdots \times \bar{\mathcal{O}}'_r = (\mathcal{O}/\mathfrak{m})[x]/(\overline{p(x)}) = (\mathcal{O}/\mathfrak{m})[x]/(f'(x)) \times \mathcal{O}/\mathfrak{m}[x]/(g'(x))$. Como la descomposición de un álgebra en producto de álgebras locales es única, se obtiene una descomposición $\mathcal{O}' = B_1 \times B_2$ de modo que $\bar{B}_1 = (\mathcal{O}/\mathfrak{m})[x]/(f'(x))$ y $\bar{B}_2 = (\mathcal{O}/\mathfrak{m})[x]/(g'(x))$. Como $\mathcal{O}'$ es un $\mathcal{O}$-módulo libre también lo son B_1 y B_2. Si $f'(x)$ tiene grado r, entonces $1, x, \cdots, x^r$ es base de B_1, pues módulo $\mathfrak{m}$ es base de $\mathcal{O}/\mathfrak{m}[x]/(f'(x))$. Por tanto, $x^{r+1} = \sum_{i=0}^{r} a_i x^i$, en B_1, con $a_i \in \mathcal{O}$. Denotemos $f(x) = x^{r+1} - \sum_{i=0}^{r} a_i x^i$; el epimorfismo $\mathcal{O}[x]/(f(x)) \to B_1$ es isomorfismo porque son libres del mismo rango y es isomorfismo módulo $\mathfrak{m}$. Además, $\overline{f(x)} = f'(x)$. La clase de $p(x)$ en B_1 es cero, luego $f(x)$ divide a $p(x)$. Tomando $g(x) = \frac{p(x)}{f(x)}$, se concluye. □

32. Corolario: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, completo y separado por la topología $\mathfrak{m}$-ádica. Sea $p(x) \in \mathcal{O}[x]$ un polinomio mónico. Si $\overline{p(x)} \in (\mathcal{O}/\mathfrak{m})[x]$ tiene una raíz en $\mathcal{O}/\mathfrak{m}$ de multipicidad 1, entonces $p(x)$ tiene una raíz en $\mathcal{O}$.*

4.5. Problemas

1. Prueba que si un anillo tiene un número finito de elementos, entonces es noetheriano y de dimensión cero.

2. Sea $X = \operatorname{Spec} k[x,y,z]/(y + x + x^3 + y^4, y - x + x^2)$ y $x \in X$ el origen. Prueba que $C_{X,x} = \operatorname{Spec} k[x,y,z]/(y+x, y-x) = \mathbb{A}_1$.

3. Calcula el polinomio de Samuel del anillo local en el origen de $k[x,y]/(y^2 - x^2 + x^3)$.

4. Sea $\mathcal{O}$ un anillo local noetheriano. Prueba que la dimensión de Krull de $\mathcal{O}$ es igual a la dimensión del cono tangente $G_{\mathfrak{m}}\mathcal{O} = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ en el origen (que es el ideal maximal $\bigoplus_{n=1}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$).

5. Sea A un anillo noetheriano. Prueba que $\dim A[x] = 1 + \dim A$ (Pistas: Si $\mathfrak{p} \subset A$ es un ideal primo entonces $\mathfrak{p}A[x]$ es un ideal primo de $A[x]$. Dado un ideal primo $\mathfrak{p}_y$ de $A[x]$, existen un ideal primo $\mathfrak{p}$ de A y $p(x) \in A[x]$ tales que $\mathfrak{p}_y \cdot A[x]_y = (\mathfrak{p}, p(x))$).

6. Sea A un anillo noetheriano de dimensión de Krull 2. Prueba que el conjunto $\operatorname{Spec} A$ tiene infinitos puntos.

7. Consideremos el anillo de polinomios de infinitas variables $A = k[x_1, x_2, \ldots, x_n, \ldots]$. Sean $\mathfrak{p}_i := (x_{2^i}, \ldots, x_{2^{i+1}-1}) \subset A$ y $S = A \setminus \bigcup_i \mathfrak{p}_i$.

   a) Prueba que $\operatorname{Spec}_{max} A_S = \{\mathfrak{p}_i \cdot A_S\}_i$.

   b) Prueba que toda función no nula de A_S pertenece a un número finito de ideales maximales.

   c) Prueba que A_S es un anillo noetheriano.

   d) Prueba que $\dim A_S = \infty$. (Nagata)

8. Sea $A = k[\xi_1, \ldots, \xi_n]$ un anillo graduado, con $\operatorname{gr} \xi_i = 1$. Prueba:

   a) Si $\mathfrak{p} \subset A$ es un ideal primo, el ideal generado por los elementos homogéneos de $\mathfrak{p}$ es un ideal primo.

   b) Los ideales primos minimales de A son ideales primos homogéneos.

   c) $\dim A = \dim A_{or}$, donde $\mathfrak{m}_{or} = (\xi_1, \ldots, \xi_n)$.

   d) $\dim \operatorname{Proj} A$ es igual al grado del polinomio $p(n) := \dim_k [A]_n$.

9. Sean A y B dos k-álgebras y $x \in \operatorname{Spec} A = X$, $y \in \operatorname{Spec} B = Y$ dos puntos racionales. Prueba que

$$C_{(x,y)}(X \times_k Y) = C_x X \times_k C_y Y$$

10. Calcula el polinomio de Samuel de un anillo local regular de dimensión 2.

11. Prueba que la localización de $\mathbb{Z}[x]$ en cualquier punto es un anillo regular.

12. Calcula los puntos de $\mathbb{Z}[\sqrt[2]{5}]$ en los que no es regular.

13. Demuestra que todo ideal de $k[[x]]$ es de la forma (x^n).

14. Prueba que los ideales de los enteros p-ádicos, $\hat{\mathbb{Z}}_p$, son de la forma (p^n). Expresa $(1-p)^{-1}$ como una serie en p. Prueba que el 2 tiene raíz cuadrada en $\hat{\mathbb{Z}}_7$.

15. Sea $\hat{A}$ el completado I-ádico del anillo noetheriano A. Prueba que si $f \in A$ no es divisor de cero entonces no es divisor de cero en $\hat{A}$.

16. Sea $A = k[x,y]/(y^2 - x^2 + x^3)$ y $\mathfrak{m}$ el maximal $(\bar{x}, \bar{y})$. Supongamos que $\operatorname{car} k \neq 2$. Prueba que $\widehat{A} = k[[x,y]]/(y^2 - x^2 + x^3)$. Prueba que $y^2 - x^2 + x^3$ descompone en producto de dos series ("ramas"), que se corresponden con los dos ideales primos minimales del anillo completo considerado.

17. Calcula la compleción de $k[x_1,\ldots,x_n]/(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$ por el ideal $(x_1,\ldots,x_n)$.

18. Sea $\cdots \to X_n \to \cdots \to X_2 \to X_1 \to X_0$ una sucesión de aplicaciones entre conjuntos finitos no vacíos. Pruébese que $\varprojlim_i X_i$ es no vacío.

19. Sea $p(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ y $p \in \mathbb{Z}$. Prueba que la condición necesaria y suficiente para que $p(x) = 0$ tenga una solución en $\hat{\mathbb{Z}}_p^n$ es que tenga alguna solución en cada $(\mathbb{Z}/p^m\mathbb{Z})^n$, para todo $m > 0$.

20. Calcula el inverso de $1 + x$ en $k[[x]]$. Prueba que el único ideal maximal de $k[[x]]$ es (x). ¿Existe la raíz cuadrada de $1 + x$ en $k[[x]]$?

21. Prueba que $\dim k[[x_1,\ldots,x_n]] = n$.

22. Sea $I \subset A$ un ideal y M un A-módulo.

    a) Dado un abierto V que contiene a $(I)_0$, demuesta que existe $i \in I$ tal que $(I)_0 \subseteq U_{1+i} \subseteq V$.

    b) Prueba que

    $$\operatorname{Spec} A_{1+I} = \bigcap_{\substack{\text{Abierto } U \\ (I)_0 \subset U}} U \quad \text{y} \quad \operatorname{Spec}_{\max} A_{1+I} = \operatorname{Spec}_{\max} A/I.$$

    c) Demuestra que la compleción I-ádica de M coincide con la compleción I-ádica de M_{1+I}.

    d) Supongamos que A es un anillo noetheriano y M es finito generado. Prueba que el núcleo del morfismo de compleción $M \to \hat{M}$ coincide con el núcleo del morfismo de localización $M \to M_{1+I}$.

23. Sea A un anillo noetheriano íntegro, $I \subset A$ un ideal propio. Prueba que A es separado con la topología I-ádica.

24. Sea A un anillo noetheriano. Prueba que $\bigcap_{x,n} \mathfrak{m}_x^n = 0$.

25. Sea A un anillo noetheriano y M un A-módulo finito generado. Prueba que $M = 0$ si y solo si sus compleciones en todo punto cerrado de $\operatorname{Spec} A$ son nulas.

26. Sea $\mathfrak{m} \subset A$ un ideal maximal finito generado. Sea N un A-módulo plano. Prueba que la compleción $\mathfrak{m}$-ádica de N es isomorfa a la compleción de un A-módulo libre. Si N es finito generado, prueba que $\hat{N}$ es un $\hat{A}$-módulo libre finito generado.

Capítulo 5

Curvas algebraicas

5.1. Introducción

La Teoría de Curvas Algebraicas y la Teoría de Números son teorías estrecha y sorprendentemente relacionadas. $\mathbb{Z}$ y $k[x]$ son anillos euclídeos y ambos son dominios de factorización única. Los anillos de funciones de las curvas algebraicas son $k[x]$-álgebras finitas (geométricamente: toda curva se proyecta vía un morfismo finito en la recta afín). Los anillos de enteros, como veremos, son $\mathbb{Z}$-álgebras finitas ($\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$ son ejemplos). Estamos hablando en ambos casos de anillos noetherianos de dimensión de Krull 1. En la teoría de Galois se han estudiado anillos de dimensión de Krull cero, ahora estudiamos los de dimensión de Krull 1. Entre estos anillos, en ambas teorías, destacarán los anillos que son localmente anillos de ideales principales: los anillos de Dedekind.

Por concisión, hablemos solo de las curvas algebraicas; en la Teoría de Números tendremos resultados equivalentes. Los anillos de funciones de las curvas algebraicas son localmente anillos de Dedekind, salvo en un número finito de puntos: los puntos singulares de la curva. Probaremos que toda curva es isomorfa, salvo en un número finito de puntos, a una curva sin puntos singulares. Estudiaremos el proceso denominado de explosión que nos permitirá desingularizar las curvas. Definiremos la multiplicidad de una variedad en un punto. Calcularemos la multiplicidad de intersección de una curva y una hipersuperficie en un punto. Veremos que el número de ramas analíticas de una curva en un punto coincide con el número de puntos en los que desingulariza la curva en el punto. Por último, en el caso de una única rama introduciremos el desarrollo en serie de Puiseux, que parametriza analíticamente la curva.

Fuera del estudio local de las variedades, probaremos el teorema de Bézout, que dice que dos curvas planas proyectivas de grados n y m se cortan en $n \cdot m$ puntos, contando grados y multiplicidades de intersección. Probaremos también el lema de Max

Noether, que nos permitirá probar como ejercicios, los teoremas de Pascal y Pappus.

5.2. Anillos de valoración

En la clasificación de la curvas algebraicas es fundamental el caracterizar los puntos singulares (los puntos no regulares) de las curvas y la regularización o desingularización de éstas. Como veremos, los anillos locales regulares de dimensión uno son los anillos de valoración discreta, y la intersección de los anillos de valoración que contienen a un anillo es su cierre entero, que en el caso de anillos de curvas es el anillo de su desingularización.

1. Definición: Sea Σ un cuerpo y $\Sigma^* = \Sigma\backslash\{0\}$. Una valoración discreta de Σ es una aplicación epiyectiva $v\colon \Sigma^* \to \mathbb{Z}$ que verifica

1. $v(fg) = v(f) + v(g)$, para todo $f, g \in \Sigma^*$.
2. $v(f+g) \geq \min\{v(f), v(g)\}$, para todo $f, g \in \Sigma^*$ (con la convención $v(0) = \infty$).

2. Ejemplo: Sea $\mathcal{O}$ un anillo local y regular de ideal maximal $\mathfrak{m}$ y cuerpo de fracciones Σ. Para cada $f \in \mathcal{O}$ no nula, denotemos $v_{\mathfrak{m}}(f)$ al máximo número natural n tal que $f \in \mathfrak{m}^n$. Es fácil ver que la aplicación

$$\begin{aligned} v_{\mathfrak{m}}\colon \Sigma^* &\to \mathbb{Z} \\ f/g &\mapsto v_{\mathfrak{m}}(f/g) = v_{\mathfrak{m}}(f) - v_{\mathfrak{m}}(g) \end{aligned}$$

está bien definida y es una valoración discreta de Σ. Esta valoración se denomina valoración $\mathfrak{m}$-ádica.

Si además $\mathcal{O}$ es de dimensión 1, entonces es d.i.p por la proposición 4.3.9 y es inmediato ver que $\mathcal{O} = \{f \in \Sigma \mid v_{\mathfrak{m}}(f) \geq 0\}$.

3. Proposición: *Sea $v\colon \Sigma^* \to \mathbb{Z}$ una valoración discreta de un cuerpo Σ y denotemos $\mathcal{O}_v = \{f \in \Sigma : v(f) \geq 0\}$. Entonces $\mathcal{O}_v$ es un anillo noetheriano local y regular de dimensión 1, de cuerpo de fracciones Σ y $v = v_{\mathfrak{m}}$, siendo $\mathfrak{m}$ el maximal de $\mathcal{O}_v$.*

Demostración. Observemos que $v(1) = v(1 \cdot 1) = v(1) + v(1)$, luego $v(1) = 0$. Por tanto, $0 = v(1) = v(f \cdot f^{-1}) = v(f) + v(f^{-1})$, luego $v(f^{-1}) = -v(f)$.

Todo ideal $I \subset \mathcal{O}_v$ es principal y está generado por un elemento de valor mínimo: en efecto, sea $f \in I$ de valor mínimo. Dada $g \in I$, $v(g) \geq v(f)$, luego $v(g/f) = v(g) - v(f) \geq 0$. Por tanto, $g/f \in \mathcal{O}_v$ y $g = g/f \cdot f$, es decir, $I = (f)$.

Así pues, $\mathcal{O}_v$ es un anillo de ideales principales, luego noetheriano. $\mathcal{O}_v$ es un anillo local que no es un cuerpo, porque los invertibles son precisamente $\{f \in \mathcal{O}_v : v(f) = 0\}$

y el ideal maximal es $\mathfrak{p}_v := \{f \in \mathcal{O}_v : v(f) > 0\}$. Por tanto, $\mathcal{O}_v$ es un anillo local regular de dimensión 1. Además, para toda $f \in \Sigma$, o bien $f \in \mathcal{O}_v$ o bien $f^{-1} \in \mathcal{O}_v$ (pues $v(f) \geq 0$ ó $v(f^{-1}) = -v(f) \geq 0$). Por tanto, el cuerpo de fracciones de $\mathcal{O}_v$ es Σ. Para concluir, veamos que $v = v_{\mathfrak{m}}$. Sea t un parámetro que genere $\mathfrak{p}_v$. Si $f \in \mathcal{O}_v$, entonces $f = ut^n$, con u invertible, luego $v(f) = nv(t)$. Por tanto, $\operatorname{Im} v = v(t) \cdot \mathbb{Z}$, y como v es epiyectiva $v(t) = 1 = v_{\mathfrak{m}}(t)$, de donde se concluye que $v = v_{\mathfrak{m}}$. □

4. Definición: Dada una valoración discreta v diremos que $\mathcal{O}_v$ es un anillo de valoración discreta.

Por la proposición anterior, un anillo es de valoración discreta si y solo si es un anillo noetheriano, local y regular de dimensión 1.

5. Ejercicio: Sea $\mathcal{O}_v$ un anillo de valoración discreta y $f \in \mathcal{O}_v$. Prueba que $v(f) = l(\mathcal{O}_v/(f))$.

6. Definición: Sea $\mathcal{V}$ un anillo íntegro y Σ su cuerpo de fracciones. Diremos que $\mathcal{V}$ es un anillo de valoración si para todo $f \in \Sigma$, se verifica que $f \in \mathcal{V}$ ó $f^{-1} \in \mathcal{V}$.

Diremos que Σ es el anillo de valoración trivial de Σ. En la demostración anterior hemos visto que un anillo de valoración discreta es un anillo de valoración.

7. Proposición: *Sea $\mathcal{V}$ un anillo de valoración e I_1, I_2 ideales de $\mathcal{V}$. Entonces, $I_1 \subseteq I_2$ o $I_2 \subseteq I_1$. En particular, $\mathcal{V}$ es local.*

Demostración. Si $I_1 \not\subseteq I_2$ e $I_2 \not\subseteq I_1$, entonces existen $f_1 \in I_1, f_1 \notin I_2$ y $f_2 \in I_2, f_2 \notin I_1$. Si $f_1/f_2 \in \mathcal{V}$, entonces $f_1 = (f_1/f_2) \cdot f_2 \in I_2$, contradicción. Análoga contradicción si $f_2/f_1 \in \mathcal{V}$. □

El ideal maximal de un anillo de valoración $\mathcal{V}$ se denota $\mathfrak{p}_{\mathcal{V}}$ y se le llama ideal de valoración.

8. Proposición: *Un anillo noetheriano $\mathcal{V}$ es de valoración (no trivial) si y solo si es un anillo de valoración discreta.*

Demostración. Ya sabemos que si $\mathcal{V}$ es de valoración discreta entonces es de valoración. Recíprocamente, si $\mathcal{V}$ es noetheriano y de valoración, entonces todo ideal es principal, pues dado $I = (f_1, \ldots, f_n)$ tenemos que $(f_1) \subseteq (f_2)$ (o al revés), luego $I = (f_2, \ldots, f_n)$. Recurrentemente, obtendremos que I es principal. Por tanto, si $\mathcal{V}$ no es trivial, es un anillo local y regular de dimensión 1, es decir, un anillo de valoración discreta. □

Sea $\mathcal{V}$ un anillo de valoración y Σ su cuerpo de fracciones. Denotemos por $\mathcal{V}^*$ el grupo de los invertibles de $\mathcal{V}$. En el grupo $\Sigma^*/\mathcal{V}^*$, la relación definida por $\bar{f} \geq \bar{g}$ si $f \cdot g^{-1} \in \mathcal{V}$, es una relación de orden total: en efecto, dados $\bar{f}, \bar{g}$, o bien $f \cdot g^{-1} \in \mathcal{V}$, o bien

$g \cdot f^{-1} \in \mathcal{V}$, es decir, o bien $\bar{f} \geq \bar{g}$, o bien $\bar{g} \geq \bar{f}$. Es obvio además que si $\bar{f} \geq \bar{g}$, entonces $\bar{f} \cdot \bar{h} \geq \bar{g} \cdot \bar{h}$, para todo $\bar{h}$, es decir, el orden es lineal.

Denotemos $v : \Sigma^* \to \Sigma^*/\mathcal{V}^*$ el morfismo de paso al cociente. Se cumple que

1. $v(fg) = v(f) + v(g)$ (¡ahora denotamos la operación de $\Sigma^*/\mathcal{V}^*$ aditivamente!).

2. $v(f+g) \geq \text{mín}\{v(f), v(g)\}$ (seguimos la convención $v(0) \geq c$, para todo $c \in \Sigma^*/\mathcal{V}^*$).

Sólo tenemos que probar 2. Debemos demostrar que, o bien $(f+g)\cdot g^{-1} = f \cdot g^{-1} + 1 \in \mathcal{V}$, o bien $(f+g)\cdot f^{-1} = 1 + g \cdot f^{-1} \in \mathcal{V}$, lo que es obvio.

Recíprocamente, si G es un grupo abeliano totalmente ordenado y $v : \Sigma^* \to G$ es una aplicación cumpliendo las dos condiciones anteriores, entonces $\mathcal{V} = \{f \in \Sigma : v(f) \geq 0\}$ es un anillo de valoración. La condición necesaria y suficiente para que sea un anillo de valoración discreta es que $\text{Im}\, v$ sea isomorfo a $\mathbb{Z}$. Denotaremos los anillos de valoración, por razones obvias, $\mathcal{O}_v$.

9. Lema: *Los anillos de valoración son íntegramente cerrados en su cuerpo de fracciones.*

Demostración. Sea $\mathcal{O}_v$ un anillo de valoración y Σ su cuerpo de fracciones. Sea $f \in \Sigma$ entero sobre $\mathcal{O}_v$. Por tanto, verifica una relación entera

$$f^n + a_1 f^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathcal{O}_v$$

Si $f^{-1} \in \mathcal{O}_v$, entonces $f = -a_1 - a_2 f^{-1} - \cdots - a_n f^{1-n} \in \mathcal{O}_v$. Si $f^{-1} \notin \mathcal{O}_v$ entonces $f \in \mathcal{O}_v$, pues $\mathcal{O}_v$ es un anillo de valoración. En conclusión, $\mathcal{O}_v$ es íntegramente cerrado en su cuerpo de funciones.

De otro modo:

$$\begin{aligned} nv(f) = v(f^n) = v(-a_1 f^{n-1} - \ldots - a_n) &\geq \text{mín}\{v(-a_1 f^{n-1}), \ldots, v(-a_n)\} \\ &\geq \text{mín}\{(n-1)v(f), \ldots, v(f), 0\}, \end{aligned}$$

de donde se deduce que $v(f) \geq 0$. □

5.3. Cierre entero y anillos de valoración

1. Definición: Un morfismo $f : \mathcal{O} \hookrightarrow \mathcal{O}'$ inyectivo entre anillos locales de ideales maximales $\mathfrak{m}$,$\mathfrak{m}'$ se dice dominante si $\mathfrak{m} \hookrightarrow \mathfrak{m}'$, es decir, si $\mathfrak{m}' \cap \mathcal{O} = \mathfrak{m}$. También se dice que $\mathcal{O}'$ domina a $\mathcal{O}$.

2. Lema: *Sea A un anillo íntegro incluido en un cuerpo Σ. Se cumple que $\xi \in \Sigma$ es entero sobre A si y solo si $\xi \in A[\xi^{-1}]$.*

Demostración. Si ξ es entero sobre A, entonces existe una relación entera

$$\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0 = 0, \qquad \text{con } a_i \in A.$$

Multiplicando por ξ^{-n+1} obtenemos $\xi^1 + a_{n-1} + \cdots + a_0\xi^{-n+1} = 0$, luego $\xi \in A[\xi^{-1}]$.

Si $\xi \in A[\xi^{-1}]$, entonces $\xi = \sum_{i=1}^{n} a_i(\xi^{-1})^i$. Multiplicando por ξ^n tendremos

$$\xi^{n+1} - a_0\xi^n - \cdots - a_n = 0$$

Es decir, ξ es entero sobre A. □

3. Lema: *Sea $\mathcal{O}$ un anillo local íntegro incluido en un cuerpo Σ y sea $\xi \in \Sigma$. Entonces, un localizado (en un punto cerrado) de $\mathcal{O}[\xi]$ o $\mathcal{O}[\xi^{-1}]$ domina a $\mathcal{O}$.*

Demostración. Si ξ es entero sobre $\mathcal{O}$, entonces el morfismo $\mathcal{O} \hookrightarrow \mathcal{O}[\xi]$ es finito. Sea $\mathfrak{m}_x$ un ideal maximal de $\mathcal{O}[\xi]$ tal que $\mathfrak{m}_x \cap \mathcal{O} = \mathfrak{m}$, que existe porque los morfismos finitos inyectivos inducen una epiyección entre los espectros (3.3.18). Entonces el morfismo $\mathcal{O} \hookrightarrow \mathcal{O}[\xi]_x$ es dominante. Si ξ no es entero sobre $\mathcal{O}$, por el lema anterior $\xi \notin \mathcal{O}[\xi^{-1}]$, luego $(\xi^{-1}) \subsetneq \mathcal{O}[\xi^{-1}]$. Es más, como $\mathcal{O}[\xi^{-1}]/(\xi^{-1}) = \mathcal{O}/I$, entonces $\mathfrak{m}_x := (\mathfrak{m}, \xi^{-1})$ es un ideal maximal de $\mathcal{O}[\xi^{-1}]$. El morfismo $\mathcal{O} \hookrightarrow \mathcal{O}[\xi^{-1}]_x$ es dominante. □

4. Proposición: *Sea $\mathcal{O}$ un anillo local íntegro incluido en el cuerpo Σ. $\mathcal{O}$ es un anillo de valoración de Σ si y solo si el único anillo local $\mathcal{O}' \subset \Sigma$ que domina a $\mathcal{O}$ es $\mathcal{O}$.*

Demostración. Supongamos que $\mathcal{O}$ es de valoración. Sea $\mathcal{O}' \subset \Sigma$ un anillo local que contenga estrictamente a $\mathcal{O}$ y sea $\xi \in \mathcal{O}' \setminus \mathcal{O}$. Entonces $\xi^{-1} \in \mathcal{O}$, por ser $\mathcal{O}$ de valoración. Es más, ξ^{-1} pertenece al ideal maximal $\mathfrak{m}$ de $\mathcal{O}$, porque $\xi \notin \mathcal{O}$. En particular, $\xi^{-1} \in \mathcal{O}'$, luego ξ^{-1} no puede pertenecer a su ideal maximal $\mathfrak{m}'$, pues $\xi \in \mathcal{O}'$. En conclusión, $\xi^{-1} \in \mathfrak{m}$ y $\xi^{-1} \notin \mathfrak{m}'$, luego $\mathcal{O}'$ no domina a $\mathcal{O}$.

Supongamos ahora que en Σ no hay anillos locales que dominen a $\mathcal{O}$. Dado $\xi \in \Sigma$, por el lema 5.3.3, ξ o ξ^{-1} pertenecen a $\mathcal{O}$, luego es de valoración.

□

5. Corolario: *Sea $\mathcal{O}$ un anillo local íntegro incluido en el cuerpo Σ. Existe un anillo de valoración de Σ que domina a $\mathcal{O}$.*

Demostración. Por el lema de Zorn existe un anillo local $\mathcal{O}'$ incluido en Σ maximal dominando a $\mathcal{O}$. Por la maximalidad de $\mathcal{O}'$, éste no está dominado por ningún subanillo local de Σ, luego es un anillo de valoración de Σ por la proposición 5.3.4.

□

6. Teorema: *Sea A un anillo íntegro, Σ un cuerpo que contiene a A y $\bar{A}$ el cierre entero de A en Σ. Entonces $\bar{A}$ es la intersección de todos los anillos de valoración de Σ que contienen a A.*

Demostración. Sea $\xi \in \Sigma$. Si $\xi \in \bar{A}$ y $\mathcal{O}_v$ es un anillo de valoración que contiene a A, entonces ξ es entero sobre $\mathcal{O}_v$. Como $\mathcal{O}_v$ es íntegramente cerrado, $\xi \in \mathcal{O}_v$.

Si $\xi \notin \bar{A}$, entonces $\xi^{-1}A[\xi^{-1}] \subsetneq A[\xi^{-1}]$ por el lema 5.3.2. Por tanto, existe un ideal maximal $\mathfrak{m}_x \subset A[\xi^{-1}]$ que contiene a ξ^{-1}. Consideremos el anillo local $A[\xi^{-1}]_x$ y sea $\mathcal{O}_v$ un anillo de valoración de Σ que lo domine. Sea $\mathfrak{p}_v$ el ideal de valoración de $\mathcal{O}_v$, entonces $\xi^{-1} \in \mathfrak{p}_v$, luego $\xi \notin \mathcal{O}_v$.

□

Añadamos hipótesis noetherianas. Necesitamos antes el siguiente lema.

7. Lema: *Sea $A \hookrightarrow B$ un morfismo de anillos íntegros, tal que B/A es un A-módulo de longitud finita. Si $a \in A$ es tal que A/aA es un A-módulo de longitud finita entonces $l_A(A/aA) = l_A(B/aB)$.*

Demostración. Empecemos observando que el morfismo $B/A \xrightarrow{a\cdot} aB/aA$, $\bar{b} \mapsto \overline{ab}$, es un isomorfismo. Por tanto, $l_A(aB/aA) = l_A(B/A)$. Si consideramos el cuadrado conmutativo

$$\begin{array}{ccc} aA & \hookrightarrow & A \\ \downarrow & & \downarrow \\ aB & \hookrightarrow & B \end{array}$$

como la longitud de un cociente de módulos es el número de eslabones de las cadenas irrefinables que empiezan en el submódulo y terminan en el módulo, tendremos que $l_A(aB/aA) + l_A(B/aB) = l_A(B/aA) = l_A(B/A) + l_A(A/aA)$, y por lo tanto que $l_A(A/aA) = l_A(B/aB)$.

□

8. Lema : *Si A es un anillo noetheriano íntegro de dimensión 1, entonces el cierre entero de A en su cuerpo de fracciones es un anillo noetheriano de dimensión 1.*

Demostración. Sea $\bar{A}$ el cierre entero de A. Sabemos que $\dim \bar{A} = \dim A = 1$. Todo ideal no nulo de $\bar{A}$ corta a A en un ideal no nulo, pues dado $a' \in \bar{A}$ si el morfismo $A \to \bar{A}/a'\bar{A}$ fuese inyectivo tendríamos que $\dim A = \dim \bar{A}/a'\bar{A} \leq \dim \bar{A} - 1 = 0$, lo que es contradictorio. Entonces, para probar que $\bar{A}$ es noetheriano basta ver que $\bar{A}/a\bar{A}$ es un A-módulo de longitud finita, para todo $a \in A$. $\bar{A} = \varinjlim_i A_i$ es el límite inductivo de sus A-subálgebras finitas. Si $l_A(\bar{A}/a\bar{A}) > l_A(A/aA)$ entonces $l_A(A_i/aA_i) > l_A(A/aA)$, para algún i. Ahora bien, A_i/A y A/aA son A-módulos de longitud finita (pues su soporte es un número finito de puntos cerrados de $\operatorname{Spec} A$) y por el lema 5.3.7, $l_A(A_i/aA_i) = l_A(A/aA)$. En conclusión, $l_A(\bar{A}/a\bar{A}) \leq l_A(A/aA)$.

□

9. Lema: *Sea $\mathcal{O}$ un anillo local noetheriano de cuerpo de fracciones Σ. Existe un anillo de valoración discreta de Σ que domina a $\mathcal{O}$.*

Demostración. Sea $\mathcal{O}_v$ un anillo de valoración que domine a $\mathcal{O}$, $\mathfrak{m} = (a_1, \ldots, a_n)$ el ideal maximal de $\mathcal{O}$ y a_i tal que $v(a_i) \leq v(a_j)$, para todo j. Entonces, $A := \mathcal{O}[\frac{a_1}{a_i}, \ldots, \frac{a_n}{a_i}, a_i]$ está incluido en $\mathcal{O}_v$, $\mathfrak{m} \cdot A = (a_i)$ y localizando convenientemente A obtenemos un anillo local noetheriano $\mathcal{O}'$ de dimensión 1 que domina a $\mathcal{O}$. El cierre entero de $\mathcal{O}'$ en su cuerpo de fracciones es un anillo noetheriano de dimensión 1 normal, localizando convenientemente tenemos un anillo de valoración discreta que domina a $\mathcal{O}'$, luego a $\mathcal{O}$.

□

De nuevo, como en el teorema 5.3.6 , obtenemos el siguiente teorema.

10. Teorema: *Sea A un anillo noetheriano íntegro de cuerpo de fracciones Σ y $\bar{A}$ el cierre entero de A en Σ. Entonces, $\bar{A}$ es la intersección de todos los anillos de valoración discreta de Σ que contienen a A.*

11. Notación: Denotemos $\mathfrak{p}_{x,n}$ el ideal $\mathfrak{p}_x$-primario que al localizar en x es igual a $\mathfrak{p}_x^n$, es decir, "el ideal $\mathfrak{p}_x$-primario de todas las funciones cuyo desarrollo de Taylor hasta orden n en x es nulo".

12. Definición: Diremos que un ideal primo $\mathfrak{p}_x \subset A$ es de altura r si $\dim A_x = r$.

13. Teorema: *Si A es un anillo normal, entonces*

1. *Los ideales primos asociados de un ideal principal tienen altura 1.*

2. *La descomposición primaria reducida de cualquier ideal principal* (a)*, (distinto de* 0 *y* A*) es única y es igual a*

$$(a) = \mathfrak{p}_{x_1,n_1} \cap \cdots \cap \mathfrak{p}_{x_r,n_r},$$

con $\mathfrak{p}_{x_i}$ *de altura 1 y* $n_i = v_{x_i}(a)$ *(siendo* $A_{v_{x_i}} = A_{x_i}$*).*

3. $A = \bigcap_{alt.\,\mathfrak{p}_x=1} A_x$.

Demostración. 1. Sea $\mathfrak{p}$ un primo asociado a $(a) \subset A$. Podemos suponer que A es local de ideal maximal $\mathfrak{p} = \mathfrak{m}$. Sabemos que existe $b \in A$ tal que $(a : b) = \mathfrak{m}$. Por tanto $\frac{b}{a} \cdot \mathfrak{m} \subseteq A$. Si $\frac{b}{a} \cdot \mathfrak{m} \subseteq \mathfrak{m}$, entonces $\frac{b}{a}$ es entero sobre A, luego $\frac{b}{a} \in A$ y $(a : b) = A$, contradicción. Por tanto, $\frac{b}{a} \cdot \mathfrak{m} = A$ y $\mathfrak{m}$ es un A-módulo isomorfo a A, luego es un ideal principal y $\mathfrak{m}$ es de altura 1.

2. Sea $(a) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ una descomposición primaria reducida. Por 1. sabemos que los primos asociados, $\mathfrak{p}_{x_i}$, a los $\mathfrak{q}_i$ son de altura 1. En particular la descomposición primaria es única. Además, $(a)_{x_i} = \mathfrak{p}_{x_i}^{n_i} A_{x_i}$, porque A_{x_i} es un dominio de Dedekind local. Por tanto, $\mathfrak{q}_i = \mathfrak{p}_{x_i,n_i}$, además $v_{x_i}(a) = n_i$.

3. Escribamos $(a) = \mathfrak{p}_{x_1,n_1} \cap \cdots \cap \mathfrak{p}_{x_r,n_r}$ y $(b) = \mathfrak{p}_{x_1,m_1} \cap \cdots \cap \mathfrak{p}_{x_r,m_r}$, con $\mathfrak{p}_{x_i}$ de altura 1 y $n_i, m_i \geq 0$. Por tanto, $\frac{b}{a} \in A$ si y solo si si $m_i \geq n_i$, para todo i, que equivale a $\frac{b}{a} \in \bigcap_{\text{alt.}\,\mathfrak{p}_x=1} A_x$. □

14. Corolario: *Sea* A *un anillo noetheriano íntegro.* A *es un anillo normal si y solo si todo ideal principal (propio) es intersección, sin componentes sumergidas, de un número finito de primarios* $\mathfrak{p}_{x,n_x}$.

Demostración. Sólo nos falta probar el recíproco. Consideremos solo los ideales primos $\mathfrak{p}_x$ asociados a las descomposiciones primarias de los ideales principales. Repitiendo los argumentos del apartado 3. de la demostración anterior, tenemos que $A = \cap_x A_x$. Además, A_x es un anillo de valoración, pues dado $a \in A$ tal que $a \in \mathfrak{p}_x \cdot A_x$, $a \notin \mathfrak{p}_x^2 \cdot A_x$, tenemos que $(a)_x = \mathfrak{p}_x \cdot A_x$, luego A_x es un anillo de valoración. Por tanto, si $f \in A_{A \setminus \{0\}}$ es entero sobre A entonces es entero sobre todo A_x, luego $f \in A_x$ y $f \in \cap_x A_x = A$. □

15. Ejercicio: Sea A un subanillo de un cuerpo K y $\bar{k}$ un cuerpo algebraicamente cerrado. Si $f : A \to \bar{k}$ es un morfismo de anillos, entonces existe un subanillo $\mathcal{O}_v$ de valoración de K que contiene a A y un morfismo $f' : \mathcal{O}_v \to \bar{k}$, tal que ${f'}_{|A} = f$ y $\operatorname{Ker} f' = \mathfrak{p}_v$.

Resolución: Sea $A' \subset K$ un anillo local (no necesariamente de valoración) cumpliendo las propiedades exigidas a $\mathcal{O}_v$ y no dominado por ningún otro anillo local que cumpla las propiedades.

Pruébese que A' es íntegramente cerrado en su cuerpo de fracciones.

Sea $\xi \in K$. Si $\xi^{-1} \notin A'$, entonces no es entero sobre A'. Por el lema, $\xi A'[\xi] \neq A'[\xi]$. Por tanto, $\xi A'[\xi] \cap A'$ está incluido en el ideal maximal de A' y tenemos el diagrama conmutativo

$$\begin{array}{ccccccc} A' & \longrightarrow & A'[\xi] & \longrightarrow & A'[\xi]/\xi A'[\xi] & = & A'/(\xi A'[\xi] \cap A') \\ & \searrow^{f'} & & & & & \downarrow \\ & & & & & & \bar{k} \end{array}$$

Un localizado de $A'[\xi]$ cumplirá las propiedades exigidas a $\mathcal{O}_v$. Por la maximalidad de A' llegaremos a contradicción, salvo que $\xi \in A'$. En conclusión, A' es de valoración.

5.4. Variedad de Riemann

Sea K una k-extensión de cuerpos de tipo finito de grado de trascendencia 1, es decir, K es una $k(x)$-extensión finita de cuerpos. Sea C el conjunto de todos los anillos de valoración de K, triviales sobre k (es decir, que contienen a k). Dotemos a C de la siguiente estructura de espacio topológico: sus cerrados propios son los conjuntos finitos de anillos de valoración, distintos del anillo de valoración trivial.

Sea $U = \{v \in C : v(x) \geq 0\}$ y $V = \{v \in C : v(\frac{1}{x}) \geq 0\}$. Obviamente, $C = U \cup V$. Sea A el cierre entero de $k[x]$ en K. La asignación $\operatorname{Spec} A \to U$, $y \mapsto A_y$ es inyectiva, porque si $A_y = A_{y'}$ entonces $\mathfrak{p}_y = A \cap \mathfrak{p}_y A_y = A \cap \mathfrak{p}_{y'} A_{y'} = \mathfrak{p}_{y'}$. Veamos que la asignación es epiyectiva. Dado un anillo de valoración $\mathcal{O}_v$ de K, tal que $v(x) \geq 0$, entonces $k[x] \subseteq \mathcal{O}_v$ y tomando cierres enteros $A \subseteq \mathcal{O}_v$. Sea $\mathfrak{p}_y := \mathfrak{p}_v \cap A$. Localizando en y, obtenemos el morfismo dominante $A_y \subseteq \mathcal{O}_v$. Como A_y es un anillo de valoración, se cumple que $A_y = \mathcal{O}_v$. Igualmente, si A' es el cierre entero de $k[1/x]$ en K, se cumple que $\operatorname{Spec} A' = U'$. V es un abierto de C, ya que

$$C \setminus V = \{v \in C : v(1/x) < 0\} = \{v \in C : v(x) > 0\} = \operatorname{Spec} A/(x)$$

que es un número finito de puntos. Igualmente, U es un abierto de C. Además,

$$U \cap V = \{v \in U : v(x) = 0\} = \operatorname{Spec} A \setminus (x)_0 = \operatorname{Spec} A_x = \operatorname{Spec} A'_{1/x}$$

En conclusión, C se recubre por dos abiertos U, V, cada uno de ellos es una curva afín íntegra no singular, y $C \setminus U$ y $C \setminus V$ son conjuntos finitos.

1. Definición : Se dice que C es la variedad de Riemann asociada a K.

2. Todo morfismo $K \to K'$ de k-extensiones, entre extensiones de tipo finito de grado de trascendencia 1, induce un morfismo $\pi\colon C_{K'} \to C_K$ entre las variedades de Riemann asociadas, definido por $\mathscr{O}_{v'} \mapsto \mathscr{O}_v \cap K$. Dado $x \in K$ trascendente, sean A y A' el cierre entero de $k[x]$ en K y K' respectivamente, y $U := \operatorname{Spec} A$ y $U' = \operatorname{Spec} A'$. Entonces, el morfismo $\pi\colon U' \to U$ es el morfismo inducido por el morfismo de anillos natural $A \to A'$, que es un morfismo finito.

3. Sea $C' = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$ ($\operatorname{gr}\xi_i = 1$, para todo i) una curva proyectiva y supongamos que $k[\xi_0,\dots,\xi_n]$ es un anillo íntegro. Sea $\Sigma := k(\xi_1/\xi_0,\dots,\xi_n/\xi_0)$, "el cuerpo de funciones de C'" (que no depende de la ordenación de los ξ_i). Dado un punto $x \in U^h_{\xi_i} = \operatorname{Spec} k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, denotaremos $\mathscr{O}_{C',x} := k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]_x \subseteq \Sigma$ (que no depende del abierto $U^h_{\xi_i}$ que contiene a x, considerado).

Dado un anillo de valoración $\mathscr{O}_v$ de Σ, trivial sobre k, existe un único punto $x \in C'$, tal que $\mathscr{O}_v$ domina a $\mathscr{O}_{C',x}$: Sea ξ_j/ξ_i tal que $v(\xi_j/\xi_i)$ sea máximo entre todos los i,j. Observemos que $v(\xi_k/\xi_i) \geq 0$, porque si $v(\xi_k/\xi_i) < 0$, entonces $v(\xi_j/\xi_k) = v(\xi_i/\xi_k \cdot \xi_j/\xi_i) = v(\xi_i/\xi_k) + v(\xi_i/\xi_j) > v(\xi_i/\xi_j)$, lo cual es contradictorio. Por tanto, $k[\xi_0/\xi_i,\dots,\xi_n/\xi_i] \subset \mathscr{O}_v$. Si $\mathfrak{p}_x := \mathfrak{p}_v \cap k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, tenemos que $\mathscr{O}_v$ domina a $\mathscr{O}_{C',x}$. Sea otro $x' \in C'$ tal que $\mathscr{O}_v$ domina a $\mathscr{O}_{C',x'}$. Sea k tal que $x' \in U^h_{\xi_k}$. Si $x' \notin U^h_{\xi_i}$, entonces $\xi_i/\xi_k \in \mathfrak{p}_{x'}\mathscr{O}_{C',x'}$, luego $v(\xi_i/\xi_k) > 0$ y $v(\xi_j/\xi_k) = v(\xi_i/\xi_k \cdot \xi_j/\xi_i) = v(\xi_i/\xi_k) + v(\xi_j/\xi_i) > v(\xi_j/\xi_i)$, lo cual es contradictorio. Entonces, $x' \in U^h_{\xi_i}$ y $\mathfrak{p}_{x'} := \mathfrak{p}_v \cap k[\xi_0/\xi_i,\dots,\xi_n/\xi_i] = \mathfrak{p}_x$ y $x' = x$.

Sea C la variedad de Riemann de Σ. Consideremos el morfismo natural $\pi\colon C \to C'$, donde $\pi(v)$ es tal que $\mathscr{O}_v$ domina a $\mathscr{O}_{C',\pi(v)}$. Consideramos el abierto

$$U^h_{\xi_0} = \operatorname{Spec} k[\xi_1/\xi_0,\dots,\xi_n/\xi_0]$$

y un morfismo finito $k[x] \hookrightarrow k[\xi_1/\xi_0,\dots,\xi_n/\xi_0]$. Sea A el cierre entero de $k[x]$ en Σ (que es el cierre entero de $k[\xi_1/\xi_0,\dots,\xi_n/\xi_0]$ en Σ) y $U = \operatorname{Spec} A$. El morfismo inducido por la inclusión $k[\xi_1/\xi_0,\dots,\xi_n/\xi_0] \hookrightarrow A$ es el morfismo $\pi\colon U \to U^h_{\xi_0}$.

Se dice que C es la desingularización de C'. Si C' es una curva proyectiva no singular en todo punto, entonces $C = C'$. Se puede probar el recíproco: las variedades de Riemann son curvas proyectivas no singulares en todo punto.

La variedad de Riemann asociada a $k(x)$ es la recta proyectiva $\mathbb{P}^1$.

4. Sea C la variedad de Riemann asociada a K y $f \in K$ trascendente. Consideremos la inclusión $k(f) \hookrightarrow K$ y el morfismo inducido $f\colon C \to \mathbb{P}^1$ entre las variedades de Riemann. Sea A el cierre entero de $k[f]$ y A' el cierre entero de $k[1/f]$. Tenemos los morfismos $k[x] \to A$, $x \mapsto f$ y $k[1/x] \to A'$, $1/x \mapsto 1/f$, que inducen en espectros los morfismos $U = \operatorname{Spec} A \to \operatorname{Spec} k[x]$, $p \mapsto f(p)$ y $V = \operatorname{Spec} A' \to \operatorname{Spec} k[1/x]$, $p' \mapsto 1/f(p')$, que coinciden sobre las intersecciones y define el morfismo $f\colon C \to \mathbb{P}^1$ de partida.

Recordemos que el número de puntos de las fibras (contando grados y multiplicidades) es constante. Veamos el número de puntos de la fibra del $0 \in \operatorname{Spec} k[x] \subset \mathbb{P}^1$ ($\mathfrak{p}_0 = (x)$): La x en A es f, $(f) = \mathfrak{m}_{x_1}^{e_1} \cdots \mathfrak{m}_{x_n}^{e_n}$, donde $\{x_1, \ldots, x_n\}$ son los puntos de la fibra de 0 y $e_i = v_{x_i}(f)$ (y $v_x(f) = 0$, para todo $x \in U$ distinto de los x_i). Por tanto,

$$\text{Nº de puntos de la fibra del } 0 = \dim_k A/(f) = \sum_{x \in C, v_x(f) \geq 0} v_x(f) \cdot \operatorname{gr}_k x,$$

número que se denomina *número de ceros de* f. Igualmente, el número de puntos de la fibra del $\infty \in \operatorname{Spec} k[1/x] \subset \mathbb{P}^1$ ($\mathfrak{p}_\infty = (1/x)$) es

$$\text{Nº de puntos de la fibra del } \infty = \dim_k A'/(1/f) = \sum_{x \in C, v_x(1/f) \geq 0} v_x(1/f) \cdot \operatorname{gr}_k x,$$

número que se denomina *número de polos de* f. Por tanto,

$$0 = \text{Nº de puntos de la fibra del } 0 \; - \; \text{nº de puntos de la fibra del } \infty = \sum_{x \in C} v_x(f) \cdot \operatorname{gr}_k x.$$

5. Teorema: *Sea K una extensión de tipo finito de k de grado de trascendencia 1, C la variedad de Riemann asociada a K y $f \in K$. Entonces,*

$$\boxed{\textstyle\sum_{x \in C} v_x(f) \cdot \operatorname{gr}_k x = 0},$$

es decir, el número de ceros de f es igual a su número de polos.

5.5. Explosión a lo largo de un cerrado. Desingularización

1. Definiciones: Sea A un anillo e $I \subseteq A$ un ideal. Se llama dilatado de A por I, o anillo de Rees de A en I, al anillo graduado

$$D_I A = A \oplus I \oplus I^2 \oplus \cdots \oplus I^n \oplus \cdots$$

El morfismo natural $\widetilde{X} = \operatorname{Proj} D_I A \to X = \operatorname{Spec} A$, $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ se denomina morfismo de explosión centrado en $(I)_0$. Si I es maximal, también se denomina transformación cuadrática. Se dice que $\widetilde{X}$ es la explosión de X a lo largo de $(I)_0$.

Si $X' = \operatorname{Spec} A/J \hookrightarrow \operatorname{Spec} A = X$ es un cerrado, la explosión $\widetilde{X}'$, de X' a lo largo de $X' \cap (I)_0$ se denomina la transformada propia de X' por el morfismo de explosión $\tilde{X} \to X$. Observemos que $\widetilde{X}' = \operatorname{Proj} D_{\bar{I}}(A/J)$ es un cerrado de $\widetilde{X}$.

2. Proposición: *Sea $X = \operatorname{Spec} A$ y $\pi\colon \widetilde{X} \to X$ el morfismo de explosión en un punto cerrado x. Se cumple que*

1. $\pi^{-1}(X\setminus x) \overset{\pi}{=} X\setminus x$.
2. $\pi^{-1}(x) = T_x X$. *"La fibra de x es igual al espacio tangente de X en x".*

Demostración. 1. Sea $\mathfrak{m}$ el maximal correspondiente a x. Consideremos el morfismo $A \to D_{\mathfrak{m}}A$. Dado $\xi \in \mathfrak{m}$, tenemos que

$$\begin{aligned}\pi^{-1}(U_\xi) &= \operatorname{Proj}(A \oplus \mathfrak{m} \oplus \cdots)_\xi = \operatorname{Proj}(A_\xi \oplus \mathfrak{m}_\xi \oplus \cdots)\\ &= \operatorname{Proj}(A_\xi \oplus A_\xi \oplus \cdots) = \operatorname{Proj} A_\xi[t] = \operatorname{Spec} A_\xi = U_\xi\end{aligned}$$

Recubriendo $X\setminus x$ por abiertos del tipo U_ξ obtenemos el punto 1.

2. Por ser x cerrado

$$\pi^{-1}(x) = \operatorname{Proj}[(D_{\mathfrak{m}}A) \otimes_A A/\mathfrak{m}] = \operatorname{Proj} G_{\mathfrak{m}}A = T_x X.$$

□

3. Observación: En la proposición anterior, dado $y \in \operatorname{Spec} A$ distinto de x, $\pi^{-1}(y)$ se corresponde con el punto de $\operatorname{Proj} D_{\mathfrak{m}}A$ de ideal $\mathfrak{p}_y \oplus (\mathfrak{p}_y \cap \mathfrak{m}) \oplus (\mathfrak{p}_y \cap \mathfrak{m}^2) \oplus \cdots$, pues éste es un ideal primo homogéneo cuya imagen por π es y.

Con la misma demostración, tenemos la siguiente proposición.

4. Proposición: *Sea $X = \operatorname{Spec} A$, $I \subset A$ un ideal, y $\pi\colon \widetilde{X} \to X$ el morfismo de explosión de X centrado en $Y = (I)_0$. Se verifica*

1. $\pi^{-1}(X\setminus Y) \overset{\pi}{=} X\setminus Y$.
2. $\pi^{-1}(Y) = \operatorname{Proj} G_I A$. *"La fibra de Y es igual al espacio normal a Y en X".*

Sea $I = (\xi_1, \ldots, \xi_n)$. Dado $\xi \in I$ denotemoslo $\tilde{\xi}$ cuando lo pensemos como el elemento de grado 1 de $D_I A$. $D_I A$ es un álgebra graduada generada por sus elementos de grado uno, pues se tiene un epimorfismo graduado

$$\begin{aligned}A[x_1, \ldots, x_n] &\to D_I A\\ x_i &\mapsto \tilde{\xi}_i\end{aligned}$$

Entonces, $D_I A = A[\tilde{\xi}_1, \ldots, \tilde{\xi}_n]$. Sabemos que $\operatorname{Proj} D_I A \setminus (\tilde{\xi})_0^h = \operatorname{Spec} A[\frac{\tilde{\xi}_1}{\tilde{\xi}}, \ldots, \frac{\tilde{\xi}_n}{\tilde{\xi}}]$. Además $A[\frac{\tilde{\xi}_1}{\tilde{\xi}}, \ldots, \frac{\tilde{\xi}_n}{\tilde{\xi}}]$ es isomorfo, con el isomorfismo obvio, al subanillo $A[\frac{\xi_1}{\xi}, \ldots, \frac{\xi_n}{\xi}]$ de A_ξ.

5. Ejercicio: Prueba que $\operatorname{Proj} D_I A = \operatorname{Proj} D_{I^n} A$ para todo $n \in \mathbb{N}$ (Pista: Consideremos la inclusión natural $D_{I^n}A \subset D_I A$ que multiplica los grados por n. Dado $\xi \in I$, pruébese las igualdades

$$\operatorname{Proj} D_I A \setminus (\tilde{\xi})_0^h = \operatorname{Spec}[(D_I A)_{\tilde{\xi}}]_0 = \operatorname{Spec}[(D_I A)_{\tilde{\xi}^n}]_0 = \operatorname{Spec}[(D_{I^n} A)_{\tilde{\xi}^n}]_0 = \operatorname{Proj} D_{I^n} A \setminus (\tilde{\xi}^n)_0^h.$$

donde $[\quad]_0$ denota tomar la componente de grado cero.)

6. Ejercicio: Sea $x \in \mathbb{A}^n$ el "origen" y $\pi \colon \widetilde{\mathbb{A}}^n \to \mathbb{A}^n$ la explosión en x. Prueba que

1. $\pi^{-1}(\mathbb{A}^n \setminus x) \overset{\pi}{=} \mathbb{A}^n \setminus x$.
2. $\pi^{-1}(x) = \mathbb{P}^{n-1}$. "La fibra de x es igual a la proyectivización del cono tangente de $\mathbb{A}^n$ en x, que coincide con el conjunto de direcciones en x".

Se dice que $\pi^{-1}(x)$ es el ciclo excepcional. Dado $X = \operatorname{Spec} A$, denotemos $\mathcal{O}_X = A$. Sea $C \overset{i}{\hookrightarrow} \mathbb{A}^n$ una subvariedad que pasa por el origen. Se tiene un epimorfismo natural $D_{\mathfrak{m}}\mathcal{O}_{\mathbb{A}^n} \to D_{\bar{\mathfrak{m}}}\mathcal{O}_C$, siendo $\mathfrak{m}, \bar{\mathfrak{m}}$ los maximales de $\mathcal{O}_{\mathbb{A}^n}$ y $\mathcal{O}_C$ correspondientes al origen. Se tiene entonces un diagrama conmutativo

$$\begin{array}{ccc} \widetilde{C} & \overset{\tilde{i}}{\hookrightarrow} & \widetilde{\mathbb{A}}^n \\ \downarrow \pi_C & & \downarrow \pi \\ C & \overset{i}{\hookrightarrow} & \mathbb{A}^n \end{array}$$

Prueba que si C es una recta, que pasa por el origen, entonces $\widetilde{C} \overset{\pi}{=} C$. Diremos que $\tilde{i}(\pi_C^{-1}(x))$ es la dirección definida por la recta C en x. Prueba que si $n = 2$ y C es la curva nodal $y^2 - x^2 + x^3 = 0$, entonces $\tilde{i}(\pi_C^{-1}(x))$ se identifica con las dos direcciones definidas por las tangentes de C en x.

7. Teorema: *Sea A un anillo semilocal (i.e., con un número finito de puntos cerrados), noetheriano, íntegro y de dimensión 1. Sea $\mathfrak{m}$ un ideal maximal, y supongamos que $A/\mathfrak{m}$ tiene infinitos elementos. Existe un anillo A_1 y un morfismo de anillos $A \to A_1$ tal que*

$$\operatorname{Proj} D_{\mathfrak{m}} A = \operatorname{Spec} A_1$$

y el morfismo $\operatorname{Spec} A_1 \to \operatorname{Spec} A$ es el morfismo de explosión.

Demostración. Escribamos $\mathfrak{m} = (\xi_1, \ldots, \xi_n)$. Consideremos el isomorfismo graduado

$$D_{\mathfrak{m}} A = A[\tilde{\xi}_1, \ldots, \tilde{\xi}_n]$$

Dado $\xi \in \mathfrak{m}$, $\operatorname{Proj} D_{\mathfrak{m}} A \setminus (\tilde{\xi})_0^h = U_{\tilde{\xi}}^h = \operatorname{Spec} A[\tilde{\xi}_1/\tilde{\xi}, \ldots, \tilde{\xi}_n/\tilde{\xi}] = \operatorname{Spec} A[\xi_1/\xi, \ldots, \xi_n/\xi]$. Para demostrar el teorema, basta encontrar $\xi \in \mathfrak{m}$ tal que $(\tilde{\xi})_0^h = \emptyset$, es decir $\tilde{\xi}$ no se anula en ningún punto cerrado de $\operatorname{Proj} D_{\mathfrak{m}} A$. Por la proposición 5.5.2 (y observación) buscamos $\xi \in \mathfrak{m}$ tal que

1. $\tilde{\xi}$ no se anule en ningún punto cerrado de $\operatorname{Proj} D_{\mathfrak{m}}A \setminus \pi^{-1}(x) = \operatorname{Spec} A \setminus x$, siendo x el punto definido de ideal $\mathfrak{m}$. Es decir, si denotamos por $y_1, \ldots, y_r$ los puntos cerrados de $\operatorname{Spec} A$ distintos de x, buscamos $\xi \notin \mathfrak{m} \cap \mathfrak{m}_{y_i}$ para todo i. Geométricamente, buscamos un parámetro que se anule en x y no en los y_i.

2. $\tilde{\xi}$ no se anule en ningún punto cerrado de $\pi^{-1}(x) = \operatorname{Proj} G_{\mathfrak{m}}A$. Ahora bien, $G_{\mathfrak{m}}A$ es un anillo que en el vértice tiene la misma dimensión que A en x, que es 1. Por tanto, como los ideales primos homogéneos de $G_{\mathfrak{m}}A$ están incluidos estrictamente en el ideal de funciones que se anulan en el vértice (ideal irrelevante), son ideales minimales, luego un número finito. En conclusión, si denotamos $\mathfrak{p}_i$ dichos ideales primos homogéneos y $\mathfrak{p}_{i,1}$ su componente homogénea de grado 1, buscamos $\xi \in \mathfrak{m}$ de modo que $\bar{\xi} \notin \mathfrak{p}_{i,1} \underset{\neq}{\subset} \mathfrak{m}/\mathfrak{m}^2$. Geométricamente, buscamos un parámetro que pasa por x transversalmente.

Sea $\bar{e} \in \mathfrak{m}/\mathfrak{m}^2 \subset A/\mathfrak{m}^2$ tal que $\bar{e} \notin \mathfrak{p}_{i,1}$ para todo i (existe porque la unión de los subespacios propios $\mathfrak{p}_{i,1}$ no puede ser todo $\mathfrak{m}/\mathfrak{m}^2$, ya que $A/\mathfrak{m}$ tiene infinitos elementos). Consideremos ahora el morfismo natural

$$\phi\colon A \to A/\mathfrak{m}^2 \times A/\mathfrak{m}_{y_1} \times \cdots \times A/\mathfrak{m}_{y_n}$$

que es epimorfismo, como se comprueba localmente. Si $\xi \in \mathfrak{m}$ es tal que $\phi(\xi) = (\bar{e}, 1, \ldots, 1)$, entonces es el parámetro buscado.

□

8. Observaciones: 1. El anillo $A_1 = A[\xi_1/\xi, \ldots, \xi_n/\xi]$ del teorema no depende de la elección del parámetro ξ. Si ξ' es otro parámetro tal que $(\tilde{\xi}')_0^h = \emptyset$ en $\operatorname{Proj} D_{\mathfrak{m}}A$, entonces $(\xi'/\xi)_0 = \emptyset$ en $\operatorname{Spec} A[\xi_1/\xi, \ldots, \xi_n/\xi]$, luego ξ'/ξ es invertible y $A[\xi_1/\xi', \ldots, \xi_n/\xi'] \subseteq A[\xi_1/\xi, \ldots, \xi_n/\xi]_{\xi'/\xi} = A[\xi_1/\xi, \ldots, \xi_n/\xi]$. Por simetría tenemos la inclusión inversa, con lo que concluimos la igualdad.

2. El ideal $\mathfrak{m}A_1$ es principal. En efecto: $\mathfrak{m}A_1 = (\xi_1, \ldots, \xi_n) \cdot A[\xi_1/\xi, \ldots, \xi_n/\xi] = \xi A_1$.

9. Nota para la Teoría de Números: *El teorema es igualmente válido sin la hipótesis de que* $A/\mathfrak{m}$ *tenga infinitos elementos. Ahora bien, la* ξ *escogida será* $\tilde{\xi} \in \mathfrak{m}^m \subset D_{\mathfrak{m}}A$*, con* $m >> 0$*, tal que* $\bar{\xi} \notin \mathfrak{p}_{i,m}$ *para todo* i*, y no pase por los demás puntos cerrados de* $\operatorname{Spec} A$*. Observemos que* $\operatorname{Proj} D_{\mathfrak{m}}A \setminus (\tilde{\xi})_0^h = \operatorname{Proj} D_{\mathfrak{m}^m}A \setminus (\tilde{\xi})_0^h = \operatorname{Spec}[(D_{\mathfrak{m}^m}A)_{\tilde{\xi}}]_0$*. Así pues,* $A_1 = A[\frac{\xi_1^{m_1} \cdots \xi_n^{m_n}}{\xi}]_{m_1+\cdots+m_n=m}$*.* A_1 *tampoco depende de la elección del parámetro* ξ*. Como* $\operatorname{Spec} A_1 = \operatorname{Proj} D_{\mathfrak{m}}A$*, entonces*

$$U_{\frac{\xi_i^m}{\xi}} = U_{\tilde{\xi}_i}^h = \operatorname{Spec} A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]$$

y es fácil demostrar que $(A_1)_{\frac{\xi^m_i}{\xi}} = A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]$. *Además,* $\mathfrak{m}A_1$ *es localmente principal.*

10. Definición: El anillo A_1 del teorema anterior se llama anillo de la transformación cuadrática o anillo de la explosión (en x).

11. Lema: *Con las notaciones e hipótesis del teorema anterior, se cumple que* $A = A_1 \Leftrightarrow$ *el punto cerrado* x *en el que estamos explotando es no singular.*

Demostración. $\Rightarrow$) $\mathfrak{m} = \mathfrak{m}A_1$, el cual es localmente principal, luego x es no singular.

$\Leftarrow$) En el complementario de x, A y A_1 son isomorfos. Localizando en x, $\mathfrak{m}_x = (\xi)$ y $\operatorname{Proj} D_{\mathfrak{m}_x} A = U^h_{\tilde{\xi}} = \operatorname{Spec} A[\xi/\xi] = \operatorname{Spec} A$, luego $A_1 = A$. □

12. Lema: *Si* $\mathcal{O}_v$ *es un anillo de valoración que contiene a* A, *entonces* $A_1 \subseteq \mathcal{O}_v$. *Por tanto, el morfismo* $A \to A_1$ *es finito.*

Demostración. Escribamos $\mathfrak{m} = (\xi_1, \ldots, \xi_n)$ y $D_{\mathfrak{m}}A = A[\tilde{\xi}_1, \ldots, \tilde{\xi}_n]$. Entonces,

$$\operatorname{Proj} D_{\mathfrak{m}} A = \bigcup_i \operatorname{Spec} A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i].$$

Sea $\xi \in \mathfrak{m}$ de modo que $\operatorname{Proj} D_{\mathfrak{m}}A = \operatorname{Spec} A[\xi_1/\xi, \ldots, \xi_n/\xi]$, es decir, $A_1 = A[\xi_1/\xi, \ldots, \xi_n/\xi]$. Como ξ/ξ_i es invertible en $A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]$ (pues sus ceros son el vacío), se deduce que

$$A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i] = A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]_{\xi/\xi_i} = A[\xi_1/\xi, \ldots, \xi_n/\xi]_{\xi_i/\xi} = A_{1\,\xi_i/\xi}$$

Así pues, si $\mathcal{O}_v$ contiene a algún $A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]$ contiene a A_1.

Sea ξ_j/ξ_i tal que $v(\xi_j/\xi_i)$ sea máximo entre todos los i, j. Entonces $v(\xi_k/\xi_i) \geq 0$ para todo k: en efecto, si $v(\xi_k/\xi_i) < 0$, entonces $v(\xi_i/\xi_k) > 0$, luego $v(\xi_j/\xi_i) < v(\xi_j/\xi_i) + v(\xi_i/\xi_k) = v(\xi_j/\xi_i \cdot \xi_i/\xi_k) = v(\xi_j/\xi_k)$, lo que es contradictorio.

Por tanto, $A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i] \subseteq \mathcal{O}_v$ y hemos terminado. □

13. Teorema: *Sea* A *un anillo semilocal, noetheriano, íntegro, de dimensión 1. Si el cierre entero de* A *en su cuerpo de fracciones es un* A*-módulo finito generado, entonces dicho cierre entero se alcanza por un número finito de explosiones en puntos cerrados.*

Demostración. Si A no es regular, sea x un punto singular. Por el lema 5.5.11, A está incluido estrictamente en A_1= anillo de explosión en x. Por el lema 5.5.12, A_1 está incluido en el cierre entero $\bar{A}$ de A en su cuerpo de fracciones. Así pues, tenemos $A \underset{\neq}{\subseteq} A_1 \subseteq \bar{A}$.

Procediendo del mismo modo con A_1, tendremos $A \subsetneq A_1 \subsetneq A_2 \subseteq \bar{A}$. Como $\bar{A}$ es un A-módulo finito generado y A es noetheriano, este proceso es finito y terminará cuando $A_n = \bar{A}$.

□

14. Definición: La fibra por el morfismo de explosión del punto en el que se explota se denomina fibra excepcional. En las condiciones y notaciones del teorema anterior, si consideramos la cadena

$$\operatorname{Spec}\bar{A} = \operatorname{Spec}A_n \xrightarrow[\pi_n]{} \operatorname{Spec}A_{n-1} \xrightarrow[\pi_{n-1}]{} \cdots \longrightarrow \operatorname{Spec}A_1 \xrightarrow[\pi_1]{} \operatorname{Spec}A,$$

la cadena correspondiente de fibras excepcionales es un orden finito arbolado que se conoce como árbol de explosión de A.

5.6. Multiplicidad de un punto singular

1. Definición: Se llama multiplicidad de un anillo local noetheriano $\mathcal{O}$ de dimensión r, al coeficiente de mayor grado de su polinomio de Samuel multiplicado por $r!$. Lo denotaremos $m(\mathcal{O})$. En definitiva, $m(\mathcal{O}) = \Delta^r S_{\mathcal{O}}(n)$. Si x es un punto de $X = \operatorname{Spec}A$, llamaremos multiplicidad de X en x, que denotaremos $m_x(X)$, a la multiplicidad del anillo de gérmenes de funciones de X en el punto x, es decir, $m_x(X) := m(A_x)$.

2. Ejemplo: Sea A un anillo noetheriano de dimensión de Krull cero y $x \in X = \operatorname{Spec}A$ un punto (cerrado). Entonces, $m_x(X) = l_A(A_x)$, pues $S_{A_x}(n) = l_{A_x}(A_x)$, para $n >> 0$.

3. Ejemplo: Los anillos locales regulares son de multiplicidad 1: Si $\mathcal{O}$ es un anillo local regular de ideal maximal $\mathfrak{m}$, entonces $G_{\mathfrak{m}}\mathcal{O} = \mathcal{O}/\mathfrak{m}[x_1,\ldots,x_r]$ y el polinomio de Samuel es $S_{\mathcal{O}}(n) = \binom{n+r-1}{r} = \frac{1}{r!}n^r + \ldots$. Por tanto, $m(\mathcal{O}) = \frac{1}{r!}\cdot r! = 1$.

4. Ejemplo: Sea X una hipersuperficie del espacio afín $\mathbb{A}^m$ definida por los ceros del polinomio p, que escribimos como suma de polinomios homogéneos, $p(x_1,\ldots,x_m) = p_r(x_1,\ldots,x_m) + \cdots + p_s(x_1,\ldots,x_m)$. Denotemos $A = k[x_1,\ldots,x_m]$, $\mathfrak{m} = (x_1,\ldots,x_m)$, $\mathcal{O}_X = A/(p)$ y $\bar{\mathfrak{m}}$ la imagen de $\mathfrak{m}$ en $\mathcal{O}_X$. Por la proposición 4.2.5, la sucesión

$$0 \to G_{\mathfrak{m}}A \xrightarrow{\cdot p_r} G_{\mathfrak{m}}A \longrightarrow G_{\bar{\mathfrak{m}}}\mathcal{O}_X \to 0$$

es exacta. Por tanto, el polinomio de Samuel de X en el origen es

$$S_{\mathcal{O}_{X,0}}(n) = \binom{m+n-1}{m} - \binom{m+n-1-r}{m} = \frac{r}{(m-1)!}n^{m-1} + \cdots$$

Luego la multiplicidad de X en el origen es igual r. En el caso particular de que X sea una curva plana, se obtiene

$$S_{\mathcal{O}_{X,0}}(n) = r \cdot n - \frac{r(r-1)}{2}$$

siendo r la multiplicidad de X en el origen.

Sea, ahora, $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Sea $f \in \mathcal{O}$ tal que $f \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}$ y supongamos que $f_r = \bar{f} \in \mathfrak{m}^r/\mathfrak{m}^{r+1}$ no es divisor de cero en $G_{\mathfrak{m}}\mathcal{O}$. Se cumple que $m(\mathcal{O}/(f)) = r \cdot m(\mathcal{O})$. En efecto, consideremos la sucesión exacta

$$0 \to G_{\mathfrak{m}}\mathcal{O} \xrightarrow{\cdot f_r} G_{\mathfrak{m}}\mathcal{O} \longrightarrow G_{\bar{\mathfrak{m}}}(\mathcal{O}/(f)) \to 0$$

Por tanto, $S_{\mathcal{O}/(f)}(n) = S_{\mathcal{O}}(n) - S_{\mathcal{O}}(n-r)$ y se concluye con un sencillo cálculo.

Sea $X \subset \mathbb{A}^n$ una variedad algebraica irreducible (por sencillez) de dimensión r y $x \in X$ un punto racional. Supongamos que existe una sucesión de hiperplanos $\{H_1, \ldots, H_r\}$ tal que: H_1 es un hiperplano transversal a X en x, H_2 es un plano transversal a $X \cap H_1$ en x y no pasa por ninguna componente irreducible de $X \cap H_1$; y así sucesivamente. Obtendremos una variedad $Y = X \cap H_1 \cap \cdots \cap H_r$ de dimensión cero, en la que la multiplicidad de Y en x es igual a $m_x(X)$.

5. Lema de estabilidad del ideal: *Sean A, $\mathfrak{m}$, A_1 como en el teorema 5.5.7, y $A \to A_1$ el morfismo de explosión. Para todo $s >> 0$ se cumple que $\mathfrak{m}^s = \mathfrak{m}^s \cdot A_1$.*[1]

Demostración. Sea $\mathfrak{m} = (\xi_1, \ldots, \xi_n)$ y $\xi \in \mathfrak{m}$ tal que $A_1 = A[\xi_1/\xi, \ldots, \xi_n/\xi]$. Un sistema generador de A_1 como A-módulo lo forman los elementos de la forma $\frac{\xi_1^{\alpha_1} \ldots \xi_n^{\alpha_n}}{\xi^{\alpha_1+\cdots+\alpha_n}}$. Cada uno de ellos satisface que $\xi^s \cdot \frac{\xi_1^{\alpha_1} \ldots \xi_n^{\alpha_n}}{\xi^{\alpha_1+\cdots+\alpha_n}} \in \mathfrak{m}^s$ para $s \geq \alpha_1 + \cdots + \alpha_n$. Como A_1 es un A-módulo finito generado, un número finito de ellos generan, luego $\mathfrak{m}^s \cdot A_1 = \xi^s A_1 \subseteq \mathfrak{m}^s$, para s bastante grande. □

6. Observación: Si A es el anillo local de una curva plana en un punto racional, puede tomarse s igual a la multiplicidad de A menos uno (véase).

7. Teorema: *Sean A, $\mathfrak{m}_x$ y A_1 como en el teorema 5.5.7. La multiplicidad de A en x, es igual al número de puntos de la fibra excepcional (contando multiplicidades y grados sobre x). El coeficiente de grado cero del polinomio de Samuel de A es igual a $-l_A(A_1/A)$.* [2]

[1] **Nota para la Teoría de Números:** Si $\#(A/\mathfrak{m}) < \infty$ el lema de estabilidad es igualmente cierto, sin más que sustituir en la demostración $\mathfrak{m}$ por $\mathfrak{m}^m$, donde m es el número natural que aparece en la nota anterior.

[2] **Nota para la Teoría de Números:** Si $\#(A/\mathfrak{m}) < \infty$ el teorema es igualmente cierto, sin más que sustituir en la demostración $\mathfrak{m}^n$ por $\mathfrak{m}^{mn}$, donde m es el número natural que aparece en la nota anterior.

Demostración. Por el lema de estabilidad para $n >> 0$ se tiene la sucesión exacta

$$0 \to A/\mathfrak{m}_x^n \to A_1/\mathfrak{m}_x^n A_1 \to A_1/A \to 0$$

Tomando longitudes, $S_{A_x}(n) = l_A(A_1/\mathfrak{m}_x^n A_1) - l_A(A_1/A) = l_A(A_1/\mathfrak{m}_x A_1)n - l_A(A_1/A)$, porque $\mathfrak{m}_x A_1$ es principal. Luego, $m(A_x) = l_A(A_1/\mathfrak{m}_x A_1) = \dim_{A/\mathfrak{m}_x A}(A_1/\mathfrak{m}_x A_1)$ y $S_{A_x}(0) = -l_A(A_1/A)$. □

8. Corolario: *Sean A, $\mathfrak{m}_x$ como en el teorema 5.5.7. La multiplicidad de A en x, es igual al número de puntos (contando grados y multiplicidades) que aparecen en la fibra de x en el morfismo de desingularización.*[3]

Demostración. Sea A_1 el anillo de la explosión de A en x y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. Sólo tenemos que probar, por el teorema anterior, que $l_A(A_1/\mathfrak{m}_x A_1) = l_A(\bar{A}/\mathfrak{m}_x \bar{A})$, lo cual es cierto porque $\mathfrak{m}_x A_1$ es localmente principal (y arguméntese como en 5.3.7). □

9. Corolario: *Sea A como en el teorema 5.5.7. Sea $\bar{A}$ su cierre entero en su cuerpo de fracciones. Supongamos que $\bar{A}$ es finito sobre A. Sea $A \to A_1 \to \cdots \to A_n = \bar{A}$, la cadena de las sucesivas explosiones; digamos que A_{i+1} es la explosión de A_i en y_i. Entonces,*

$$l_A(\bar{A}/A) = -\sum_{y_i \in \acute{a}rb.expl.} S_{A_{i,y_i}}(0) \cdot \dim_{A/\mathfrak{m}_x}(A_{i,y_i}/\mathfrak{m}_{y_i})$$

Demostración. Por la aditividad de la longitud, $l_A(\bar{A}/A) = \sum_i l_A(A_{i+1}/A_i)$. Por tanto,

$$\begin{aligned} l_A(\bar{A}/A) &= \sum_i l_A(A_{i+1}/A_i) = \sum_i l_{A_i}(A_{i+1}/A_i) \cdot \dim_{A/\mathfrak{m}_x}(A_{i,y_i}/\mathfrak{m}_{y_i}) \\ &= -\sum_{y_i \in \text{árb.expl.}} S_{A_{i,y_i}}(0) \cdot \dim_{A/\mathfrak{m}_x}(A_{i,y_i}/\mathfrak{m}_{y_i}) \end{aligned}$$

donde la última igualdad es consecuencia del teorema anterior. □

10. Corolario: *Si A es el anillo local de una curva plana sobre un cuerpo algebraicamente cerrado, entonces*

$$l_A(\bar{A}/A) = \sum_{y \in \acute{a}rb.expl.} \frac{m_y(m_y - 1)}{2}$$

donde denotamos por m_y la multiplicidad del punto y.

[3] **Nota para la Teoría de Números:** Si $\#(A/\mathfrak{m}) < \infty$ el corolario es igualmene cierto.

Demostración. Los anillos locales de los puntos del árbol de explosión de A son anillos locales de curvas planas. Se concluye por el corolario anterior, y por el cálculo del ejemplo anterior.

□

5.7. Multiplicidad de intersección de una curva con una hipersuperficie

Dado $X = \operatorname{Spec} A$ denotaremos $\mathcal{O}_X = A$.

1. Definición: Sea X una curva de un espacio afín $\mathbb{A}^m$ y $H = (p(x_1,\dots,x_m))_0$ una hipersuperficie que no pasa por ninguna componente de X. Entonces $X \cap H$ es un número finito de puntos. Se llama multiplicidad de intersección de X con H en un punto $x \in X$ al número

$$(X \cap H)_x := l(\mathcal{O}_{X\cap H,x})$$

que coincide con la multiplicidad de $X \cap H$ en x.

Obsérvese que $\dim_k \mathcal{O}_{X\cap H,x} = (X \cap H)_x \cdot \dim_k \mathcal{O}_X/\mathfrak{m}_x$, porque los factores de toda serie de composición de $\mathcal{O}_{X\cap H,x}$ como $\mathcal{O}_{X\cap H,x}$-módulo son isomorfos a $\mathcal{O}_X/\mathfrak{m}_x$, luego la dimensión de $\mathcal{O}_{X\cap H,x}$ es igual a su longitud multiplicada por $\dim_k \mathcal{O}_X/\mathfrak{m}_x$. Denotemos $\operatorname{gr} x = \dim_k \mathcal{O}_X/\mathfrak{m}_x$. Si $\mathfrak{m}_x$ es racional entonces $\dim_k \mathcal{O}_{X\cap H,x} = (X \cap H)_x$.

Llamaremos número de puntos de corte de C con H, contando multiplicidades y grados, al número

$$(C \cap H) := \dim_k \mathcal{O}_{X\cap H}$$

Por definición

$$(C \cap H) = \dim_k \mathcal{O}_{X\cap H} = \sum_{x_i \in C\cap H} \dim_k \mathcal{O}_{C\cap H,x_i} = \sum_{x_i \in C\cap H} (C \cap H)_{x_i} \cdot \operatorname{gr} x_i$$

2. Notación: Supondremos, a partir de ahora en esta sección, las k-variedades algebraicas sobre un cuerpo k algebraicamente cerrado.

3. Teorema: *Sean C una curva íntegra y H una hipersuperficie de un espacio afín $\mathbb{A}^n$. Sean $\widetilde{C} \hookrightarrow \widetilde{\mathbb{A}}^n$, $\widetilde{H} \hookrightarrow \widetilde{\mathbb{A}}^n$ las explosiones respectivas en un punto cerrado $x \in C \cap H$ y sean $\{y_1,\dots,y_r\}$ los puntos de $\widetilde{C} \cap \widetilde{H}$ en la fibra de x. Entonces,*

$$(C \cap H)_x = m_x(C) \cdot m_x(H) + \sum_{i=1}^{r} (\widetilde{C} \cap \widetilde{H})_{y_i}.$$

Demostración. Consideremos el diagrama de las variedades explotadas en x

$$\begin{array}{ccccc} \tilde{C} & \longrightarrow & \tilde{\mathbb{A}}^n & \longleftarrow & \tilde{H} \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi''} \\ C & \longrightarrow & \mathbb{A}^n & \longleftarrow & H \end{array}$$

Sea $A = k[x_1,\dots,x_n]$ y supongamos que x es el origen de $\mathbb{A}^n$. Sea $\xi \in \mathfrak{m}_x \backslash \mathfrak{m}_x^2$ un parámetro transversal a C en x. Sabemos que $\tilde{C}$ está contenido en el abierto afín U_ξ^h de $\tilde{\mathbb{A}}^n$ cuyo anillo es $A[x_1/\xi,\dots,x_n/\xi]$. Si $H = (p)_0$, la ecuación de $\tilde{H}$ en el abierto U_ξ^h es $0 = p/\xi^r =: p'$, siendo r la multiplicidad de H en x (es decir, p_r es la componente homogénea de grado mínimo de p).

Denotemos $\mathcal{O}$ el anillo local de C en x y $\mathcal{O}_1$ el anillo de su explosión en x. Entonces

$$\begin{aligned}(C\cap H)_x = l(\mathcal{O}/(p)) \overset{5.3.7}{=} l(\mathcal{O}_1/(p)) = l(\mathcal{O}_1/(\xi^r\cdot p')) &= r\cdot l(\mathcal{O}_1/(\xi)) + l(\mathcal{O}_1/p') \\ &= m_x(H)\cdot m_x(C) + \sum_i (\tilde{C}\cap\tilde{H})_{y_i}.\end{aligned}$$

□

4. Corolario: *La multiplicidad de intersección de una curva íntegra con una hipersuperficie en un punto, es mayor o igual que el producto de sus multiplicidades en dicho punto, siendo igual precisamente si sus espacios tangentes no tienen parte común en dicho punto. En este caso, se dice que se cortan transversalmente y, en el otro, que son tangentes en el punto.*

Demostración. Siguiendo las notaciones de la demostración anterior, se tiene

$$T_xC = \pi'^{-1}(x) \hookrightarrow \pi^{-1}(x) = T_x\mathbb{A}^n \hookleftarrow T_xH = \pi''^{-1}(x)$$

luego $\{y_1,\dots,y_r\} = T_xC \cap T_xH$. La fórmula anterior nos dice que $(C\cap H)_x \geq m_x(C)\cdot m_x(H)$ y que se da la igualdad si y solo si $T_xC \cap T_xH$ es vacío.

□

5. Corolario: *La multiplicidad de una curva íntegra en un punto es igual a la multiplicidad de intersección de la curva explotada con el ciclo excepcional. La multiplicidad de una curva íntegra en un punto es mayor o igual que la suma de las multiplicidades de los puntos de la fibra excepcional de la curva explotada, y es igual si y solo si el ciclo excepcional es transversal a la curva explotada en todos los puntos de corte.*

Demostración. Sea A el anillo local de la curva en el punto dado, digamos x. Sea A_1 el anillo de la explosión de la curva. Sea $\xi = 0$ una hipersuperficie (no singular en x) transversal a la curva en el punto. Entonces $A/(\xi)$ es el anillo de la intersección de la curva con la hipersuperficie $H = (\xi)_0$, y su longitud es justamente la multiplicidad de la curva en x. Por otra parte, $A_1/(\xi)$ es el anillo de la intersección de la curva explotada con el ciclo excepcional. Como $l(A/(\xi)) = l(A_1/(\xi))$, se concluye.

□

5.8. Ramas analíticas

1. Notación : Sea $\mathcal{O}$ un anillo noetheriano íntegro y local de dimensión 1, de modo que el cierre entero en su cuerpo de fracciones sea un $\mathcal{O}$-módulo finito generado. Denotemos $\mathfrak{m}_x$ su ideal maximal.

2. Definición : Se llaman ramas analíticas de $\mathcal{O}$ en x a los ideales primos minimales del completado $\widehat{\mathcal{O}}$ de $\mathcal{O}$ por la topología $\mathfrak{m}_x$-ádica.

3. Teorema : *Sea $\bar{\mathcal{O}}$ el cierre entero de $\mathcal{O}$ en su cuerpo de fracciones Σ. Denotemos $y_1, \ldots, y_s$ los puntos cerrados de* $\mathrm{Spec}\bar{\mathcal{O}}$. *Se verifica que*

$$\bar{\mathcal{O}} \underset{\mathcal{O}}{\otimes} \widehat{\mathcal{O}} = \widehat{\bar{\mathcal{O}}_{y_1}} \times \cdots \times \widehat{\bar{\mathcal{O}}_{y_s}}$$

siendo $\widehat{\bar{\mathcal{O}}_{y_i}}$ la compleción de $\bar{\mathcal{O}}_{y_i}$ por la topología $\mathfrak{m}_{y_i}$-ádica. Por tanto, existe una correspondencia biunívoca entre el espectro minimal de $\bar{\bar{\mathcal{O}}} = \bar{\mathcal{O}} \otimes_{\mathcal{O}} \widehat{\mathcal{O}}$ y el espectro maximal de $\bar{\mathcal{O}}$.

Demostración. Se tiene que

$$\begin{aligned}\bar{\mathcal{O}} \underset{\mathcal{O}}{\otimes} \widehat{\mathcal{O}} = \bar{\bar{\mathcal{O}}} &= \varprojlim_n \bar{\mathcal{O}}/\mathfrak{m}_x^n\bar{\mathcal{O}} = \varprojlim_n \Big(\prod_{i=1}^{s} (\bar{\mathcal{O}}/\mathfrak{m}_x^n\bar{\mathcal{O}})_{y_i}\Big) = \prod_{i=1}^{s} \Big(\varprojlim_n (\bar{\mathcal{O}}_{y_i}/\mathfrak{m}_x^n\bar{\mathcal{O}}_{y_i})\Big) \\ &= \prod_{i=1}^{s} \Big(\varprojlim_n (\bar{\mathcal{O}}_{y_i}/\mathfrak{m}_{y_i}^n)\Big)\end{aligned}$$

donde la última igualdad se debe a que $\mathfrak{m}_y^s \subset \mathfrak{m}_x\bar{\mathcal{O}}_{y_i}$ para $s >> 0$.

Ahora bien, $\bar{\mathcal{O}}_{y_i}$ es un anillo local regular de dimensión 1, luego $\widehat{\bar{\mathcal{O}}_{y_i}}$ también. Por tanto, este último tiene un solo ideal primo maximal y un solo ideal primo minimal.

□

Considérese la sucesión exacta $0 \to \mathscr{O} \to \bar{\mathscr{O}} \to \mathscr{C} \to 0$. Completando se obtiene la sucesión exacta $0 \to \widehat{\mathscr{O}} \to \widehat{\bar{\mathscr{O}}} \to \widehat{\mathscr{C}} \to 0$. Se verifica que $\widehat{\mathscr{C}} = \mathscr{C}$ ya que $\mathscr{C}$ es un $\mathscr{O}$-módulo finito generado de soporte x. En particular, si $\mathfrak{p}_y$ es un ideal primo mínimo de $\widehat{\mathscr{O}}$, entonces $(\widehat{\mathscr{C}})_y = 0$, luego $(\widehat{\mathscr{O}})_y = (\widehat{\bar{\mathscr{O}}})_y$.

4. Teorema: *Hay una correspondencia biunívoca entre las ramas analíticas de $\mathscr{O}$ en x y las valoraciones de Σ que dominan a $\mathscr{O}$, esto es, entre el espectro minimal de $\widehat{\mathscr{O}}$ y el espectro maximal de $\bar{\mathscr{O}}$.*

Demostración. Si $\mathfrak{p}_y$ es un ideal primo minimal de $\widehat{\mathscr{O}}$, la fibra de y por el morfismo $\mathrm{Spec}\widehat{\bar{\mathscr{O}}} \to \mathrm{Spec}\widehat{\mathscr{O}}$ es el espectro de $\widehat{\bar{\mathscr{O}}}_y/\mathfrak{p}_y\widehat{\bar{\mathscr{O}}}_y = \widehat{\mathscr{O}}_y/\mathfrak{p}_y\widehat{\mathscr{O}}_y$ por el comentario anterior. Por tanto, la fibra de y es un solo punto que habrá de ser minimal, luego el espectro minimal de $\widehat{\mathscr{O}}$ está en correspondencia biunívoca con el espectro minimal de $\widehat{\bar{\mathscr{O}}}$. Por el teorema anterior se concluye. □

5. Ejemplo: Sea $C \equiv p(x,y) = 0$ una curva plana íntegra que pasa por el origen, or. Sea $\mathscr{O} = (\mathbb{C}[x,y]_{or}/(p(x,y)))$ es el anillo local de C en or y $\widehat{\mathscr{O}} = \mathbb{C}[[x,y]]/(p(x,y))$.

Sabemos que $\mathbb{C}[[x,y]]$ es un anillo de factorización única (como todo anillo local regular). Por tanto, p descompone en producto de series irreducibles $p(x,y) = f_1 \cdots f_r$, diferentes entre sí porque $\widehat{\mathscr{O}}$ no tiene nilpotentes (ya que $\widehat{\bar{\mathscr{O}}}$, que es producto de anillos regulares, no los tiene). Así pues, las ramas analíticas pueden ser interpretadas como las series en las que factoriza p. Sigamos notaciones previas. Tenemos, además, un morfismo inyectivo $\mathbb{C}[[x,y]]/(f_i) \hookrightarrow \widehat{\bar{\mathscr{O}}_{y_i}} = \mathbb{C}[[t]]$. Entonces, $x = t^n \cdot u(t) \in \mathbb{C}[[t]]$, donde $u(t)$ es una serie invertible. Por cambio de variable ($t' = t \cdot \sqrt[n]{u(t)}$), podemos suponer que $x = t^n$, y por otra parte que $y = t^m \cdot v(t)$, con $v(t)$ invertible. En conclusión, hemos obtenido una parametrización analítica de la rama f_i de $p(x,y)$.

5.8.1. Polígono de Newton

Consideremos la curva plana que pasa por el origen, $0 = p(x,y) = \sum a_{ij}x^i y^j$, $a_{00} = 0$. Las ecuaciones de las distintas ramas de la curva plana son de la forma $x = t^n$, $y = t^m \cdot (a_0 + \dot{t})$, $a_0 \neq 0$ $n, m > 0$. Quiero calcular n, m con la ayuda del polígono de Newton, que definimos más abajo.

Tendremos que $0 = p(t^n, t^m(a_0 + \dot{t})) = \sum a_{ij} t^{ni+mj} \cdot (a_0 + \dot{t})^j$. Sea (i_1, j_1), con $a_{i_1 j_1} \neq 0$ tal que $ni_1 + mj_1 = r$ sea mínimo. Si la ecuación anterior se cumple entonces

$$\sum_{ni+mj=r} a_{ij} a_0^j = 0.$$

Por tanto, la recta $nx + my = r$ pasa por dos o más puntos (i_k, j_k), con $a_{i_k j_k} \neq 0$, y para los demás puntos (i,j), con $a_{ij} \neq 0$, $ni + mj > r$.

Es decir, si dibujamos en el plano los puntos (i,j), con $a_{ij} \neq 0$, la recta $nx+my=r$ $(n,m>0)$ pasa por dos o más de estos puntos y los demás quedan por encima de esta recta. El conjunto de las rectas con estas propiedades se denomina polígono de Newton de $p(x,y)=0$.

Recíprocamente, sea $nx+my=r$ (o $ncx+mcy=rc$, con $c>0$), $n,m>0$ una recta del polígono de Newton. Sea $a_0 \neq 0$ una solución de la ecuación $\sum_{ni+mj=r} a_{ij}a_0^j = 0$. La curva

$$q(t,z) := t^{-r} \cdot p(t^n, t^m(a_0+z))$$

se anula en el origen y tendrá una parametrización $t=u^c$, $z=\dot{u}=s(u)\in k[[u]]$, luego $x=u^{nc}$ e $y=u^{mc}\cdot(a_0+s(u))$. En conclusión, a la recta del polígono de Newton, de ecuación $ncx+mcy=rc$, le corresponde una rama $x=u^{nc}$ e $y=u^{mc}\cdot(a_0+s(u))$.

Observemos que hemos dado un procedimiento recursivo para calcular las ramas.

5.9. Puntos cuspidales y contacto maximal

1. Definición: Sea $x\in C$ un punto de una curva íntegra y $\mathcal{O}$ su anillo local. Diremos que x es un punto cuspidal si el cierre entero de $\mathcal{O}$ es un anillo local.

2. Ejemplo: El origen de la curva cuspidal $y^2-x^3=0$ es un punto cuspidal.

3. Teorema: *Sea C una curva plana sobre un cuerpo algebraicamente cerrado y $x\in C$ un punto cuspidal. Existe un número natural $c_x>0$, llamado contacto maximal con la curva C en la cúspide x, con las siguientes propiedades:*

1. $(C\cap C')_x \leq c_x$, *para toda curva C' regular en x.*
2. $(C\cap C')_x = c_x$ *si y solo si $(C\cap C')_x$ no es múltiplo de la multiplicidad de C en x.*

Demostración. Como el anillo de la explosión $\mathcal{O}_1$ es local, y la multiplicidad de $\mathcal{O}$ en x es igual a la multiplicidad de intersección del ciclo excepcional con la curva explotada $C_1=\mathrm{Spec}\mathcal{O}_1$, tenemos que la multiplicidad de $\mathcal{O}$ es mayor estrictamente que la de $\mathcal{O}_1$ si y solo si el ciclo excepcional es tangente a C_1.

Sea $\mathcal{O}_n$ el primer anillo de la cadena de explosiones cuya multiplicidad r' es menor estrictamente que la de $\mathcal{O}$. Se tienen dos posibilidades:

1. Para algún $i\leq n$, las explosiones i-ésimas C_i y C_i' de C y C' no se cortan. En este caso, $(C\cap C')_x = l\cdot r$, siendo l el primero de tales índices.

2. En otro caso, $(C \cap C')_x = n \cdot r + (C_n \cap C'_n)_x$. Ahora bien, C_n es tangente al ciclo excepcional, pues la multiplicidad ha descendido. Por otra parte, C'_n no puede ser tangente al ciclo excepcional, pues C'_{n-1} es regular (porque C' es regular) y su multiplicidad no puede descender al explotar. En conclusión, C_n y C'_n son transversales y $(C \cap C')_x = n \cdot r + r'$.

Por último, sea C' una curva tal que C'_n es regular en el punto considerado y corta transversalmente a C_n (existe). C' es regular en x: en efecto, C'_n es transversal al ciclo excepcional, pues es transversal a C_n y ésta es tangente al ciclo excepcional, luego C'_{n-1} es regular. Por otra parte, C'_{n-1} es tangente a C_{n-1}, luego transversal al ciclo excepcional correspondiente. Por tanto, C'_{n-2} es regular. Así sucesivamente, vamos obteniendo que las curvas C'_i son regulares para todo i.

Además $(C \cap C')_x = n \cdot r + r'$. □

Sea $\mathcal{O}$ el anillo local de una curva en un punto cuspidal de multiplicidad m. Supongamos que el cuerpo base es algebraicamente cerrado de característica cero.

Como $\bar{\mathcal{O}}$ es local, $\hat{\bar{\mathcal{O}}} = k[[t]]$, siendo t un parámetro de $\bar{\mathcal{O}}$. Si $f \in \mathfrak{m} \setminus \mathfrak{m}^2$ es transversal a $\operatorname{Spec}\mathcal{O}$, entonces $m = l(\mathcal{O}/(f)) = l(\bar{\mathcal{O}}/(f)) = l(\hat{\bar{\mathcal{O}}}/(f))$. Por tanto, $f = s \cdot t^m$, siendo s una serie formal invertible. Como k es algebraicamente cerrado, s tiene raíz m-ésima en $\hat{\bar{\mathcal{O}}} = k[[t]]$. Si definimos $u = \sqrt[m]{s} \cdot t$, entonces $\hat{\bar{\mathcal{O}}} = k[[u]]$ y $f = u^m$. Así pues, toda función de $\hat{\bar{\mathcal{O}}}$ (y por tanto de $\mathcal{O}$) admite un desarrollo en serie formal en $u = \sqrt[m]{f}$. Esto se conoce como desarrollo de Puiseux de dicha función.

En particular, si $\mathcal{O} = k[x_1, \ldots, x_n]/I$, donde x_1 es transversal a $\operatorname{Spec}\mathcal{O}$, cada $\bar{x}_i$ admite un desarrollo de Puiseux $\bar{x}_i = \sum_{j \geq 0} a_j (\sqrt[m]{\bar{x}_1})^j$, con $a_j \in k$.

5.9.1. Desingularización de curvas planas vía el contacto maximal

Para demostrar que las curvas desingularizan mediante un número finito de explosiones, el argumento principal ha sido la finitud del cierre entero. Podría argumentarse de otro modo: El número de puntos singulares es finito, el explotar en un punto las multiplicidades de los puntos de la fibras excepcionales siempre son menores que la partida, salvo que en la fibra excepcional aparezca un solo punto, en tal caso puede mantenerse la multiplicidad. Si sabemos que después de un número finito de explosiones las multiplicidades han bajado, conseguiremos desingularizar la curva.

En este apartado vamos a demostrar, dada una curva plana, la existencia de curvas de "contacto maximal". Es decir, dada un punto de una curva plana, existe una curva regular que pasa por el punto y cuya multiplicidad de intersección en el punto con la curva dada es máxima. Esta curva verificará que pasa por el punto y por los puntos

de las sucesivas fibras excepcionales siempre que no bajen de multiplicidad. Como la multiplicidad de corte de dos curvas es finita (siempre que no tengan componentes comunes) obtendremos que la multiplicidad de una curva en un punto habrá de bajar después de un número finito de explosiones. Así tendremos una nueva demostración de la desingularización de las curvas planas por un número finito de explosiones.

La razón fundamental de la introducción de este apartado es que las técnicas e ideas aquí desarrolladas para la desingularización de curvas planas serán básicamente las que utilizaremos más tarde para la desingularización de superficies.

En este apartado supondremos que k es un cuerpo algebraicamente cerrado de característica cero. Denotaremos $A = k[x, y]$.

4. Definición: Diremos que una aplicación $D : A \to A$ es un operador diferencial de orden 1 si es la suma de una homotecia y una derivación: $D = f + D_0$, con $f \in A$ y D_0 una derivación.

5. Lema: *Si $P(x, y) = 0$ es una curva de multiplicidad m en un punto p y $D : A \to A$ es una derivación, entonces la curva de ecuación $DP(x, y) = 0$ tiene multiplicidad mayor o igual que $m - 1$ en p.*

Demostración. Si $\mathfrak{m}$ es el maximal de A correspondiente al punto p, entonces $D\mathfrak{m}^n \subseteq \mathfrak{m}^{n-1}$, por la regla de Leibnitz. Se concluye inmediatamente. □

6. Observación: El lema sigue siendo cierto si D es un operador diferencial de orden 1.

7. Lema: *Con las notaciones anteriores, existe una derivación D tal que $DP(x, y)$ tiene multiplicidad $m - 1$ en p.*

Demostración. Podemos suponer que p es el origen de coordenadas, es decir, $\mathfrak{m} = (x, y)$. Escribamos $P = P_m + P_{m+1} + \cdots + P_n$ como suma de polinomios homogéneos. Es claro que $\frac{\partial P_m}{\partial x}$ o $\frac{\partial P_m}{\partial y}$ es no nulo (pues $m \geq 1$). Supongamos $\frac{\partial P_m}{\partial x} \neq 0$. Entonces

$$\frac{\partial P}{\partial x} = \frac{\partial P_m}{\partial x} + \text{monomios de grado } \geq m$$

luego $\frac{\partial P}{\partial x}$ tiene multiplicidad $m - 1$. □

8. Definición: Sea p un punto de multiplicidad m de una curva plana C. Diremos que una curva plana X tiene contacto maximal con C en p, si es regular en p y para toda sucesión de transformaciones cuadráticas $C_r \to .^{\pi}. \to C$ la transformada propia X_r de X por la sucesión de explosiones pasa por todos los puntos de $\pi^{-1}(p)$ de multiplicidad m.

9. Teorema: *Sea $C = (P)_0$ una curva plana y $p \in C$ un punto de multiplicidad $m > 1$. Sea $D : A \to A$ un operador diferencial de orden 1 tal que $C' = (DP)_0$ tiene multiplicidad $m-1$ en p. Si X es una curva de contacto maximal con C' en p, entonces también es de contacto maximal con C en p.*

Demostración. La explosión del plano $\mathbb{A}^2 = \mathrm{Spec}\, A$ en el origen está recubierto por dos abiertos afines $\mathrm{Spec}\, A[\frac{x}{t}, \frac{y}{t}]$, con $t = x, y$. Denotemos $\tilde{A} = A[\frac{x}{t}, \frac{y}{t}]$. El teorema va a ser consecuencia del siguiente lema.

10. Lema fundamental: *Sea $D : A \to A$ un operador diferencial de orden 1. Existe un operador diferencial de orden 1, $\tilde{D} : \tilde{A} \to \tilde{A}$, tal que para todo $P \in A$ (de multiplicidad m en el origen) se cumple que*

$$\frac{DP}{t^{m-1}} = \tilde{D}(\frac{P}{t^m}).$$

"La transformada propia de la derivada es la derivada de la transformada propia".

Demostración. Todo operador diferencial de orden 1 es la suma de una homotecia y una derivación. Basta demostrar el lema para cuando D sea una homotecia y para cuando sea una derivación.

1. Si $D = f$ es una homotecia, basta tomar $\tilde{D} = t \cdot f$.

2. Sea D una derivación. Por la regla de Leibnitz, $D(P/t^m) = (DP)/t^m - m(PDt)/t^{m+1}$, de donde se deduce
$$\frac{DP}{t^{m-1}} = (tD)(\frac{P}{t^m}) + (mDt)(\frac{P}{t^m})$$
luego basta tomar $\tilde{D} = m \cdot Dt + tD$. Observemos que $\tilde{D}$ es un operador diferencial de orden 1 de $\tilde{A}$, porque $m \cdot Dt \in \tilde{A}$ y tD es una derivación de A_t que deja estable a $\tilde{A}$, pues $tD(\frac{x}{t}) = Dx - \frac{x}{t}Dt$ y $tD(\frac{y}{t}) = Dy - \frac{y}{t}Dt$.

□

Concluyamos ahora la demostración del teorema. Basta ver, por recurrencia, que si un punto de la explosión de C en p tiene multiplicidad m, entonces es un punto de la explosión de C' en p de multiplicidad $m-1$. Ahora bien, la explosión de C en p tiene ecuación $P/t^m = 0$ y la explosión de C' en p tiene ecuación $DP/t^{m-1} = \tilde{D}(P/t^m) = 0$. Por tanto, si un punto de la explosión de C tiene multiplicidad m, entonces es un punto de la explosión de C' de multiplicidad mayor o igual que $m-1$, luego igual a $m-1$, pues la multiplicidad no aumenta al explotar.

□

11. Observación: La fórmula del lema fundamental demuestra directamente, para curvas planas, que la multiplicidad no aumenta al explotar. En efecto, si C es de multiplicidad 1 en p, entonces la curva explotada es isomorfa a C y no hay nada que decir. Si $C = (P)_0$ es de multiplicidad $m > 1$, sea D tal que DP es de multiplicidad $m-1$. Por inducción sobre la multiplicidad, DP/t^{m-1} es de multiplicidad menor o igual que $m-1$ (en los puntos de la fibra excepcional). Como $DP/t^{m-1} = \tilde{D}(P/t^m)$, P/t^m es de multiplicidad menor o igual que m (en los puntos de la fibra excepcional), por los lemas anteriores.

12. Teorema de existencia de curvas de contacto maximal: *Sea p un punto de multiplicidad m de una curva plana C. Existe una curva plana X que tiene contacto maximal con C en p.*

Demostración. Procedemos por inducción sobre la multiplicidad m de C en p. Si $m = 1$, la propia C es una curva de contacto maximal.

Supongamos que $m > 1$. Sea $C = (P)_0$. Consideremos un operador diferencial D de orden 1 tal que $DP = 0$ tenga multiplicidad $m-1$ en p. Por inducción, existe una curva X que tiene contacto maximal con $C' = (DP)_0$ en p. Por el teorema anterior, X tiene contacto maximal con C en p. □

13. Ejemplo: Calculemos una curva de contacto maximal en el origen a la curva $y^3 + x^2y^4 + 3x^2y^2 + 3yx^4 + x^6 = 0$: Equivale a calcular la curva de contacto maximal de $\frac{\partial(y^3+x^2y^4+3x^2y^2+3yx^4+x^6)}{\partial y} = 3y^2 + 4y^3x^2 + 6yx^2 + 6x^4 = 0$, que equivale a calcular la curva de contacto maximal de $\frac{\partial(3y^2+4y^3x^2+6yx^2+6x^4)}{\partial y} = 6y + 12y^2x^2 + 6x^2 = 0$. Luego una curva de contacto maximal en el origen a $y^3 + y^2x^2 + x^6 + x^7 = 0$ es $y + 2y^2x^2 + x^2 = 0$.

En el caso de un punto cuspidal, la curva de contacto maximal del teorema es la curva regular de máxima multiplicidad de intersección con C en p (véase el teorema 5.9.3 y su demostración).

14. Corolario: *Toda curva plana reducida desingulariza mediante un número finito de transformaciones cuadráticas.*

Demostración. Sea $C = (P)_0$ y descompongamos P en irreducibles, $P = P_1 \cdots P_r$ (con los P_i primos entre sí). Explotando hasta separar las componentes, podemos suponer que P es irreducible.

Consideremos una curva X de contacto maximal con C en p. Si explotando indefinidamente la curva C siempre hubiera algún punto sobre p de multiplicidad m, entonces la multiplicidad de intersección de C y X sería infinita (por 5.7.3), lo cual no es posible. Por tanto, después de un número finito de explosiones la multiplicidad debe bajar estrictamente, y se concluye por inducción. □

5.10. Teoremas de Bézout y Max Noether

Sea C una curva proyectiva del espacio proyectivo $\mathbb{P}^n(k)$ y H una hipersuperficie que no contiene ninguna componente irreducible de C. Entonces, $C \cap H = \{y_1, \dots, y_m\}$ es un número finito de puntos cerrados. Cada punto y_i está en un abierto afín $\mathbb{P}^n - (x_j)_0^h$ y deshomogeneizando tenemos que $(C \cap H) \cap U_{x_j}^h = \operatorname{Spec} A_i$. El número de puntos de corte (contando multiplicidades y grados) de C con H, que denotaremos $(C \cap H)$, diremos que es $\dim_k A_{i,y_i}$. Este número no depende de la elección de $U_{x_j}^h$ y es estable por cambios de cuerpo base.

1. Teorema de Bézout: *Sean C, C' dos curvas proyectivas planas sin componentes comunes y de grados r, r'. Entonces*

$$(C \cap C') = r \cdot r'$$

Demostración. Podemos suponer, por cambio de base, que el cuerpo es algebraicamente cerrado. Mediante un cambio de coordenadas, podemos suponer que el hiperplano del infinito $x_0 = 0$ no pasa por ninguno de los puntos de intersección de las curvas C y C'.

Escribamos $C = \operatorname{Proj} k[x_0, x_1, x_2]/(p_r(x_0, x_1, x_2))$, $C' = \operatorname{Proj} k[x_0, x_1, x_2]/(p_{r'}(x_0, x_1, x_2))$. Sea $p(x, y) = \frac{p_r(x_0, x_1, x_2)}{x_0^r}$ y $p'(x, y) = \frac{p_{r'}(x_0, x_1, x_2)}{x_0^{r'}}$. Tenemos que probar que

$$\dim_k k[x, y]/(p(x, y), p'(x, y)) = r \cdot r'.$$

Denotemos $B = k[x_0, x_1, x_2]/(p_r, p_{r'})$, $B' = k[x, y]/(p(x, y), p'(x, y))$. Se tiene que

$$B' = [B_{\bar{x}_0}]_0 = \bigcup_i \frac{B_i}{\bar{x}_0^i}$$

Veamos que para $n >> 0$

$$B' = \frac{B_n}{\bar{x}_0^n} \quad \text{y} \quad \frac{B_n}{\bar{x}_0^n} \simeq B_n$$

Como $\frac{B_i}{\bar{x}_0^i} \subseteq \frac{B_{i+1}}{\bar{x}_0^{i+1}}$ y B' es de dimensión finita, se concluye que $B' = \frac{B_n}{\bar{x}_0^n}$ para $n >> 0$. Sólo queda ver que $\frac{B_n}{\bar{x}_0^n} \simeq B_n$, es decir, que en B_n no hay elementos anulados por $\bar{x}_0$. Para $n >> 0$, $\dim_k B_n$ es constante y $[B/(x_0)]_n = 0$ porque $B/(x_0)$ es una k-álgebra finita, porque es de dimensión de Krull cero, ya que su espectro proyectivo es vacío. De la sucesión exacta

$$0 \to \operatorname{Ker} x_0 \cdot \to B \xrightarrow{x_0 \cdot} B \to B/(x_0) \to 0$$

se deduce que $[\operatorname{Ker} x_0]_n = 0$, para $n >> 0$, que es lo que queríamos probar.

Denotemos $A = k[x_0, x_1, x_2]$. La sucesión (complejo de Koszul de $p_r, p_{r'}$)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \oplus A & \longrightarrow & A & \longrightarrow & B \longrightarrow 0 \\ & & q & \longmapsto & (p_{r'} \cdot q, -p_r \cdot q) & & q & \longmapsto & \bar{q} \\ & & & & (q, q') & \longmapsto & p_r \cdot q + p_{r'} \cdot q' & & \end{array}$$

es exacta. Denotemos por $A[-n]$ al anillo A pero donde dotamos de grado $m+n$ a los polinomios homogéneos de grado m. Entonces la anterior sucesión exacta se reescribe:

$$0 \to A[-r-r'] \to A[-r] \oplus A[-r'] \to A \to B \to 0$$

y ahora los morfismos conservan la graduación. Por tanto, se tiene una sucesión exacta en cada grado y tomando dimensiones

$$\dim_k B_m = \binom{m+2}{2} + \binom{m+2-r-r'}{2} - \binom{m+2-r}{2} - \binom{m+2-r'}{2} = r \cdot r'$$

para $m \geq r + r'$.

□

2. Un algoritmo para el cálculo de las componentes irreducibles de una curva plana: Sea $C \equiv p(x,y) = 0$ una curva plana de grado n y $p \in C$ un punto racional no singular. Si C es reducible entonces una de sus componentes es una curva C' de grado menor que n que pasa por p, y p es un punto no singular de C'. C' es una curva que corta a C en p con multiplicidad infinita. Si una curva irreducible de grado $r < n$ corta a C en p con multiplicidad mayor que $n \cdot r$, entonces es una componente de C, por el teorema de Bézout.

Supongamos que C es reducible y por cambio de coordenadas que $x = 0$ es transversal a C en $p = (0, \beta_1)$. Veamos que condiciones habrá de verificar los coeficientes b_{ij} de $C' \equiv q(x,y) = \sum_{0 \leq i+j < n} b_{ij} x^i y^j$ para que C' esté incluida en C (y pase por p). C' ha de pasar por p, es decir, $q(0, \beta_1) = 0$, que es una ecuación lineal en los b_{ij}. Los coeficientes de la explosión de C' en p, $\tilde{C}'$, en las coordenadas $x, z = (y - \beta_1)/x$ son una combinación lineal de los coeficientes b_{ij} de C'. El ciclo excepcional, $x = 0$, es transversal a la explosión de C en el único punto de la fibra excepcional, digamos $(0, \beta_2)$. $\tilde{C}'$ ha de pasar por $(0, \beta_2)$, que es de nuevo una ecuación lineal en los coeficientes b_{ij}. En conclusión, imponer que C' corte a C en p con multiplicidad $n \cdot (n-1) + 1$ es resolver un sistema de $n \cdot (n-1) + 1$ ecuaciones lineales en las b_{ij}. Si calculamos la solución C' de menor grado de este sistema de ecuaciones habremos calculado la componente irreducible de C que pasa por p.

Dada una curva proyectiva plana $C = (p_n(x_0,x_1,x_2))_0^h$, un punto cerrado $x \in C$ y un abierto afín que lo contiene, digamos $U_{x_0}^h \subset \mathbb{P}^2$, tenemos que $C \cap U_{x_0}^h$ es la curva del plano afín de ecuación $p_n(x_0,x_1,x_2)/x_0^n = p_n(1,x_1/x_0,x_2/x_0) = 0$. Denotaremos $\mathfrak{p}_{C,x} = (p_n(1,x_1/x_0,x_2/x_0)) \subset k[x_1/x_0,x_2/x_0]_x$ y diremos que es el ideal de gérmenes en x de funciones del plano que se anulan en C, ideal que no depende del abierto afín considerado.

3. Teorema de Max Noether : *Sean $p_i \in k[x_0,x_1,x_2]$ polinomios homogéneos ($i = 1,2,3$) y consideremos las curvas proyectivas planas $C_i = (p_i)_0^h$. Supongamos que C_1, C_2 no tienen componentes comunes. Existe una ecuación*

$$p_3 = a \cdot p_1 + b \cdot p_2$$

con a,b polinomios homogéneos de grados $\operatorname{gr} a = \operatorname{gr} p_3 - \operatorname{gr} p_1, \operatorname{gr} b = \operatorname{gr} p_3 - \operatorname{gr} p_2$, si y solo si para todo $x \in C_1 \cap C_2$ se verifica que $\mathfrak{p}_{C_3,x} \subseteq \mathfrak{p}_{C_1,x} + \mathfrak{p}_{C_2,x}$.

Demostración. La necesidad es obvia, veamos la suficiencia.

La hipótesis equivale a que $(\frac{p_3}{x_i^{n_3}}) \subseteq (\frac{p_1}{x_i^{n_1}}) + (\frac{p_2}{x_i^{n_2}})$, para todo i, porque localmente es así. Luego la hipótesis se mantiene por cambio de cuerpo base. La tesis es cierta si lo es por cambio de cuerpo base. Podemos suponer que el cuerpo es algebraicamente cerrado.

Haciendo un cambio de coordenadas homogéneo, podemos suponer que x_0 no se anula en ningún punto de $C_1 \cap C_2$, es decir, $p_1(0,x_1,x_2)$ es primo con $p_2(0,x_1,x_2)$. Sabemos que

$$\frac{p_3}{x_0^{n_3}} = a \cdot \frac{p_1}{x_0^{n_1}} + b \cdot \frac{p_2}{x_0^{n_2}}$$

porque $(\frac{p_3}{x_0^{n_3}}) \subseteq (\frac{p_1}{x_0^{n_1}}) + (\frac{p_2}{x_0^{n_2}})$. Homogeneizando tenemos que

$$x_0^r \cdot p_3 = a' p_1 + b' p_2.$$

Sea r mínimo en las igualdades de esta forma. Si $r > 0$, entonces

$$0 = a'(0,x_1,x_2)p_1(0,x_1,x_2) + b'(0,x_1,x_2)p_2(0,x_1,x_2).$$

Por tanto, $a'(0,x_1,x_2) = h \cdot p_2(0,x_1,x_2)$ y $b'(0,x_1,x_2) = -h \cdot p_1(0,x_1,x_2)$. Luego $a'' := a' - h \cdot p_2$ y $b'' := b' + h \cdot p_1$ son divisibles por x_0, y $x_0^r \cdot p_3 = a'' p_1 + b'' p_2$. Dividiendo esta igualdad por x_0 llegamos a contradicción, porque $r - 1 < r$. En conclusión,

$$p_3 = a \cdot p_1 + b \cdot p_2.$$

□

4. Proposición: *Sean C_i curvas proyectivas planas definidas por los respectivos polinomios homogéneos $p_i \in k[x_0,x_1,x_2]$ ($i = 1,2,3$). Supongamos que C_1, C_2 no tienen componentes comunes y que k es algebraicamente cerrado. Entonces C_3 verifica las condiciones de Noether en un punto cerrado $x \in C_1 \cap C_2$ (es decir, $\mathfrak{p}_{C_3,x} \subseteq \mathfrak{p}_{C_1,x} + \mathfrak{p}_{C_2,x}$) en cualquiera de los casos siguientes*

1. *C_1 y C_2 son no singulares en x, se cortan transversalmente en x y $x \in C_3$.*
2. *x es un punto no singular de C_1 y $(C_1 \cap C_3)_x \geq (C_1 \cap C_2)_x$ (es decir, la multiplicidad de intersección de C_3 con C_1 en x es mayor o igual que la multiplicidad de intersección de C_2 con C_1 en x).*
3. *C_1 y C_2 poseen tangentes distintas en x y $m_x(C_3) \geq m_x(C_1) + m_x(C_2) - 1$.*

Demostración. Como la proposición es local, podemos suponer que las curvas C_i son curvas planas afines de ecuaciones $p_i(x,y) = 0$.

1. Por las hipótesis $(k[x,y]/(p_1,p_2))_x = k$. Por tanto, si denotamos $\mathfrak{m}_x$ el ideal maximal de las funciones que se anulan en x, tenemos que $\mathfrak{m}_x = (p_1,p_2)_x$, luego $(p_3)_x \subset (p_1,p_2)_x$.

2. Si x es un punto no singular de C_1, entonces $\overline{\mathfrak{m}}_x = (t)$ en $(k[x,y]/(p_1(x,y)))_x$. Además, $\overline{(p_i(x,y))} = (t^{(C_i \cap C_1)_x})$. Por tanto, $\overline{(p_3(x,y))} \subseteq \overline{(p_2(x,y))}$, luego $(p_3)_x \subset (p_1,p_2)_x$.

3. Vamos a usar el lema de estabilidad para curvas planas: si $\mathcal{O}_{C_1,x} \to \tilde{\mathcal{O}}_{C_1,x}$ es el morfismo de explosión en el punto x, entonces $\mathfrak{m}_x^{m_x(C_1)-1} = \mathfrak{m}_x^{m_x(C_1)-1} \cdot \tilde{\mathcal{O}}_{C_1,x}$

Por otra parte, si ξ es un parámetro transversal a C_1 en x, por el que explotamos, y $p'(x/\xi, y/\xi) = p_2(x,y)/\xi^{m_x(C_2)} = 0$ la ecuación de la explosión de C_2 en x, tenemos que $p_2(x,y) \cdot \tilde{\mathcal{O}}_{C_1,x} = p'(x/\xi, y/\xi) \cdot \xi^{m_x(C_2)} \cdot \tilde{\mathcal{O}}_{C_1,x} = \xi^{m_x(C_2)} \cdot \tilde{\mathcal{O}}_{C_1,x}$, porque C_1 y C_2 no tienen tangentes comunes en x. Por tanto, $p_2(x,y) \cdot \tilde{\mathcal{O}}_{C_1,x} = \mathfrak{m}_x^{m_x(C_2)} \cdot \tilde{\mathcal{O}}_{C_1,x}$.

Con todo,

$$\begin{aligned} p_3(x,y) \in \mathfrak{m}_x^{m_x(C_3)} &\subset \mathfrak{m}_x^{m_x(C_1)+m_x(C_2)-1} = \mathfrak{m}_x^{m_x(C_2)} \cdot \mathfrak{m}_x^{m_x(C_1)-1} \\ &= \mathfrak{m}_x^{m_x(C_2)} \cdot \mathfrak{m}_x^{m_x(C_1)-1} \cdot \tilde{\mathcal{O}}_{C_1,x} = p_2(x,y) \cdot \mathfrak{m}_x^{m_x(C_1)-1} \cdot \tilde{\mathcal{O}}_{C_1,x} \\ &= p_2(x,y) \cdot \mathfrak{m}_x^{m_x(C_1)-1} \subset p_2(x,y)\mathcal{O}_{C_1,x} \end{aligned}$$

por lo que $(p_3)_x \subset (p_1,p_2)_x \in k[x,y]$.

□

5.11. Problemas

1. Sea A un anillo íntegro de cuerpo de fracciones Σ y $v\colon A \to \mathbb{Z}$ una aplicación (no nula) que cumple que $v(aa') = v(a) + v(a')$ y que $v(a+a') \geq \text{ínf} v(a), v(a')$ (para

todo $a, a' \in A$ y seguimos la convención $v(0) = \infty$). Probar que v extiende de modo único a una valoración discreta de Σ.

2. Pruébese que el anillo local de $k[x, y]$ en el origen es íntegramente cerrado pero no es un anillo de valoración.

3. Sea $\mathcal{O}_v$ un anillo de valoración de cuerpo de fracciones Σ. Pruébese

   a) Si B es un subanillo de valoración de Σ contenido en $\mathcal{O}_v$, entonces existe un ideal primo $\mathfrak{p}_x$ de B de modo que $\mathcal{O}_v = B_x$.

   b) Si $\mathfrak{p}_x$ es un ideal primo de $\mathcal{O}_v$, entonces $\mathcal{O}_v/\mathfrak{p}_x$ es un anillo de valoración.

   c) Sea $\pi : \mathcal{O}_v \to \mathcal{O}_v/\mathfrak{p}_v$ el morfismo de paso al cociente. Si $\bar{B}$ es un subanillo de valoración de $\mathcal{O}_v/\mathfrak{p}_v$ entonces $\pi^{-1}(\bar{B})$ es un subanillo valoración.

   d) Existe una correspondencia biunívoca entre los anillos de valoración de Σ contenidos en $\mathcal{O}_v$ y los subanillos de valoración de $\mathcal{O}_v/\mathfrak{p}_v$.

4. Consideremos el morfismo $\mathbb{C}[x, y] \to \mathbb{C}[[\theta]]$, $x \mapsto \theta, y \mapsto \operatorname{sen}\theta$. Demuestra que $\mathcal{O}_v = \mathbb{C}(x, y) \cap \mathbb{C}[[\theta]]$ es un anillo de valoración discreta, tal que $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{C}$. Explica la frase "$v(p(x, y))$ es igual a la multiplicidad de intersección de $p(x, y) = 0$ con $y = \operatorname{sen} x$, en el origen".

5. Sea $\mathcal{O}_v$ un anillo de valoración discreta de $\mathbb{C}(x, y)$ trivial sobre $\mathbb{C}$.

   a) Demuestra que $\mathcal{O}_v$ contiene a $\mathbb{C}[x, y]$, o a $\mathbb{C}[\frac{1}{x}, \frac{y}{x}]$, o a $\mathbb{C}[\frac{1}{y}, \frac{x}{y}]$.

   b) Si $\mathcal{O}_v$ contiene a $\mathbb{C}[x, y]$ y $\mathfrak{p}_v \cap \mathbb{C}[x, y] = \mathfrak{p}_C$ es el ideal de una curva, demuestra que $\mathcal{O}_v = \mathbb{C}[x, y]_C$.

   c) Si $\mathcal{O}_v$ contiene a $\mathbb{C}[x, y]$ y $\mathfrak{p}_v \cap \mathbb{C}[x, y] = \mathfrak{m}_x$ es un ideal maximal, por ejemplo $\mathfrak{m}_x = (x, y)$, demuestra que $\mathcal{O}_v$ contiene a $\mathbb{C}[x_1, y_1]$ con $x_1 = x$, $y_1 = \frac{y}{x}$ ó $x_1 = \frac{x}{y}$, $y_1 = y$.

   d) Con las notaciones obvias a partir del apartado anterior. Supongamos que $\mathfrak{p}_v \cap \mathbb{C}[x_n, y_n]$ es un ideal maximal para todo $n \in \mathbb{N}$. Demuestra que existe un $m \in \mathbb{N}$, de modo que $v(x_m)$ (o $v(y_m)$) es mínimo entre todos los $v(x_n), v(y_n)$. Demostrar que $\widehat{\mathcal{O}}_v = \varprojlim_i \mathcal{O}_v/(\mathfrak{p}_v^i) = \mathbb{C}[[x_m]]$ y que por tanto $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{C}$.

6. Sea $\mathbb{Z} \times \mathbb{Z}$ con el orden lexicográfico. Fijemos $q(x, y) \in \mathbb{C}[x, y]$ y fijemos un punto q de $q(x, y) = 0$. Consideremos la aplicación $v : \mathbb{C}[x, y] \setminus \{0\} \to \mathbb{Z} \times \mathbb{Z}$, definida por, $v(p(x, y)) = (n, m)$, donde $p(x, y) = q(x, y)^n \cdot r(x, y)$ ($r(x, y)$ no divisible por $q(x, y)$) y donde m es la multiplicidad de $p(x, y)$ en el origen. Demuestra que v extiende a una valoración de $\mathbb{C}(x, y)$.

7. Sea α un número irracional positivo. Demuestra que $v : \mathbb{C}[x,y] \to \mathbb{Z}+\mathbb{Z}\alpha$, definida por $v(\sum c_{n,m}x^n y^m) = \text{mín}\{n+m\alpha | c_{n,m} \neq 0\}$ extiende a una valoración de $\mathbb{C}(x,y)$.

8. Sea Σ un cuerpo. Un valor absoluto en Σ es una aplicación $f : \Sigma \to \mathbb{R}^+$ satisfaciendo los siguientes axiomas

   a) $f(x) = 0$ si y solo si $x = 0$.

   b) $f(xy) = f(x)f(y)$, para todo $x, y \in \Sigma$.

   c) $f(x+y) \leq C\,\text{máx}\{f(x), f(y)\}$ para todo $x, y \in \Sigma$ y cierto $C \in \mathbb{R}^+$.[4]

   Pruébese que existe una correspondencia biunívoca entre los valores absolutos con $C = 1$ ("no arquimedianos") y las valoraciones de Σ con valores en $\mathbb{R}$. (Pista: Dado un valor absoluto f, pruébese que $-\log(f)$ es una valoración.)

9. Sea $\tilde{\mathbb{C}} = \mathbb{C} \coprod \infty$. Impongamos $-\infty = \infty$, $0^{-1} = \infty$, $\infty^{-1} = 0$; $a + \infty = \infty + a = \infty$, para todo $a \in \mathbb{C}$; $\infty \cdot a = a \cdot \infty = \infty$, para todo $a \in \tilde{\mathbb{C}}$. Sea K un cuerpo. Sea $f : K \to \tilde{\mathbb{C}}$ una aplicación tal que

$$f(x+y) = f(x) + f(y), \quad f(x \cdot y) = f(x) \cdot f(y), \quad f(1) = 1$$

   siempre que los términos escritos tengan sentido. [5]Demuestra que los $x \in K$ tales que $f(x) \neq \infty$ (es decir, valor finito) forman un subanillo de valoración de K.

10. Prueba que $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ es un dominio de Dedekind.

11. Sea A un dominio de Dedekind, $x_1, \ldots, x_r \in \text{Spec}\, A$ puntos cerrados y $n_1, \ldots, n_r \in \mathbb{N}$. Prueba que existe $f \in A$, de modo que $v_{x_i}(f) = n_i$, para $1 \leq i \leq r$.

12. Sea A un dominio de Dedekind y M un A-módulo finito generado.

    a) Pruébese que si M es libre de torsión es suma directa de ideales. (Recuérdese 0.6.79)

[4]En Bourbaki, Commutative Algebra, puede verse: Se verifica que $C \geq 1$. Si $C \leq 2$ la condición tercera, supuestas las dos primeras, equivale a $f(x+y) \leq f(x) + f(y)$. Todo valor absoluto define la topología donde la base de entornos de un punto $x \in \Sigma$ es $\{y \in \Sigma | f(x-y) < \epsilon\}$, para $\epsilon \in \mathbb{R}^+$. Si identificamos dos valores absolutos si definen la misma topología, podremos suponer (tomando f^α, para cierto $\alpha \in \mathbb{R}^+$) que $C = 1$ o que $C = 2$ (denominado valor absoluto "arquimediano"). Así puede verse que los valores absolutos de $\mathbb{Q}$ están en correspondencia con el conjunto de números primos positivos junto con el valor absoluto "arquimediano" estándar de $\mathbb{Q}$. El teorema de Gelfand-Mazur, dice que si Σ es una $\mathbb{R}$-extensión de cuerpos, y posee una norma compatible con la estructura de álgebra de Σ, entonces Σ es $\mathbb{R}$ o $\mathbb{C}$. El teorema de Ostrowski dice que si f es un valor absoluto arquimediano, entonces Σ es una subextensión densa de $\mathbb{R}$ o $\mathbb{C}$ y f es equivalente al valor absoluto estándar.

[5]Sea K el cuerpo de funciones meromorfas sobre una variedad analítica compleja de dimensión 1. Entonces $f : K \to \tilde{\mathbb{C}}$, $g \mapsto g(z_0)$, siendo z_0 un punto de la variedad, es un ejemplo.

b) Prueba que M es isomorfo a la suma directa de su parte de torsión, un A-módulo libre y un ideal.

13. Demuestra que el cierre entero de $\mathbb{Z}[\sqrt[2]{5}]$ en $\mathbb{Q}[\sqrt[2]{5}]$ es finito sobre $\mathbb{Z}[\sqrt[2]{5}]$. (Pista: $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt[2]{5}]$ es finito y $\mathbb{Z}$ es íntegramente cerrado en su cuerpo de fracciones).

14. Sea $\mathcal{O}$ un anillo local íntegro. Prueba que el cierre entero de $\mathcal{O}$ en su cuerpo de fracciones es la intersección de los anillos de valoración del cuerpo de fracciones que dominan a $\mathcal{O}$.

15. Sea $\mathfrak{m}_{or} = (x) \subseteq k[x]$ y $\mathcal{O} := k[x]_{or}$. Sea $\Sigma := k(x^{1/n})_{n\in\mathbb{N}}$. Prueba que no existe ningún anillo de valoración discreta de Σ que domine a $\mathcal{O}$.

16. Sea A un anillo noetheriano íntegro y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones.

    a) Si $0 \neq I \subset A$ es un ideal, definir inclusiones naturales, $A \hookrightarrow \mathrm{Hom}_A(I,I) \hookrightarrow \bar{A}$.

    b) Si $0 \neq I \subset A$ es un ideal radical, prueba que $\mathrm{Hom}_A(I,A) \cap \bar{A} = \mathrm{Hom}_A(I,I)$.

17. Sea A un anillo noetheriano íntegro y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. Sea $Y \subset \mathrm{Spec}\, A$ el conjunto de los puntos x, tales que A_x no sea íntegramente cerrado en su cuerpo de fracciones. Sea I un ideal radical no nulo que se anule en todo Y.

    a) Dada $h = \frac{f}{g} \in \bar{A}$, prueba que $(\mathrm{Anul}(hA/(hA \cap A)))_0 = \{x \in \mathrm{Spec}\, A : h \notin A_x\} \subset Y$.

    b) Prueba que existe $n \in \mathbb{N}$ de modo que $I^n \subset \mathrm{Anul}(hA/(hA \cap A))$.

    c) Prueba que si $A = \mathrm{Hom}_A(I,I)$ entonces A es íntegramente cerrado en su cuerpo de fracciones.

18. Sea $X = \mathrm{Spec}\, A$ una variedad algebraica íntegra sobre un cuerpo algebraicamente cerrado. Prueba que el conjunto de puntos $x \in X$ tales que A_x sea íntegramente cerrado en su cuerpo de fracciones es un abierto de X.

19. Prueba que los anillos de valoración del cuerpo de fracciones de $\mathbb{C}[x,y]/(x^2+y^2-1)$ que contienen a $\mathbb{C}$, se corresponden con los puntos de la circunferencia en el plano proyectivo.

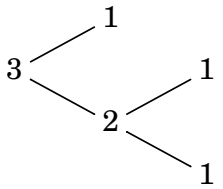
20. Prueba que las $\mathbb{C}$-álgebras $\mathbb{C}[x,y]/(x^2+y^2-1)$, $\mathbb{C}[x]$ no son isomorfas aunque sí son birracionalmente isomorfas.

21. Calcula los anillos de valoración del cuerpo de fracciones de $\mathbb{C}[x,y]/(y^2-x^2+x^3)$, que contengan a $\mathbb{C}$.

22. Desingularizar la curva $y^2 - x^7 = 0$. ¿Es esta curva birracional a la recta afín?

23. Calcula la multiplicidad de intersección de $y^2 - x^3 + y^4 = 0$ con $yx + x^3 + y^3 = 0$ en el origen.

24. Definir una curva plana que pase por el origen y cuyo árbol de explosión en el origen sea



25. Prueba que el morfismo $k[x,y]/(y^2 - x^2 + x^3) \hookrightarrow [k[x, \frac{y}{x}]/((\frac{y}{x})^2 - 1 + x)]_{\frac{y}{x}-1}$ no es un morfismo finito.

26. Calcula el grado del revestimiento $k[x] \to k[x,y]/(x^2 + y^2 - 1)$. Calcula los puntos en que ramifica.

27. Sean X e Y dos k-variedades algebraicas y $x \in X$ e $y \in Y$ dos puntos racionales. Prueba que
$$m_{(x,y)}(X \times_k Y) = m_x(X) \cdot m_y(Y)$$

28. Prueba que las cúbicas proyectivas $y^2 - x^3 - 1 = 0$ y $y^2 - x^3 - 2 = 0$ se cortan en un único punto con multiplicidad 9.

29. Parametrizar la curva $x^6 - x^2y^3 - y^5 = 0$. Calcula sus soluciones racionales.

30. Prueba el Teorema de Pascal: Si un hexágono está inscrito en una cónica irreducible, entonces los lados opuestos se cortan en puntos alineados.

31. Prueba el Teorema de Pappus: Sean R_1, R_2 dos rectas; $p_1, p_2, p_3 \in R_1$ y $q_1, q_2, q_3 \in R_2$ (ninguno de ellos se encuentran sobre $R_1 \cap R_2$). Sea R_{ij} la recta que une p_i y q_j. Prueba que los puntos $p_{ij} = R_{ij} \cap R_{ji}$ $(i < j)$ están alineados.

32. Ley de grupo en las cúbicas. Sea C una cúbica plana no singular. Fijemos un punto $p_0 \in C$. Dados dos puntos $p, q \in C$, la recta que pasa estos dos puntos, corta a C en un tercer punto r. Definamos $\phi\colon C \times C \to C$, $(p,q) \mapsto r$. Probar que la aplicación $C \times C \to C$, $(p,q) \mapsto \phi(p_0, \phi(p,q))$ dota a C de estructura de grupo abeliano.

33. Sean C_3, C_3' dos cúbicas planas que se cortan en 9 puntos distintos, de manera que 6 de ellos están sobre una cónica. Probar que los tres restantes están alineados.

34. Demuestra que las tangentes a una cúbica irreducible plana en 3 puntos alineados cortan a la cúbica en otros 3 puntos alineados.

35. Demuestra que si un triángulo está inscrito en una cónica irreducible, entonces los puntos de corte de cada lado del triángulo con la tangente a la cónica en el vértice opuesto, están alineados.

36. Prueba que una recta que pase por dos puntos de inflexión de una cúbica plana irreducible pasa por un tercer punto de inflexión.

37. Prueba que si una cúbica pasa por ocho de los nueve puntos distintos de corte de otras dos cúbicas, entonces también pasa por el noveno.

38. Sea C_3 una cúbica plana y $x \in C_3$ un punto de inflexión. Probar que los puntos $y \in C_3$ para los que existe una cónica que cumpla $m_x(C_3 \cap C_2) = m_y(C_3 \cap C_2) = 3$, son las terceras intersecciones de las rectas que unen los puntos de inflexión con x.

39. Teorema de Cayley-Bacharay: Sea C_{n+m-3} una curva plana de $n+m-3$ que pasa por $n \cdot m - 1$ de los puntos de intersección de dos curvas de grados n y m. Prueba que C_{n+m-3} pasa por el punto restante.

40. Si una curva $C_{n+m-\gamma}$ de grado $n+m-\gamma$ ($\gamma > 3$), pasa por $n \cdot m - \frac{(\gamma-1)(\gamma-2)}{2}$ de los $n \cdot m$ puntos distintos en los que se cortan dos curvas de grados n y m, entonces pasa también por los restantes puntos siempre que dichos puntos no estén en una curva de grado $\gamma - 3$.

41. *a*) Sea C la cúbica plana $y^2 = x^2 + x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}_1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcula el área del "ojo del lazo" definido por la curva $y^2 = x^2 + x^3$.

    b) Sea C la cúbica plana $y^2 = x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}_1 \to C$, $x = t^2$, $y = t^3$.

42. Prueba que si una cónica tiene un punto singular entonces no es irreducible.

43. Prueba que si una cúbica plana tiene dos puntos singulares entonces no es irreducible.

44. Prueba que si una cuártica plana tiene cuatro puntos singulares entonces no es irreducible.

45. Prueba que $(0,0),(2,0),(0,2)$ son puntos singulares de la cuártica plana $xy(x+y-2)-(x^2+y^2-2x-2y)^2=0$. ¿Existen más puntos singulares? Parametrizar esta cuártica (mediante un haz de cónicas).

46. Justificar por qué las circunferencias $x^2+y^2-1=0$, $x^2+y^2-2=0$ han de ser tangentes en algún punto del infinito, sin hacer el cálculo explícito de sus tangentes en los puntos del infinito.

47. Calcula la multiplicidad de intersección de las cúbicas proyectivas planas $y^2-x^3=0$ con $y^2-x^3-1=0$, en todos los puntos de intersección. Poner un ejemplo de dos cúbicas planas afines irreducibles, cuyos puntos de corte estén alineados.

48. Sean $X=\operatorname{Spec}A$ e $Y=\operatorname{Spec}B$ variedades sobre un cuerpo algebraicamente cerrado. Sean $x\in X$, $y\in Y$ dos puntos cerrados. Prueba que las multiplicidades cumplen
$$m_{(x,y)}(X\times Y)=m_x(X)\cdot m_y(Y)$$

49. Sea $X=\operatorname{Spec}\mathscr{O}_X$, supongamos que $\mathscr{O}_X$ es un anillo noetheriano e $I\subset\mathscr{O}_X$ un ideal. Se verifica que

    a) La explosión de X por el ideal I es isomorfa a la explosión de X por I^n, para todo $n>0$.

    b) Si X es regular, $\pi\colon X'\to X$ es el morfismo de explosión por I y $U\subset X$ es el máximo abierto tal que $\pi^{-1}(U)=U$, entonces π es la explosión por un ideal I', tal que $(I')_0\subseteq X-U$.

    Resolución: (a) El morfismo graduado, $B=\mathscr{O}_X\oplus I^m\oplus I^{2m}\oplus\ldots\subset B'=\mathscr{O}_X\oplus I\oplus I^2\oplus\ldots$, donde las funciones de grado 1, I^m, de B se aplican en los elementos de grado m, I^m, de B', establece un isomorfismo entre los espectros proyectivos correspondientes, como puede comprobarse.

    (b) El ideal I es localmente principal en U, ya que el morfismo de explosión, π, sobre U es un isomorfismo. Así pues, si $x_1,\ldots,x_r$ son los puntos genéricos de $(I)_0\cap U$, la descomposición primaria de I será de la forma
$$I=\mathfrak{p}_{x_1}^{n_1}\cap\ldots\cap\mathfrak{p}_{x_r}^{n_r}\cap I'=\mathfrak{p}_{x_1}^{n_1}\cdot\ldots\cdot\mathfrak{p}_{x_r}^{n_r}\cdot I'$$
    de modo que $(I')_0\subseteq X-U$. Basta probar que la explosión por un ideal $I=I_1\cdot I_2$, es isomorfa a la explosión por I_2, si I_1 es localmente principal: Localmente, si

$I_1 = (f)$, los isomorfismos $I_2^m \xrightarrow{f^m \cdot} I^m$ definen un isomorfismo entre las álgebras de Rees de I_2 y I, que al tomar espectros proyectivos no dependen de la elección del generador f de I_1. Luego tenemos un isomorfismo global de las explosiones de X por I_2 e I.

Capítulo 6

Teoría de Números Algebraica

6.1. Introducción

[1]Para el estudio y clasificación de los anillos de números enteros, A, se introducen el discriminante de A, el grupo Pic(A) y el grupo de las unidades de A. Dado un cuerpo de números, K, tenemos la inmersión canónica $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$ y resulta que el anillo de enteros de K, A, es una red de $\mathbb{R}^d$. Dada $a \in A$, hay una relación fundamental entre los valores de a en las valoraciones discretas definidas por los puntos cerrados de Spec$A$ y los valores absolutos de las coordenadas de $a \in \mathbb{R}^r \times \mathbb{C}^s$. La aritmética de A está ligada con cuestiones topológico-analíticas de A en su inmersión en $\mathbb{R}^d$. El discriminante de A, que es el determinante de la métrica de la traza, es igual $\pm 2^s \cdot Vol(\mathbb{R}^d/A)^2$. El teorema de Hermite afirma que solo existe un número finito de cuerpos de números de discriminante fijo dado. El grupo de los ideales de A módulo isomorfismos, Pic$A$, es un grupo finito. Como consecuencia se obtiene que existe una extensión finita de K, L, tal que todo ideal de A extendido al anillo de enteros de L es principal. El grupo de las unidades de A, que son los elementos de norma ± 1, es un grupo finito generado de rango $r + s - 1$ y torsión el grupo de las raíces de la unidad que están en K.

Introducimos la función zeta de Riemann, que es de gran importancia en la Teoría de Números en el cálculo de la distribución de los números primos. Aplicamos la función zeta de Riemann para determinar cuándo dos extensiones de Galois son isomorfas y para demostrar que un sistema de ecuaciones diofánticas tiene soluciones complejas si y solo módulo p admite soluciones enteras, para infinitos primos p.

[1]Sigo unas notas de Juan Antonio Navarrro y Juan Sancho.

6.2. Norma de un ideal

1. Definición: Sea B una k-álgebra finita separable. Dada $b \in B$ consideremos el k-endomorfismo lineal $b\cdot : B \to B$, $b' \mapsto bb'$. Se define $N(b) = \det(b\cdot)$.

Obviamente, $N(1) = 1$ y $N(bb') = N(b)\cdot N(b')$. Sea Σ una k-extensión que trivialice a B y $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{k-alg}(B, \Sigma)$. Por la proposición 2.3.28,

$$\boxed{N(b) = \textstyle\prod_i \sigma_i(b)}$$

Si K es un cuerpo de números, entonces es una $\mathbb{Q}$-álgebra finita separable y tenemos la norma $N : K \to \mathbb{Q}$.

2. Proposición: *Sea A un anillo de enteros y $a \in A$. Se cumple que*

$$|N(a)| = |A/aA|.$$

Demostración. Existe sendas bases de los $\mathbb{Z}$-módulos A y A en las que el endomorfismo $a\cdot : A \to A$ diagonaliza. El determinante de la matriz de $a\cdot$ en estas bases es igual salvo signo a $|A/aA|$, y es igual, salvo signo al determinante del endomorfismo $a\cdot$, porque toda matriz con coeficientes enteros invertible tiene determinante ± 1. □

Denotemos los invertibles (o unidades) de A, A^*.

3. Proposición: *Sea A un anillo de enteros. Entonces, $A^* = \{a \in A : N(a) = \pm 1\}$.*

Demostración. Sea $a \in A$. $|N(a)| = |A/(a)| = 1$ si y solo si $a \in A^*$. □

4. Observación: Dado $a \in A$ sea $p_c(x) = \sum_{i=0}^{n} a_i x^{n-i}$ el polinomio característico de la homotecia $a\cdot : A \to A$. Sabemos que $N(a) = (-1)^n a_n$ y por otra parte $0 = p_c(a) = b\cdot a + a_n$, con $b \in A$. En conclusión, $N(a) = a \cdot c$, con $c \in A$.

5. Corolario: *Sea A un anillo de enteros de cuerpo de fracciones K y sea $d = \dim_{\mathbb{Q}} K$. Dado $c \in \mathbb{N}$, consideremos la acción natural de A^* por multiplicación en el conjunto $\{f \in A : |N(f)| = c\}$. Entonces,*

$$|\{f \in A : |N(f)| = c\}/A^*| \leq c^d.$$

"El número de $f \in A$, salvo multiplicación por invertibles, tales que $|N(f)| = c$ es menor o igual que c^d."

Demostración. Si $|N(f)| = |A/fA| = c$, entonces $c \cdot (A/fA) = 0$, es decir, $c \in fA$. Supongamos $|N(f)| = |N(f')| = c$. Si $\overline{f'} = g\bar{f}$ en A/cA, con $g \in A^*$, entonces $f' = gf + ce$, para cierto $e \in A$, luego $f' \in (f)$ e igualmente $f \in (f')$, es decir, $f' \in f \cdot A^*$. Por tanto, tenemos la inyección

$$\{f \in A : |N(f)| = c\}/A^* \hookrightarrow (A/cA)/A^*, \bar{f} \mapsto \overline{\bar{f}}$$

Por último, A es un $\mathbb{Z}$-módulo libre de rango d, luego A/cA es un $\mathbb{Z}/c\mathbb{Z}$-módulo libre de rango d y $|A/cA| = c^d$.

□

A partir de ahora, supondremos en esta sección que K es un cuerpo de números de anillo de números A.

6. Definición: Dado un ideal fraccionario $I = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$ de K definimos la norma de I, que denotamos $N(I)$, como el número racional positivo

$$N(I) := \prod_i |A/\mathfrak{m}_{x_i}|^{n_i}$$

Evidentemente, N: {Ideales fraccionarios de K} $\to \mathbb{Q}^*$ es un morfismo de grupos.

7. Proposición: *Dado un ideal $\mathfrak{a} \subset A$, entonces $N(\mathfrak{a}) = |A/\mathfrak{a}|$. Dados dos ideales fraccionarios $I' \subseteq I$, se cumple que $N(I')/N(I) = |I/I'|$.*

Demostración. Escribamos $\mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, entonces $A/\mathfrak{a} = \prod_i A/\mathfrak{m}_{x_i}^{n_i}$ y

$$|A/\mathfrak{a}| = \prod_i |A/\mathfrak{m}_{x_i}^{n_i}| = \prod_i |A/\mathfrak{m}_{x_i}|^{n_i} = N(\mathfrak{a}).$$

Existe un ideal $\mathfrak{a} \subseteq A$ tal que $I' = I \cdot \mathfrak{a}$. Además, $I/I' \simeq A/\mathfrak{a}$ porque son A-módulos de torsión y localmente coinciden. Entonces,

$$|I/I'| = |A/\mathfrak{a}| = N(\mathfrak{a}) = N(I')/N(I).$$

□

Por tanto, dado $a \in A$, $N((a)) = |A/(a)| = |N(a)|$.

8. Ejercicio: Sea $0 \neq f \in K$. Prueba que $|N(f)| = N(fA)$.

Solución: Escribamos $f = a/b$, $a, b \in A$. Entonces, $(f) \cdot (b) = (a)$ y

$$N((f)) = N((a))/N((b)) = |N(a)/N(b)| = N(f)$$

9. Ejercicio: Dado un ideal fraccionario I de K, prueba que $N(I) \cdot \mathbb{Z} = \langle N(f) \rangle_{f \in I}$.

Solución: Basta ver que localmente como $\mathbb{Z}$-módulos son iguales. Sea $S \subseteq \mathbb{Z}$ un sistema multiplicativo. Podemos definir igualmente $\mathrm{Div}(A_S)$, los ideales A_S-fraccionarios de K y su norma. Observemos que $N(I)\cdot\mathbb{Z}_S = N(I_S)$ y $\langle N(f)\rangle_{f\in I}\cdot\mathbb{Z}_S = \langle N(f)\rangle_{f\in I_S}$. Sea $S = \mathbb{Z}\backslash(p)$, entonces A_S es un dominio de ideales principales y como I_S es principal se concluye por el ejercicio 6.2.8.

10. Ejercicio: Sea K una $\mathbb{Q}$-extensión de Galois de grupo G. Dado un ideal fraccionario I de K, prueba que

$$N(I)\cdot A = \prod_{\sigma\in G}\sigma(I).$$

Solución: Procédase como en el ejercicio anterior.

6.3. Discriminante

1. Definición: Sea E un $\mathbb{R}$-espacio vectorial de dimensión n. Diremos que un subgrupo aditivo Γ de E es una red si está generado por alguna base $\{e_1,\dots,e_n\}$ del espacio vectorial, es decir, $\Gamma = \mathbb{Z}e_1\oplus\cdots\oplus\mathbb{Z}e_n$ y $E = \mathbb{R}e_1\oplus\cdots\oplus\mathbb{R}e_n$.

Se dice que $E/\Gamma = \{\sum_i \lambda_i\cdot\bar{e}_i \mid 0\le\lambda_i<1\}$ es el paralelepípedo definido por $e_1,\dots,e_n$.

2. Sea $T_2\colon E\times E\to\mathbb{R}$ una métrica simétrica sobre un $\mathbb{R}$-espacio vectorial E de dimensión n. T_2 extiende a $\Lambda^n_{\mathbb{R}}E$:

$$\begin{aligned}T_2(e_1\wedge\cdots\wedge e_n, e'_1\wedge\cdots\wedge e'_n) &:= (i_{e_1}T_2\wedge\cdots\wedge i_{e_n}T_2)(e'_1,\dots,e'_n)\\ &= \sum_{\sigma\in S_n}\mathrm{sign}(\sigma)\cdot T_2(e_1,e'_{\sigma(1)})\cdots T_2(e_n,e'_{\sigma(n)}).\end{aligned}$$

Se cumple que $||e_1\wedge\cdots\wedge e_n||^2 := T_2(e_1\wedge\cdots\wedge e_n, e_1\wedge\cdots\wedge e_n) = \det((T_2(e_i,e_j)))$. Se define el discriminante de $\Gamma = \mathbb{Z}e_1+\cdots+\mathbb{Z}e_n$, Δ_Γ, por

$$\boxed{\Delta_\Gamma := \det((T_2(e_i,e_j)))}$$

3. Sean $e'_1,\dots,e'_n\in E$, con $e'_i = \sum_j\lambda_{ij}e_j$, entonces $e'_1\wedge\cdots\wedge e'_n = \det(\lambda_{ij})\cdot e_1\wedge\cdots\wedge e_n$, y

$$\begin{aligned}\det((T_2(e'_i,e'_j))) &= T_2(e'_1\wedge\cdots\wedge e'_n, e'_1\wedge\cdots\wedge e'_n) = \det(\lambda_{ij})^2\cdot T_2(e_1\wedge\cdots\wedge e_n, e_1\wedge\cdots\wedge e_n)\\ &= \det(\lambda_{ij})^2\cdot\det((T_2(e_i,e_j))).\end{aligned}$$

Si $e'_1,\dots,e'_n$ es otra base del $\mathbb{Z}$-módulo Γ, entonces $\det(\lambda_{ij}) = \pm1$. Por tanto, Δ_Γ no depende de la base de Γ escogida. Si existe una base ortonormal $v_1,\dots,v_n$ de $\mathbb{R}^n$ $v_1,\dots,v_n$ y $e_i = \sum_j\lambda_{ij}v_j$, entonces $\Delta_\Gamma = \det((\lambda_{ij}))^2$.

4. Se define el volumen del paralelepípedo generado por $e_1,\dots,e_n$, por

$$\boxed{Vol(E/\Gamma) := \sqrt{|\Delta_\Gamma|} = \sqrt{|\det(T_2(e_i,e_j))|}}$$

5. Observaciones: Dado un $\mathbb{R}$-espacio vectorial E de dimensión n, si prefijamos una n-coforma $e_1\wedge\cdots\wedge e_n$ y decimos que es de volumen $v>0$, dada otra coforma $e'_1\wedge\cdots\wedge e'_n = \lambda\cdot e_1\wedge\cdots\wedge e_n$ diremos que su volumen es $|\lambda|\cdot v$. Fijado el volumen de un paralelepípedo podemos definir el volumen de cualquier otro paralelepípedo. No es necesario tener definido en E una métrica. Lo mismo decimos con el discriminante.

6. Notación: Seguiremos las siguientes notaciones: K es una $\mathbb{Q}$-extensión finita de cuerpos de grado d, A es el anillo de enteros de K y

$$\{\sigma_1,\dots,\sigma_r,\sigma_{r+1},\dots\sigma_{r+s},\sigma_{r+s+1}=\bar\sigma_{r+1},\dots,\sigma_{r+2s}=\bar\sigma_{r+s}\} = \mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})$$

(donde $\sigma_i(K)\subset\mathbb{R}$ si y solo si $i\le r$ y $\bar\sigma_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación).

Sea $\Gamma\subset K$ un $\mathbb{Z}$-módulo libre de rango d. Consideremos la inclusión canónica

$$\Gamma\hookrightarrow\Gamma\otimes_{\mathbb{Z}}\mathbb{R} = K\otimes_{\mathbb{Q}}\mathbb{R} = \mathbb{R}^r\oplus\mathbb{C}^s =: \mathscr{O}_\infty,\ a\mapsto(\sigma_1(a),\dots,\sigma_r(a),\sigma_{r+1}(a),\dots,\sigma_{r+s}(a))$$

Γ es una red de $\mathscr{O}_\infty$. *Todo anillo de enteros, como todo ideal fraccionario no nulo son redes de* $\mathscr{O}_\infty$. Sea $\{a_1,\dots,a_d\}$ una base de $\Gamma\subset K$.

En $\mathscr{O}_\infty$ tenemos la métrica de la traza T_2 (que coincide con la métrica de la traza de K, tras el cambio de cuerpo base $\mathbb{Q}\hookrightarrow\mathbb{R}$).

7. Si $\Gamma\cdot\Gamma\subseteq\Gamma$, entonces $T_2(a_i,a_j)$ es igual a la traza del endomorfismo de $\mathbb{Z}$-módulos $(a_ia_j)\cdot:\Gamma\to\Gamma$, luego es un número entero y Δ_Γ es un número entero.

8. Como $(T_2(a_i,a_j)) = (\mathrm{tr}(a_ia_j)) = (\sum_{k=1}^d\sigma_k(a_ia_j)) = (\sigma_i(a_j))^t\cdot(\sigma_i(a_j))$, entonces

$$\boxed{\Delta_\Gamma = \det((\sigma_i(a_j)))^2}$$

(donde $(\sigma_i(a_j))$ es una matriz cuadrada de números complejos de orden d) y

$$\boxed{Vol(\mathscr{O}_\infty/\Gamma) = \sqrt{|\Delta_\Gamma|} = |\det((\sigma_i(a_j)))|}$$

9. En $\mathcal{O}_\infty$ tenemos la métrica de la traza T_2 y la métrica euclídea estándar S_2. Se cumple que $\det(T_2) = (-4)^s \cdot \det(S_2)$ y por tanto el volumen de los paralelepípedos con la métrica de la traza es 2^s-veces el volumen de los paralelepípedos con la métrica euclídea estándar.

Consideremos la matriz de números reales de filas los vectores $(\sigma_1(a_j), \dots, \sigma_{r+s}(a_j)) \in \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$. Entonces

$$\boxed{\Delta_\Gamma = (-4)^s \det(\sigma_i(a_j))^2} \quad \text{y} \quad \boxed{Vol(\mathcal{O}_\infty/\Gamma) = 2^s |\det(\sigma_i(a_j))|}.$$

10. Ejercicio: Calcula el discriminante de $\mathbb{Z}[i]$.

11. Ejercicio: Sea A un anillo de números de cuerpo de fracciones K, supongamos que $i \notin K$ y sea n el rango del $\mathbb{Z}$-módulo A. Demuestra que $\Delta_{A[i]} = (-4)^n \cdot \Delta_A^2$.

12. Ejemplo: Sea $\alpha \in \mathbb{C}$ entero sobre $\mathbb{Z}$ y sea $p(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ el polinomio mínimo anulador. Sea $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(p(x))$ y $\mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) = \{\sigma_i\}$. Las raíces de $p(x)$ son $\{\alpha_i := \sigma_i(\alpha)\}_i$.

Una $\mathbb{Z}$-base de $\mathbb{Z}[\alpha]$ es $\{1, \alpha, \dots, \alpha^{d-1}\}$. Recordemos que el valor del determinante de Vandermonde es $\det(x_i^j) = \prod_{i<j}(x_i - x_j)$. Entonces,

$$\Delta_{\mathbb{Z}[\alpha]} = \det((\sigma_i(\alpha^j)))^2 = \det((\alpha_i^j))^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta(p(x)).$$

$\Delta(p(x))$ es igual[2] al determinante de la homotecia

$$h_{p(x)\cdot} \colon \mathbb{Q}[x]/(p(x)) \to \mathbb{Q}[x]/(p(x)),$$

multiplicado por $(-1)^{\frac{d(d-1)}{2}}$.

Calculemos el discriminante de $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$, con p primo distinto de 2. Hemos probado que $\Delta_{\mathbb{Z}[e^{\frac{2\pi i}{p}}]} = \Delta(\Phi_p(x))$. Observemos que $x^p - 1 = (x-1)\cdot\Phi_p(x)$, entonces

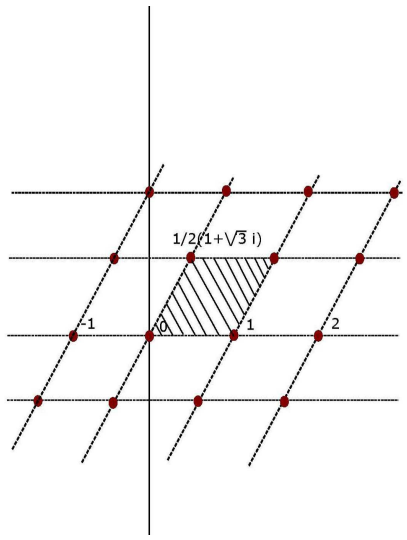
$$\Delta(x^p - 1) = \Phi_p(1)^2 \cdot \Delta(\Phi_p(x)) = p^2 \cdot \Delta(\Phi_p(x)),$$

$\Delta(x^p - 1)$ es igual al determinante de $h_{p\cdot x^{p-1}} \colon \mathbb{Q}[x]/(x^p - 1) \to \mathbb{Q}[x]/(x^p - 1)$, que es p^p, multiplicado por $(-1)^{\frac{p\cdot(p-1)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Luego,

$$\Delta_{\mathbb{Z}[e^{\frac{2\pi i}{p}}]} = \Delta(\Phi_p(x)) = (-1)^{\frac{(p-1)}{2}} \cdot p^{p-2}.$$

[2] La demostración se basa en que se puede suponer por cambio de cuerpo base que todas las raíces están en el cuerpo base y en el teorema chino de los restos.

13. Ejemplo: Consideremos el anillo de enteros $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$.



Vamos a considerar como red $\Gamma = A$. Una base del $\mathbb{Z}$-módulo A es $\{1, 1/2(1+\sqrt{-3})\}$. Tenemos que el cuerpo de números es $K = \mathbb{Q}[\sqrt{-3}]$, $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{C} = \mathbb{R}^2$ y $\mathrm{Hom}_{anillos}(K, \mathbb{C}) = \{I, c \circ I\}$, donde I es la inclusión obvia y c es la conjugación de $\mathbb{C}$. Por tanto,

$$\Delta_A = (-4)^1 \begin{vmatrix} 1 & 1/2 \\ 0 & 1/2\sqrt{3} \end{vmatrix}^2 = -3.$$

y

$$Vol(\mathbb{R}^2/A) = 2^1 \begin{vmatrix} 1 & 1/2 \\ 0 & 1/2\sqrt{3} \end{vmatrix} = \sqrt{3}.$$

Por otra parte, también

$$\Delta_A = \begin{vmatrix} 1 & 1/2 + 1/2\sqrt{-3} \\ 1 & 1/2 - 1/2\sqrt{-3} \end{vmatrix}^2 = -3.$$

14. Sean $\Gamma' \subseteq \Gamma$ dos redes. Existen bases en $\{e'_1, \ldots, e'_n\}$, $\{e_1, \ldots, e_n\}$ en Γ' y Γ de modo que $e'_i = \lambda_i \cdot e_i$, para ciertos $\lambda_i \in \mathbb{Z}$. Entonces, $\Delta_{\Gamma'} = (\lambda_1 \cdots \lambda_n)^2 \cdot \Delta_\Gamma$. Observemos que $\Gamma/\Gamma' \simeq \mathbb{Z}/\lambda_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\lambda_n\mathbb{Z}$, luego

$$\boxed{\Delta_{\Gamma'} = |\Gamma/\Gamma'|^2 \cdot \Delta_\Gamma}$$

Además, $\Delta_{\Gamma'} = \Delta_\Gamma$ si y solo si $\Gamma = \Gamma'$.

Si $I' \subset I$ son dos ideales fraccionarios, entonces $Vol(\mathscr{O}_\infty/I') = |I/I'| \cdot Vol(\mathscr{O}_\infty/I) \overset{6.2.7}{=} \frac{N(I')}{N(I)} \cdot Vol(\mathscr{O}_\infty/I)$.

15. Proposición: *Si I es un ideal fraccionario, entonces*

$$\boxed{Vol(\mathscr{O}_\infty/I) = N(I) \cdot \sqrt{|\Delta_A|}}$$

Demostración. Sean $\mathfrak{a}$, $\mathfrak{b} \subseteq A$ ideales tales que $I = \mathfrak{a} \cdot \mathfrak{b}^{-1}$ (luego, $I \subseteq \mathfrak{b}^{-1}$ y $A \subseteq \mathfrak{b}^{-1}$). Entonces,

$$Vol(\mathscr{O}_\infty/I) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot Vol(\mathscr{O}_\infty/\mathfrak{b}^{-1}) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot N(\mathfrak{b}^{-1}) \cdot Vol(\mathscr{O}_\infty/A) = N(I) \cdot \sqrt{|\Delta_A|}.$$

□

6.4. Desingularización vía el discriminante

1. Proposición: *Sea A un anillo de números, consideremos el morfismo finito $\mathbb{Z} \to A$ y el morfismo inducido en espectros $\pi\colon \operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$. Entonces,*

$$\{\textit{Puntos rama de } \pi\} = (\Delta_A)_0.$$

Demostración. Sea $\mathfrak{m}_x = (p)$. Por definición, x es un punto rama si y solo si A/pA no es una $\mathbb{Z}/p\mathbb{Z}$-álgebra separable, es decir, $\Delta_{A/pA} = \overline{\Delta_A} \in \mathbb{Z}/p\mathbb{Z}$ es nulo, es decir, $x \in (\Delta_A)_0$. □

2. Corolario: *Sea A un anillo de números. Sigamos las notaciones de la proposición anterior. Entonces,*

$$\{\textit{Puntos singulares de } \operatorname{Spec} A\} \subseteq \pi^{-1}(\{\textit{Puntos rama de } \pi\}) = (\Delta_A)_0.$$

Podemos demostrar de nuevo el siguiente teorema.

3. Teorema: *Sea K un cuerpo de números. El anillo de números de K (es decir, el cierre entero de $\mathbb{Z}$ en K) es un anillo de números (es decir, una $\mathbb{Z}$-álgebra finita íntegra).*

Demostración. Podemos escribir $K = \mathbb{Q}(\xi_1, \ldots, \xi_n)$, con $\xi_1, \ldots, \xi_n$ enteros sobre $\mathbb{Z}$. Sea $A := \mathbb{Z}[\xi_1, \ldots, \xi_n]$, cuyo cuerpo de fracciones es K y sea Δ_A su discriminante. Sea $a_1 \in K$ un elemento entero, que no pertenece a A y sea $A_1 = A[a_1]$. Tenemos el morfismo finito $A \hookrightarrow A_1$ y $(\Delta_A) \underset{\neq}{\subset} (\Delta_{A_1})$. Igualmente, sea $a_2 \in K$ un elemento entero, que no pertenece a A_1 y sea $A_2 = A_1[a_2]$. Tenemos el morfismo finito $A_1 \hookrightarrow A_2$ y $(\Delta_{A_1}) \underset{\neq}{\subset} (\Delta_{A_2})$ Obviamente este proceso ha de terminar en un número finito m de pasos y lo hará cuando A_m sea el anillo de números de K. Observemos que A_m es un anillo de números.

□

4. Definición: Sea K un cuerpo de números. Se define el discriminante de K, que denotamos por Δ_K, como el discriminante del anillo de números de K.

5. Corolario: *Sea $K \hookrightarrow K'$ una extensión finita de cuerpos de números y A y A' los anillos de números de K y K', respectivamente. Entonces, el morfismo $A \hookrightarrow A'$ es finito.*

Demostración. A' es un $\mathbb{Z}$-módulo finito generado, luego es un A-módulo finito generado.

□

6. Corolario: *Sea A un anillo de números. Se cumple que*

$$\{\textit{Puntos singulares de } \operatorname{Spec} A\} \subseteq \bigcup_{p^2|\Delta_A} (p)_0.$$

Demostración. Sea $\bar{A}$ el anillo de números de $K = A_{A\setminus\{0\}}$. $\bar{A}/A$ es un grupo abeliano finito, luego isomorfo a $\oplus_{ij}\mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}$, con p_i primos. Sea $y \in \operatorname{Spec}_{max} A$ un punto singular singular y $\mathfrak{m}_y \cap \mathbb{Z} = (p) =: \mathfrak{m}_x$, entonces $(\bar{A}/A)_y \neq 0$, luego $(\bar{A}/A)_x \neq 0$ y p divide a $|\bar{A}/A|$. Recordemos que $\Delta_A = |\bar{A}/A|^2 \cdot \Delta_{\bar{A}}$, luego p^2 divide a Δ_A. □

7. Ejemplo: Sea $\alpha \in \mathbb{C}$ raíz de un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2, y $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(p(x))$. Calculemos el anillo de números A de K.

$K = \mathbb{Q}[\sqrt{m}]$, con $m \in \mathbb{Q}$. Podemos escribir $m = r^2 \cdot n$, donde n es un número entero sin factores cuadráticos (no existe ningún número primo p tal que p^2 divida a n). Entonces, $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$. El discriminante de $x^2 - n$ es $4n$, luego $\Delta_{\mathbb{Z}[\sqrt{n}]} = 4 \cdot n$. Tenemos que $\mathbb{Z}[\sqrt{n}] \subseteq A$ y

$$\Delta_{\mathbb{Z}[\sqrt{n}]} = |A/\mathbb{Z}[\sqrt{n}]|^2 \cdot \Delta_A.$$

Si $\mathbb{Z}[\sqrt{n}] \neq A$, entonces $\Delta_A = n$ y $|A/\mathbb{Z}[\sqrt{n}]| = 2$. Por el Corolario 6.4.6, los únicos puntos singulares de $\mathbb{Z}[\sqrt{n}]$ posibles están en $(2)_0$. Ahora bien,

$$(2)_0 = \operatorname{Spec} \mathbb{Z}[\sqrt{n}]/(2) = \operatorname{Spec} \mathbb{Z}/2\mathbb{Z}[x]/(x^2 - n) = \begin{cases} (\bar{x}) \text{ si } n \text{ es par} \\ (\bar{x}+1) \text{ si } n \text{ es impar} \end{cases}$$

Es decir, $(2)_0$ es $\{(2, \sqrt{n})\}$ si n es par ó $\{(2, \sqrt{n}+1)\}$ si n es impar.

Sea $\mathfrak{m}_y = (2, x) \subset \mathbb{Z}[x]$. Si n es par, entonces $d_y(x^2 - n) = d_y 2 \neq 0$, luego $(\bar{2}, \bar{x}) \subset \mathbb{Z}[x]/(x^2 - n)$ es no singular. Es decir, $(2, \sqrt{n}) \subset \mathbb{Z}[\sqrt{n}]$ es no singular. Si n es impar, sea $\mathfrak{m}_y = (2, x+1) \subset \mathbb{Z}[x]$, entonces

$$d_y(x^2 - n) = d_y((x+1-1)^2 - n) = d_y((x+1)^2 - 2(x+1) + 1 - n) = d_y(1-n) = 0$$

si y solo si $1 - n$ es múltiplo de 4. Es decir, $(2, \sqrt{n}+1) \subset \mathbb{Z}[\sqrt{n}]$ es singular si y solo si $1 - n$ es múltiplo de 4. En este caso, observemos que $\frac{\sqrt{n}+1}{2}$ es entero porque

$$0 = \frac{(\sqrt{n}+1)^2 - 2(\sqrt{n}+1) + 1 - n}{4} = (\frac{\sqrt{n}+1}{2})^2 - \frac{\sqrt{n}+1}{2} + \frac{1-n}{4}$$

Por tanto, $A = \mathbb{Z}[\frac{\sqrt{n}+1}{2}]$.

Demostremos de nuevo que el anillo de números de un cuerpo de números es un anillo de números precisando en qué $\mathbb{Z}$-módulo finito generado está incluido.

8. Teorema: *Sea K un cuerpo de números y A su anillo de números. Sea $\alpha_1,\ldots,\alpha_n \in A$ una $\mathbb{Q}$-base de K y escribamos $\Delta_{\mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n} = r^2\cdot s$ de modo que ningún primo al cuadrado divida a s. Entonces,*

$$A \subseteq \frac{\mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n}{r}.$$

Demostración. Denotemos $M = \mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n$ y consideremos la inclusión $M \hookrightarrow A$. Existe una $\mathbb{Z}$-base $v_1,\ldots,v_n$ de M, de modo que $\frac{1}{d_1}\cdot v_1,\ldots,\frac{1}{d_n}\cdot v_n$ es una $\mathbb{Z}$-base de A, para ciertos números naturales $d_1,\ldots,d_n$. Observemos que $|A/M| = d_1\cdots d_n$, luego $\Delta_M = |A/M|^2\cdot\Delta_A = d_1^2\cdots d_n^2\cdot\Delta_A$ y por tanto $d_1\cdots d_n$ divide a r. Entonces,

$$A = \mathbb{Z}\cdot\frac{1}{d_1}\cdot v_1+\cdots+\mathbb{Z}\cdot\frac{1}{d_n}\cdot v_n \subseteq \mathbb{Z}\cdot\frac{1}{r}\cdot v_1+\cdots+\mathbb{Z}\cdot\frac{1}{r}\cdot v_n = \frac{1}{r}\cdot M.$$

□

9. Ejercicio: Sea $n\in\mathbb{Z}$, con $n\neq 0,1$ y sin factores cuadráticos. Demuestra que el discriminante de $K=\mathbb{Q}[\sqrt{n}]$ es n si $n\equiv 1 \mod 4$, y es $4n$ si $n\equiv 2,3 \mod 4$.

10. Ejercicio: Sea $n\in\mathbb{Z}$, con $n\neq 0,1$ y sin factores cuadráticos. Sea Δ el discriminante de $\mathbb{Q}[\sqrt{n}]$. Prueba que el anillo de enteros de $\mathbb{Q}[\sqrt{n}]$ es igual a $\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$.

Demos un algoritmo para el cálculo del anillo de números de un cuerpo de números.

11. Teorema: *Sea K un cuerpo de números y $\{a_1,\ldots,a_n\}$ una $\mathbb{Q}$-base de K, formada por elementos enteros. Sea M el $\mathbb{Z}$-módulo generado por la base. Si M no es igual al anillo de números de K, existe un primo p tal que p^2 divide a Δ_M y números naturales $0\leq r_1,\ldots,r_s<p$, para un $s<n$ de modo que $a=\frac{1}{p}\cdot(r_1a_1+\cdots+r_sa_s+a_{s+1})$ es entero. Si M' es el $\mathbb{Z}$-módulo generado por $\{a_1,\ldots,a_s,a,a_{s+2},\ldots,a_n\}$ entonces $\Delta_{M'}=\frac{\Delta_M}{p^2}$.*

Demostración. Sea A el anillo de números de K. Escribamos $\Delta_M = u^2\cdot v$, con $u,v\in\mathbb{N}$ y de modo que ningún primo al cuadrado divida a v. Sabemos que $M\subseteq A\subseteq\frac{M}{u}$. Si p es un primo que no divide a u (es decir, p^2 no divide a Δ_M) y denotamos $\mathfrak{m}_x=(p)$, entonces $M_x=(\frac{M}{u})_x$ y $M_x=A_x$. Sea $\mathfrak{m}_x=(p)$, tal que $M_x\neq A_x$, luego p^2 divide Δ_M o equivalentemente p divide a u. Tenemos, $M_x\subsetneq A_x\subseteq(\frac{M}{u})_x=\frac{1}{p^n}\cdot M_x$ (con $n=v_x(u)$). Entonces, existe $b=\sum_i\frac{m_i}{p^n}\cdot a_i\in A\setminus M$, con $m=\min\{v_x(\frac{m_i}{p^n})\}<0$. Entonces, $c=p^{-m-1}\cdot b\in A\cap\frac{1}{p}\cdot M$ y $c\notin M$. Escribamos $c=\sum_i\frac{n_i}{p}\cdot a_i$. Sea $s+1$ máximo tal que $n_{s+1}\notin(p)$. Sea $t\in\mathbb{N}$ tal que $t\cdot n_{s+1}=1 \mod p$. Existe $d\in M$ tal que $a=t\cdot c-d=\frac{1}{p}\cdot(r_1a_1+\cdots+r_sa_s+a_{s+1})$ es el entero buscado.

Por último, consideremos las inclusiones

$$M=\mathbb{Z}\cdot a_1+\cdots+\mathbb{Z}\cdot a_n=\mathbb{Z}\cdot a_1+\cdots+\underset{s+1}{\mathbb{Z}\cdot pa}+\cdots+\mathbb{Z}\cdot a_n\hookrightarrow\mathbb{Z}\cdot a_1+\cdots+\underset{s+1}{\mathbb{Z}\cdot a}+\cdots+\mathbb{Z}\cdot a_n=M'$$

Entonces, $\Delta_M = |M'/M|^2 \cdot \Delta_{M'} = p^2 \cdot \Delta_{M'}$.

□

En el teorema hemos pasado de un $\mathbb{Z}$-módulo M de elementos enteros de discriminante Δ_M a otro, M', de discriminante $\Delta_{M'} = \frac{1}{p^2} \cdot \Delta_M$. Si repetimos este proceso con M' y así sucesivamente este proceso ha de terminar y lo hará cuando M_n sea el anillo de números de K. Sólo un número finito de primos p cumplen que p^2 divide a Δ_M y solo un número finito de elementos $a \in K$ son de la forma escrita en el teorema. El proceso termina cuando para todo primo p tal que p^2 divide a Δ_{M_n}, todos los a de la forma escrita no son elementos enteros de K.

12. Ejemplo: Consideremos el ejemplo de Dedekind: calculemos el anillo de números de $K := \mathbb{Q}[x]/(x^3 + x^2 - 2x + 8)$. Sea $A' := \mathbb{Z}[x]/(x^3 + x^2 - 2x + 8)$. Se puede comprobar que $\Delta_{A'} = 2^2 \cdot 503$. El primo considerado en el teorema anterior, con $M := A'$, solo puede ser $p = 2$. El ideal primo $\mathfrak{m}_y = (2, x)$ es singular, entonces A' no es el anillo de números de K. Si tenemos un $\mathbb{Z}$-submódulo $M' \subset K$ formado por elementos enteros tal que $A' \subsetneq M'$, como $\Delta_{M'} = |M'/A|^2 \cdot \Delta_{A'}$, entonces $\Delta_{M'} = 503$, luego M' es el anillo de números de K.

Consideremos la $\mathbb{Z}$-base $\{1, x, x^2\}$ de A'. Por el teorema anterior, uno de lo siguientes elementos de K

$$1/2, (1+x)/2, x/2, (1+x+x^2)/2, (1+x^2)/2, (x+x^2)/2, x^2/2$$

es entero. Dividiendo $x^3 + x^2 - 2x + 8 = 0$ por 4, tenemos que

$$0 = (x/2)^2 x + (x/2)^2 - (x/2) + 2 = (x/2) = (x/2)^2(x+1) - (x/2) + 2.$$

Multiplicando por $x+1$, $(\frac{x^2+x}{2})^2 - \frac{x^2+x}{2} + 2(x+1) = 0$, luego $\frac{x^2+x}{2}$ es entero sobre A' y por tanto entero sobre $\mathbb{Z}$, es decir, es un elemento entero de K. Por tanto,

$$\mathbb{Z} \oplus \mathbb{Z} \cdot x \oplus \mathbb{Z} \cdot \frac{x^2 + x}{2}$$

es el anillo de números de K.

6.5. Valores absolutos arquimedianos

1. Definición: Un valor absoluto sobre un anillo A es una aplicación $||: A \to \mathbb{R}$ que cumple la siguientes condiciones para todo $a, b \in A$,

1. $|a| \geq 0$ y $|a| = 0$ si y solo si $a = 0$.

2. *Desigualdad triangular:* $|a+b| \leq |a|+|b|$.

3. $|ab| = |a||b|$.

Es inmediato comprobar que todo valor absoluto cumple: $|1| = 1$ y $|-a| = |a|$. También $|n| \leq n$ para todo $n \in \mathbb{N}$. Todo anillo que posea un valor absoluto es necesariamente íntegro, y el valor absoluto extiende de modo único al cuerpo de fracciones.

La aplicación $|\,|\colon A \to \mathbb{R}$ tal que $|a| := 1$ para todo $a \in A\setminus\{0\}$ y que cumple que $|0| := 0$ se denomina valor absoluto trivial.

2. Ejemplos: $|\,|\colon \mathbb{Q} \to \mathbb{R}$, $|a| := a$ si $a > 0$ y $|a| := -a$ si $a < 0$ es un valor absoluto.

Sea $p \in \mathbb{N}$ primo. La aplicación $|\,|\colon \mathbb{Q} \to \mathbb{R}$, $|a| := e^{-v_p(a)}$ es un valor absoluto.

3. Definición: Dos valores absolutos $|\,|_1$ y $|\,|_2$ sobre un cuerpo K se dicen equivalentes si existe un número real $r > 0$ tal que $|a|_1 = |a|_2^r$, para todo $a \in K$.

Todo valor absoluto $|\,|$ define una distancia $d\colon d(a,b) := |a-b|$. Por tanto, todo valor absoluto define una topología.

4. Proposición: *Dos valores absolutos sobre un cuerpo K son equivalentes si y solo si inducen la misma topología.*

Demostración. Evidentemente, si dos valores absolutos son equivalentes definen la misma topología. Veamos el recíproco.

Dejemos al lector la consideración de los valores triviales (que se caracterizan por inducir la topología discreta). La topología determina la bola abierta unidad $B(0,1)$ de un valor absoluto:

$$|x| < 1 \iff \lim_{n\to\infty} x^n = 0$$

Luego, si dos valores absolutos definen la misma topología sus respectivas bolas unidad son iguales.

Fijemos un punto x con $|x| > 1$, es decir, $1/x \in B(0,1)$. Dado y, tendremos que $|y| = |x|^\alpha$, para cierto número real α. Observemos que

$$\frac{n}{m} < \alpha \iff \frac{|x|^{\frac{n}{m}}}{|y|} < 1 \iff \left|\frac{x^n}{y^m}\right| < 1 \iff \frac{x^n}{y^m} \in B(0,1)$$

Por tanto, si $|\,|'$ es equivalente a $|\,|$, tenemos que $|y|' = |x|'^\alpha$. Si definimos $r := \log_{|x|} |x|'$, $|y|' = |x|'^\alpha = (|x|^r)^\alpha = |y|^r$, para todo y. □

5. Definición: Un valor absoluto $|\,|\colon A \to \mathbb{R}$ se dice arquimediano si $|\,|$ sobre $\mathbb{N}$ no está acotada, es decir, para toda constante $C > 0$ existe un número natural n tal que $|n| > C$.

Evidentemente, todo cuerpo dotado de un valor absoluto arquimediano debe ser de característica cero.

6. Lema: *Sea* $||:\mathbb{N}\to\mathbb{R}$ *un valor absoluto. Si* $||$ *es arquimediano, entonces* $|d|>1$ *para todo* $d>1$. *Si* $||$ *no es arquimediano, entonces* $|d|\leq 1$ *para todo* $d\in\mathbb{N}$.

Demostración. Supongamos que $|d|\leq 1$, para algún $d>1$. Desarrollemos cualquier número natural n en base d,

$$n=a_0+a_1d+\ldots+a_kd^k,\qquad \text{con } 0\leq a_i<d.$$

De donde

$$|n|\leq d+d|d|+\ldots+d|d|^k\leq d(1+k)\leq d(1+\log_d n).$$

Por tanto,

$$|n^k|\leq d(1+k\log_d n).$$

Por otra parte,

$$|n^k|=|n|^k.$$

Entonces,

$$1\leq \lim_{k\to\infty}\frac{d(1+k\log_d n)}{|n|^k}=0$$

si $|n|>1$. Por tanto, $|n|\leq 1$, para todo n.

Supongamos $|d|>1$, para un $d>1$. Entonces, $|d^m|=|d|^m>>0$, para $m>>0$ y $||$ es arquimediano.

□

7. Primer teorema de Ostrowski, 1917: *Todo valor absoluto arquimediano sobre* $\mathbb{Q}$ *es equivalente al valor absoluto usual.*

Demostración. Sea $d>1$ un natural; por el lema sabemos que $|d|>1$, así que $|d|=d^\alpha$ para cierto $\alpha>0$. Sustituyendo d por una potencia suya podemos suponer que $|d|>2$. Desarrollemos cualquier otro natural n en base d,

$$n=a_0+a_1d+\cdots+a_kd^k,\ \ 0\leq a_i<d,$$

de donde

$$\begin{aligned}|n|&\leq d+d|d|+\cdots+d|d|^k=d(1+|d|+\cdots+|d|^k)=d\cdot\frac{|d|^{k+1}-1}{|d|-1}\\&\leq d|d|^{k+1}\leq d|d|^{(log_d n)+1}=d(d^\alpha)^{log_d n+1}=d^{\alpha+1}n^\alpha,\end{aligned}$$

Sustituyendo en esta desigualdad n por n^k, sacando raíz k-ésima y tomado límite para $k \to \infty$, resulta $|n| \leq n^\alpha$. Si esta desigualdad fuera estricta para algún natural m, digamos $|m| = m^\beta$ con $\beta < \alpha$, entonces sustituyendo d por m en el argumento de arriba obtendriamos la desigualdad $|n| \leq n^\beta$ para todo $n \in \mathbb{N}$, lo que contradice $|d| = d^\alpha$.

□

Vamos ahora a determinar los valores absolutos arquimedianos sobre un cuerpo de números K (extensión finita de $\mathbb{Q}$).

8. Definición: Sea K un cuerpo dotado de un valor absoluto $||$. Una norma sobre un K-espacio vectorial E es una aplicación $||\,||: E \to \mathbb{R}$ que cumple las siguientes propiedades:

1. $||e|| \geq 0$ y $||e|| = 0$ si y solo si $e = 0$.
2. $||e_1 + e_2|| \leq ||e_1|| + ||e_2||$ (desigualdad triangular).
3. $||\lambda e|| = |\lambda| \cdot ||e||$.

9. Ejemplo: Si E es un K-espacio vectorial con una base finita $\{e_1, \ldots, e_n\}$, se define la *norma infinita* como sigue:

$$||\sum_i \lambda_i e_i|| := \text{máx}\{|\lambda_1|, \ldots, |\lambda_n|\}.$$

La norma infinita define en E la topología producto respecto de la identificación $E = K^n$, $\sum_i \lambda_i e_i \mapsto (\lambda_1, \ldots, \lambda_n)$. Toda aplicación K-lineal $E \to E$ es continua para la norma infinita. La norma infinita es la más fina sobre E: En efecto, si $||\,||'$ es otra norma, consideremos la constante $C := \text{máx}\{||e_1||', \ldots, ||e_n)||'\}$; entonces se cumple

$$||e||' = ||\sum_i \lambda_i e_i||' \leq \sum_i |\lambda_i| ||e_i||' \leq \sum_i |\lambda_i| C = C \cdot n \cdot ||e||.$$

10. Proposición: *Si F es un subespacio vectorial cerrado de un espacio vectorial normado $(E, ||\,||)$, entonces la aplicación $||\,||: E/F \to \mathbb{R}$ definida por*

$$||\bar{e}|| := \text{ínf}\{||e'||,\ \forall\ e' \in e + F\}$$

es una norma sobre E/F, y la proyección natural $E \to E/F$ es continua.

11. Proposición: *Sean $(K, ||)$ un cuerpo completo y E un K-espacio vectorial de dimensión finita. Todas las normas sobre E son topológicamente equivalentes y completas.*

Demostración. Es rutinario comprobar que E es completo para la norma infinita $||||$, y por tanto también es completo para cualquier otra norma topológicamente equivalente a la norma infinita.

Ya sabemos que cualquier norma $||||'$ sobre E es menos fina que la norma infinita. Para la afirmación inversa procedamos por inducción sobre $n = \dim_K E$. Por hipótesis de inducción, todo subespacio de E de dimensión menor que n es completo para la norma $||||'$ luego también es cerrado. Por tanto, las proyecciones $\pi_j : E \to Ke_j$, $\pi_j(\sum_i \lambda_i e_i) := \lambda_j e_j$, son continuas tomando en E la norma $||||'$ y en Ke_j la norma cociente (que equivale, como todas, a la norma infinita). Por tanto, la aplicación identidad

$$(E, ||||') \xrightarrow{\oplus_j \pi_j} (\oplus_j Ke_j = E, ||||)$$

es continua. Luego la topología definida por $||||$ es menos fina que la de $||||'$. □

12. Teorema: *Sea K un cuerpo de números. Dado un valor absoluto arquimediano $||$ sobre K, existe un morfismo de cuerpos $K \to \mathbb{C}$, único salvo conjugación compleja, tal que $||$ es equivalente a la restricción a K del valor absoluto usual de $\mathbb{C}$. Por tanto,*

$$\left\{ \begin{array}{l} \textit{valores absolutos arquimedianos} \\ \textit{sobre } K\textit{, módulo equivalencia} \end{array} \right\} = \left\{ \begin{array}{l} \textit{morfismos de anillos } K \to \mathbb{C} \\ \textit{módulo conjugación} \end{array} \right\}$$

$$||_{[\sigma]} \longmapsto [\sigma], \quad (\sigma : K \to \mathbb{C})$$

$$|f|_{[\sigma]} := |\sigma(f)|.$$

Demostración. Vamos a ver que el completado $\hat{K}$ de K se indentifica con $\mathbb{R}$ o con $\mathbb{C}$, de modo único salvo conjugación, como cuerpos y espacios topológicos. En tal caso, si denotamos por σ la composición $K \hookrightarrow \hat{K} \subset \mathbb{C}$, tenemos que la topología definida en K por $||$ es igual a la inicial por el morfismo σ, es decir, $||$ y $||_{[\sigma]}$ definen la misma topología, luego son equivalentes.

Sea $\hat{\mathbb{Q}} \to \hat{K}$ la compleción de la extensión $\mathbb{Q} \to K$ respecto del valor absoluto $||$. Como la restricción de $||$ a $\mathbb{Q}$ es equivalente al valor absoluto usual (por 6.5.7), se tiene $\hat{\mathbb{Q}} = \mathbb{R}$, dotado $\mathbb{R}$ de un valor absoluto $||$ equivalente al usual. Escribamos $K = \mathbb{Q}(a_1, ...a_n)$. El subcuerpo $\mathbb{R}(a_1, ..., a_n) \subseteq \hat{K}$ es una extensión finita de $\mathbb{R}$, así que es completo respecto $||$ por 6.5.11, luego es un cerrado de $\hat{K}$. Como este cerrado es denso en $\hat{K}$ (por contener a K), se concluye que $\mathbb{R}(a_1, ..., a_n) = \hat{K}$, es decir, $\hat{K}$ es una extensión finita de $\mathbb{R}$. Por tanto, $\hat{K} = \mathbb{R}$ ó $\hat{K} = \mathbb{C}$. Si $\hat{K} = \mathbb{R} = \hat{\mathbb{Q}}$ entonces, como hemos dicho ya, la topología definida por $||_{\hat{K}}$ en $\hat{K} = \mathbb{R}$ es la usual. En el segundo caso, la topología definida por $||_{\hat{K}}$ sobre $\hat{K} = \mathbb{C}$ es igual a la usual de $\mathbb{C}$, porque $||_{\hat{K}}$ es una norma del $\mathbb{R}$-espacio vectorial $\hat{K} = \mathbb{C}$,

y todas las normas de $\mathbb{C} = \mathbb{R}^2$ definen la misma topología (la usual). En conclusión, tenemos $K \hookrightarrow \mathbb{C}$ y la topología definida por el valor absoluto de $\mathbb{C}$ en K es igual a la topología definida definida por $||$. En cuanto a la unicidad: Supongamos que tenemos dos morfismos $\sigma_1, \sigma_2 \colon K \hookrightarrow \mathbb{C}$ de modo que la topología inicial de K es la definida por $||$. Si $\hat{K} = \mathbb{R}$ entonces $\sigma_1 = \sigma_2$. Si $\hat{\sigma}_1, \hat{\sigma}_2 \colon \hat{K} \to \mathbb{C}$ son isomorfismos de $\mathbb{R}$-álgebras, entonces $\hat{\sigma}_1 = \hat{\sigma}_2$ ó $\hat{\sigma}_1 = c \circ \hat{\sigma}_2$ (donde c es el morfismo conjugación), luego $\sigma_1 = \sigma_2$ ó $\sigma_1 = c \circ \sigma_2$. □

13. Observación: $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ porque es una $\mathbb{R}$-álgebra finita separable. Luego,

$$\mathrm{Hom}_{Anillos}(K, \mathbb{C})/Conj. = \mathrm{Hom}_{\mathbb{R}}(K \otimes_{\mathbb{Q}} \mathbb{R}, \mathbb{C})/Conj. = \mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R}).$$

Cada $y \in \mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R}K)$, se corresponde con el morfismo $K \to K \otimes_{\mathbb{Q}} \mathbb{R}/\mathfrak{m}_y = \mathscr{C}$, donde $\mathscr{C} = \mathbb{R}$ o $\mathbb{C}$.

6.6. Valores absolutos no arquimedianos y valoraciones

1. Proposición: *Un valor absoluto $|| : A \to \mathbb{R}$ es no arquimediano si y solo si verifica la desigualdad ultramétrica: $|a + b| \leq \max\{|a|, |b|\}$.*

Demostración. $\Rightarrow$) Para todo natural n se cumple $|n| \leq 1$, pues si para algún natural fuera $|n| > 1$ entonces $|n^m| = |n|^m$ no sería acotado. Dados $a, b \in A$ con $|a| \leq |b|$, se tiene

$$|a+b|^n = |(a+b)^n| \leq |a|^n + |n||a|^{n-1}|b| + \cdots + |n||a||b|^{n-1} + |b|^n \leq (1+n)|b|^n,$$

de donde

$$|a+b| \leq (1+n)^{1/n}|b|,$$

y tomando límite para $n \to \infty$ se concluye que

$$|a+b| \leq 1 \cdot |b| = \max\{|a|, |b|\}.$$

$\Leftarrow$) De la desigualdad ultramétrica, resulta por inducción que $|n| \leq 1$ para todo $n \in \mathbb{N}$. □

2. Proposición: *Dada una valoración $v \colon K \setminus \{0\} \to \mathbb{R}$, la aplicación $||_v \colon K \to \mathbb{R}$, $|a|_v := e^{-v(f)}$ es un valor absoluto no arquimediano. Recíprocamente, dado un valor absoluto no arquimediano $|| \colon K \to \mathbb{R}$, la aplicación $v_{||} \colon K \setminus \{0\} \to \mathbb{R}$, $v_{||}(a) := -\ln|a|$ es una valoración.*

3. Corolario: *Sea K un cuerpo de números y A el anillo de enteros de K. Dada un valor absoluto no arquimediano $||: K \to \mathbb{R}$ existe un número real $\alpha > 0$ y un punto cerrado $x \in \operatorname{Spec} A$, de modo que $|a| = e^{-\alpha \cdot v_x(a)}$, para todo $a \in K \setminus \{0\}$.*

4. Corolario: *Sea K una $k(x)$-extensión finita de cuerpos y C la variedad de Riemann de K. Dada un valor absoluto $||: K \to \mathbb{R}$, trivial sobre k (es decir, $|\lambda| = 1$, para todo $\lambda \in k \setminus \{0\}$), existe un número real $r > 0$ y un punto cerrado $x \in C$, de modo que $|a| = e^{-r \cdot v_x(a)}$, para todo $a \in K \setminus \{0\}$.*

5. Corolario: *Sea K un cuerpo de números y A el anillo de enteros de K. Entonces,*

$$\{\textit{Conjunto de valores absolutos no arquimedianos de } K\}/\sim = \operatorname{Spec} A$$

6. Corolario: *Sea $||_\infty$ el valor absoluto usual de $\mathbb{Q}$. Entonces,*

$$\left\{ \begin{array}{l} \textit{valores absolutos sobre } \mathbb{Q}, \\ \textit{módulo equivalencia} \end{array} \right\} = \operatorname{Spec} \mathbb{Z} \coprod \{||_\infty\}$$

7. Corolario: *Sea K un un cuerpo de números y A el anillo de enteros de K. Entonces,*

$$\left\{ \begin{array}{l} \textit{valores absolutos sobre } K, \\ \textit{módulo equivalencia} \end{array} \right\} = \operatorname{Spec} A \coprod \operatorname{Hom}_{anillos}(K, \mathbb{C})/\textit{Conj.}$$

8. Corolario: *Sea K una $k(x)$-extensión finita de cuerpos y C la variedad de Riemann de K. Entonces,*

$$\{\textit{Conjunto de valores absolutos de } K, \textit{ triviales sobre } k\}/\sim = C$$

Sea C una variedad de Riemann de cuerpo de funciones K. Dado $x \in C$, sea $||_x$ el valor absoluto asociado a x definido por $|f|_x = e^{-v_x(f)}$, para cada $f \in K$. Entonces, se cumple que

$$\boxed{\prod_{x \in C} |f|_x^{\operatorname{gr}_k x} = e^{-\sum_{x \in C} \operatorname{gr}_k x \cdot v_x(f)} \overset{5.4.5}{=} e^0 = 1}$$

Probemos la correspondiente fórmula en Teoría de Números.

Sea K un cuerpo de números y A el anillo de enteros de K. Denotemos $X = \operatorname{Spec} A$ el conjunto de valores absolutos no arquimedianos de K (módulo equivalencia), $X_\infty := \operatorname{Hom}_{Anillos}(K, \mathbb{C})/Conj. = \operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$ el conjunto de valores absolutos arquimedianos de K (módulo equivalencia), y $\bar{X} = X \coprod X_\infty$ el conjunto de valores absolutos de K (módulo equivalencia).

9. Definiciones: Dado un anillo A y un ideal maximal $\mathfrak{m}_x \subset A$, tal que $A/\mathfrak{m}_x$ sea un cuerpo finito, notaremos $\operatorname{gr} x := \ln |A/\mathfrak{m}_x|$.

Definamos el valor absoluto $\mathfrak{m}_x$-ádico $||_x$ definido por $|a|_x = e^{-v_x(a)}$. Observemos que $|a|_x^{\operatorname{gr} x} = |A/\mathfrak{m}_x|^{-v_x(a)}$.

Sea $||$ el valor absoluto usual de $\mathbb{C}$. Dado $y \in X_\infty$, sea $||_y$ el valor absoluto arquimediano de K asociado a y definido por $|f|_y = |f(y)|$, donde $f(y)$ es igual a la clase de f en $(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{p}_y$. Dicho de otro modo, si y se corresponde con $\sigma : K \to \mathbb{C}$, entonces $f(y) = \sigma(f)$ y $|f|_y = |\sigma(f)|$. Dado $y \in X_\infty$, denotemos $\operatorname{gr} y := \dim_{\mathbb{R}}(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{m}_y$.

10. Teorema: *Sea K un cuerpo de números. Para toda $f \in K$, se cumple que*

$$\boxed{\prod_{x \in \bar{X}} |f|_x^{\operatorname{gr} x} = 1}$$

Demostración. Sea A el anillo de enteros de K. Tenemos que $f = a_1/a_2$, con $a_1, a_2 \in A$. Basta probar el teorema para $f = a \in A$.Como $(a) = \prod_{x \in X} \mathfrak{m}_x^{v_x(a)}$,

$$|N(a)| = |A/aA| = |A/\prod_{x \in X} \mathfrak{m}_x^{v_x(a)}| = \prod_{x \in X} |A/\mathfrak{m}_x|^{v_x(a)} = \prod_{x \in X} |a|_x^{-\operatorname{gr} x}.$$

Por otra parte, $|N(a)| = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})} |\sigma(a)| = \prod_{y \in X_\infty} |a|_y^{\operatorname{gr} y}$.

Luego, $\prod_{x \in \bar{X}} |a|_x^{\operatorname{gr} x} = 1$.

□

11. Ejercicio: Comprueba la fórmula del teorema 6.6.10, para $K = \mathbb{Q}[i]$ y $f = i + 1$.

6.7. Divisores afines

1. Notación: En las siguientes secciones seguiremos las siguientes notaciones: K es una $\mathbb{Q}$-extensión finita de cuerpos de grado d, A es el anillo de enteros de K y

$$\{\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots \sigma_{r+s}, \sigma_{r+s+1} = \bar{\sigma}_{r+1}, \ldots, \sigma_{r+2s} = \bar{\sigma}_{r+s}\} = \operatorname{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$$

(donde $\sigma_i(K) \subset \mathbb{R}$ si y solo si $i \leq r$ y $\bar{\sigma}_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación).

2. Definición: Llamaremos grupo de divisores afines de K, que denotaremos $\operatorname{Div}(A)$, al grupo abeliano libre de base los puntos cerrados de $\operatorname{Spec} A$,

$$\operatorname{Div}(A) = \oplus_{x \in \operatorname{Spec}_{max} A} \mathbb{Z} \cdot x$$

Cada $D = \sum_i n_i \cdot x_i \in \operatorname{Div}(A)$ diremos que es un divisor afín. Diremos $D = \sum_x n_x x \geq D' = \sum_x n'_x x$ si $n_x \geq n'_x$, para todo x. Diremos que $D = \sum_x n_x x$ es efectivo si $D \geq 0$. Dado un

divisor $D = \sum_{x\in \mathrm{Spec}\, A} n_x \cdot x$, diremos que el conjunto $\mathrm{Sop}(D) = \{x \in \mathrm{Spec}\, A \text{ tal que } n_x \neq 0\}$ es el soporte de D.

3. Definición: Cada $f \in K$, no nula, define un divisor afín, llamado divisor afín principal, que denotamos $D(f)$:

$$D(f) = \sum_{x\in \mathrm{Spec}_{max} A} v_x(f) \cdot x.$$

Se dice que dos divisores afines D, D' son afínmente equivalentes si existe $f \in K$ tal que $D = D' + D(f)$. El conjunto de los divisores afines principales de $\mathrm{Div}\, A$, es un subgrupo y el cociente de $\mathrm{Div}\, A$ por el subgrupo de los divisores afines principales se denota $\mathrm{Pic}\, A = \mathrm{Div}\, A/\sim$ y se llama grupo de clases de ideales de A o grupo de Picard de A.

4. Ejercicio: Prueba que $\mathrm{Pic}\, \mathbb{Z} = \{0\}$.

5. Ejercicio: Prueba que $\mathrm{Pic}\, A = \{0\}$ si y solo si A es un dominio de ideales principales.

Si dos ideales no nulos $\mathfrak{a}, \mathfrak{a}' \subset A$ son isomorfos, localizando en el punto genérico obtenemos un isomorfismo de K-módulos de K, que es multiplicar por una $f \in K$, luego $\mathfrak{a}' = f \cdot \mathfrak{a}$.

6. Proposición: *Se cumplen las igualdades*

$$\begin{array}{rcl} \textit{Conj. de ideales no nulos de } A & = & \textit{Conj. de divisores afines efectivos} \\ \mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r} & \mapsto & D(\mathfrak{a}) := \sum_i n_i x_i \end{array}$$

$$\textit{Conjunto de ideales no nulos de } A\textit{, módulo isomorfismos} = \mathrm{Pic}\, A,\ [\mathfrak{a}] \mapsto [D(\mathfrak{a})]$$

Demostración. Veamos la segunda igualdad. La asignación es epiyectiva: Dado un divisor afín D, sea $f \in A$, tal que $D + Df = \sum_{i=1}^{r} n_i x_i$ sea un divisor afín efectivo. Sea $\mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$. Entonces, $D(\mathfrak{a}) = D + Df$.

La asignación es inyectiva: Si $D(\mathfrak{a}) = D(\mathfrak{a}') + Df$, entonces $\mathfrak{a} = f \cdot \mathfrak{a}'$ y $\mathfrak{a}$ es isomorfo a $\mathfrak{a}'$. □

7. Proposición: *Las asignaciones*

$$\begin{array}{rcl} \mathrm{Div}\, A & \longrightarrow & \{\textit{Ideales fraccionarios de } K\} \\ D = \sum_i n_i x_i & \longmapsto & I_D := \{f \in K : D(f) \geq D\} = \prod_i \mathfrak{m}_{x_i}^{n_i} \\ D(I) := \sum_x \text{ínf}\{v_x(f) :\ f \in I\} \cdot x & \longleftarrow\!\shortmid & I \end{array}$$

son inversas entre sí. Por tanto,

$$\mathrm{Pic}\, A = \textit{Conjunto de ideales fraccionarios de } K\textit{, módulo isomorfismos.}$$

Demostración. Si $I = \prod_x \mathfrak{m}_x^{n_x}$ entonces $D(I) = \sum_x n_x x$. Dado $D = \sum_x n_x x$ se cumple que

$$I_D = \{f \in K : D(f) \geq \sum_x n_x x\} = \cap_x \mathfrak{m}_x^{n_x} = \prod_x \mathfrak{m}_x^{n_x}.$$

□

8. Proposición: *Dado un ideal fraccionario $I \subseteq K$ se cumple que*

$$N(I) = e^{\mathrm{gr}(D(I))}$$

Es decir, el diagrama

$$\begin{array}{ccc} \{\textit{Divisores afines}\} & = & \{\textit{Ideales fraccionarios}\} \\ \downarrow \mathrm{gr} & & \downarrow N \\ \mathbb{R} & \xrightarrow{e^x} & \mathbb{R}^+ \end{array}$$

es conmutativo.

Demostración. Las aplicaciones $e^{\mathrm{gr}}, N \circ I$: {Divisores afines de K} $\to \mathbb{R}^+$ son morfismos de grupos. Para ver que son iguales basta comprobar que coinciden sobre los puntos $x \in \mathrm{Spec}_{max} A$. Efectivamente, $e^{\mathrm{gr}(x))} = |A/\mathfrak{m}_x| = N(\mathfrak{m}_x) = N(I(x))$. □

9. Proposición: *Sea $c \in \mathbb{Z}$. Salvo multiplicación por invertibles existe un número finito de elementos $a \in A$ tales que $N(a) = c$.*

Demostración. $|N(a)| = |A/aA| = |c|$ si y solo si $\mathrm{gr}D(a) = \ln|c|$. Ahora bien, divisores afines efectivos de grado dado solo existen un número finito. Por tanto, existen $a_1, \ldots, a_m$ de modo que $\mathrm{gr}D(a_i) = \ln|c|$ y si $\mathrm{gr}D(a) = \ln|c|$, entonces $Da = Da_i$. Luego a es igual salvo multiplicación por invertibles a alguno de los a_i.

□

6.8. Divisores completos

1. Notación: Sea $X = \mathrm{Spec}_{max} A$, $X_\infty = \mathrm{Spec} K \otimes_{\mathbb{Q}} \mathbb{R}$ y $\bar{X} = X \coprod X_\infty$.

2. Definición: Llamaremos grupo de los divisores completos de $\bar{X}$, que denotaremos $\mathrm{Div}(\bar{X})$, al grupo

$$\mathrm{Div}(\bar{X}) = (\oplus_{x \in X} \mathbb{Z} \cdot x) \oplus (\oplus_{y \in X_\infty} \mathbb{R} \cdot y)$$

y diremos que $\bar{D} = \sum_{x \in X} n_x x + \sum_{y \in X_\infty} \lambda_y y$ es un divisor completo. Diremos que $\bar{D}_{|X} := \sum_{x \in X} n_x x$ es la parte afín de $\bar{D}$ y que $\bar{D}_\infty := \sum_{y \in X_\infty} \lambda_y y$ es la parte del infinito de $\bar{D}$.

Diremos que $\bar{D} \geq 0$ si $n_x, \lambda_y \geq 0$, para todo x e y.

3. Definición: Dado $y \in X_\infty$ y $f \in K$, denotemos $v_y(f) := -\ln|f|_y$. Diremos que

$$\bar{D}(f) = \sum_{x \in \bar{X}} v_x(f) \cdot x$$

es el divisor principal completo asociado a f. El conjunto de los divisores completos principales es un subgrupo de $\mathrm{Div}(\bar{X})$. El cociente de $\mathrm{Div}(\bar{X})$ por el subgrupo de los divisores principales completos se denota $\mathrm{Pic}(\bar{X})$ y se denomina grupo de Picard completo.

4. Definición: Dado un divisor completo $\bar{D} = \sum_{x \in X} n_x \cdot x + \sum_{y \in X_\infty} \lambda_y \cdot y$ llamaremos grado de $\bar{D}$, que denotamos $\mathrm{gr}\,\bar{D}$, a

$$\mathrm{gr}(\bar{D}) := \sum_{x \in X} n_x \cdot \mathrm{gr}\, x + \sum_{y \in X_\infty} \lambda_y \cdot \mathrm{gr}\, y$$

Observemos que $\mathrm{gr}\colon \mathrm{Div}(\bar{X}) \to \mathbb{R}$ es un morfismo de grupos.

5. Teorema: *Para toda $f \in K$, se cumple que*

$$\mathrm{gr}(\bar{D}(f)) = 0$$

Demostración. Es consecuencia de la proposición 6.6.10 □

6. Ejercicio: Sea $\bar{X}$ el conjunto de valores absolutos de $\mathbb{Q}$, módulo equivalencia. Prueba que $\mathrm{Pic}\,\bar{X} = \mathbb{R}$.

6.9. Teorema de Riemann-Roch débil

1. Notación: Sea $\mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots \sigma_{r+s}, \sigma_{r+s+1} = \bar{\sigma}_{r+1}, \ldots, \sigma_{r+2s} = \bar{\sigma}_{r+s}\}$ (donde $\sigma_i(K) \subset \mathbb{R}$ si y solo si $i \leq r$ y $\bar{\sigma}_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación). Consideremos la inmersión canónica

$$K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s, \;\; f \mapsto (\sigma_1(f), \ldots, \sigma_{r+s}(f).)$$

2. Definición: Sea D' un divisor completo, definimos $\bar{I}_{D'} := \{f \in K : \bar{D}(f) \geq D'\}$.

Si $D' = n_1 x_1 + \cdots + n_m x_m + \lambda_1 y_1 + \cdots + \lambda_{r+s} y_{r+s}$, entonces

$$\begin{aligned} \bar{I}_{D'} &= \left\{ \begin{array}{r} f \in K : v_{x_i}(f) \geq n_i, \forall i \\ v_x(f) \geq 0, \forall x \neq x_i \end{array} \right\} \cap \left\{ f \in K : v_{y_i}(f) \geq \lambda_i, \; \forall y_i \right\} \\ &= \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m} \bigcap \{(\mu_i) \in \mathbb{R}^r \times \mathbb{C}^s : |\mu_i| \leq e^{-\lambda_i}, \forall i\}. \end{aligned}$$

3. Propiedades: 1. *Si* $D' = D'' + \bar{D}(g)$, *entonces* $\bar{I}_{D'} = g \cdot \bar{I}_{D''} \simeq \bar{I}_{D''}$.

2. *El conjunto* $\bar{I}_{D'}$ *es finito porque es la intersección de la red* $\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m}$ *con el compacto* $\{(\mu_j) \in \mathbb{R}^r \times \mathbb{C}^s : |\mu_j| \leq e^{-\lambda_j}, \forall j\}$, *que es finito.*

3. *En el caso* $D' = 0$, *entonces* $\bar{I}_{\{0\}} \setminus \{0\} = \{f \in K^* : \bar{D}(f) \geq 0\} = \{f \in K^* : \bar{D}(f) = 0\}$ *forma un subgrupo multiplicativo de* K^* *que, al ser finito, ha de coincidir con las raíces n-ésimas de la unidad contenidas en* K, *que denotaremos* μ_K.

4. $\bar{I}_{-D'} \setminus \{0\}/\mu_K = \{$*Div. efectivos completos linealmente equiv. a* $D'\}$, $[f] \mapsto D' + \bar{D}f$.

5. *Si* $\mathrm{gr}(D') < 0$ *entonces* $\bar{I}_{-D'} = \{0\}$.

6. *Si* $\mathrm{gr}(D') = 0$ *y* $\bar{I}_{-D'} \neq \{0\}$, *entonces existe* f *tal que* $D' = \bar{D}(f)$.

4. Teorema del punto de la red de Minkowski: *Sea* E *un* $\mathbb{R}$*-espacio vectorial de dimensión* d. *Sea* Γ *una red de* E *y* C *un compacto de* E *convexo y simétrico respecto del origen. Si* $Vol(C) \geq 2^d Vol(E/\Gamma)$[3], *entonces* C *contiene algún vector no nulo de la red* Γ.

Demostración. Como $Vol(\frac{1}{2} \cdot C) \geq Vol(E/\Gamma)$, la composición $\frac{1}{2} \cdot C \hookrightarrow E \to E/\Gamma$ no puede ser inyectiva (pues definiría un homeomorfismo $\frac{1}{2} \cdot C = E/\Gamma$, y por tanto una sección continua de $E \to E/\Gamma$). Por tanto, existen $x, y \in C$ distintos tales que $\frac{y-x}{2} \in \Gamma$. Como C es convexo y simétrico $\frac{y-x}{2} \in C$. □

5. Teorema de Riemann-Roch débil: *Sea* D' *un divisor completo. Si*

$$\mathrm{gr}\, D' \geq \ln \sqrt{|\Delta_K|} - s \cdot \ln(\pi/2)$$

entonces D' *es linealmente equivalente a un divisor completo efectivo.*

Demostración. Hay que probar que $\bar{I}_{-D'} \neq \{0\}$. $-D' = D(I) + D_\infty$, para cierto ideal fraccionario I y cierto divisor $D_\infty = \sum_i \lambda_i y_i$. Sea $C = \{(\mu_1, \ldots, \mu_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |\mu_i| \leq e^{-\lambda_i}, \forall i\}$, entonces $\bar{I}_{-D'} = I \cap C$ y

$$Vol(\mathbb{R}^r \times \mathbb{C}^s/I) \overset{6.3.15}{=} N(I) \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/A) = N(I) \cdot 2^{-s} \sqrt{|\Delta_K|} \overset{6.7.8}{=} 2^{-s} e^{\mathrm{gr}(D(I))} \cdot \sqrt{|\Delta_K|},$$
$$Vol(C) = 2^r e^{-(\lambda_1 + \cdots + \lambda_r)} \cdot \pi^s e^{-2(\lambda_{r+1} + \cdots + \lambda_{r+s})} = 2^r (\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)}.$$

El teorema del punto de la red de Minkowski asegura que $\bar{I}_{-D'} \neq \{0\}$ cuando

$$2^r (\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)} = Vol(C) \geq 2^d Vol(\mathbb{R}^r \times \mathbb{C}^s/I) = 2^r e^{\mathrm{gr}\, D(I)} \sqrt{|\Delta_K|}$$

es decir, cuando $(\frac{\pi}{2})^s e^{\mathrm{gr}\, D'} \geq \sqrt{|\Delta_K|}$. Tomando ln concluimos.

□

[3] La proporción entre volúmenes no depende del paralelepípedo de volumen 1 prefijado.

6.10. Finitud del grupo de Picard

1. Proposición: *Todo divisor afín D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que* $\ln \sqrt{|\Delta_K|}$.

Demostración. Sea D_∞ un divisor en el infinito tal que $\mathrm{gr}(D+D_\infty) = \ln \sqrt{|\Delta_K|}$. Por el teorema de Riemann-Roch débil, existe $f \in K$ tal que $D+D_\infty+\bar{D}f$ es un divisor efectivo, de grado $\ln \sqrt{|\Delta_K|}$. Como $D+D_\infty+\bar{D}f = D+D(f)+\bar{D}(f)_\infty+D_\infty$ entonces D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln \sqrt{|\Delta_K|}$. □

2. Proposición: *Todo ideal fraccionario $I \subset K$ es isomorfo a un ideal (de A) de norma menor o igual que* $\sqrt{|\Delta_K|}$.

Demostración. Es consecuencia de la proposición anterior y 6.7.8. □

3. Teorema: $\mathrm{Pic}\, A$ *es un grupo finito.*

Demostración. El número de divisores afines efectivos de grado menor o igual que cierto número es finito. Dado $[D] \in \mathrm{Pic}\, A$, D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln \sqrt{|\Delta_K|}$. □

4. Ejercicio: Sea K un cuerpo de números y A el anillo de enteros de K. Prueba que si todo ideal primo $\mathfrak{p}_x \subset A$, tal que $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|}$, es principal, entonces A es un dominio de ideales principales.

Es conocido que el anillo de enteros de $\mathbb{Q}[\sqrt{-r}]$, con $r > 0$ y no divisible por ningún primo al cuadrado, es de ideales principales si y solo si $r = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

5. Corolario: *Sea K un cuerpo de números y A el anillo de enteros de K. Existe un número natural $n > 0$, de modo que todo ideal $\mathfrak{a} \subset A$ cumple que $\mathfrak{a}^n$ es principal.*

Demostración. Sea $n = |\mathrm{Pic}\, A|$. Entonces, $[\mathfrak{a}]^n = [A]$, para todo $[\mathfrak{a}] \in \mathrm{Pic}\, A$, es decir, $\mathfrak{a}^n$ es un ideal principal, para todo ideal $\mathfrak{a} \subseteq A$. □

6. Corolario: *Sea K un cuerpo de números y A el anillo de enteros de K. Existe una extensión finita L de K, de modo que todos los ideales de A extendidos al anillo de enteros de L son principales.*

Demostración. Sea $\mathfrak{a} \subset A$ un ideal y $n > 0$ tal que $\mathfrak{a}^n = (c)$ es principal. Si K' es una extensión finita de cuerpos de K que contiene a $\sqrt[n]{c}$ y B es el anillo de enteros de K', entonces $\mathfrak{a} \cdot B = (\sqrt[n]{c})$. En efecto, $(\mathfrak{a} \cdot B)^n = c \cdot B = (\sqrt[n]{c})^n$, luego las descomposiciones en producto de ideales primos de $\mathfrak{a} \cdot B$ y la $(\sqrt[n]{c})$ han de ser la misma, luego son iguales. Si $\operatorname{Pic} A = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_n]\}$ y $\mathfrak{a}_i^n = (c_i)$, entonces $L = K[\sqrt[n]{c_1}, \ldots, \sqrt[n]{c_n}]$ es la extensión de cuerpos buscada.

□

6.11. El discriminante: invariante fundamental

Veamos que el discriminante de un cuerpo de números es un invariante asociado fundamental para su clasificación.

1. Teorema de Minkowski: *Sea K un cuerpo de números. $|\Delta_K| = 1$ si y solo si $K = \mathbb{Q}$.*

Demostración. Si $\Delta_K = \pm 1$, por el teorema de Riemann-Roch 6.9.5, todo divisor completo de grado cero es principal, lo cual es imposible porque hay un número no numerable de divisores completos de grado cero y solo un número numerable de $f \in K$; salvo que $|X_\infty| = 1$, es decir, salvo los casos $r = 1$ y $s = 0$ (luego $K = \mathbb{Q}$) y $r = 0$ y $s = 1$ (luego $d = 2$ y $K = \mathbb{Q}[\sqrt{n}]$ que tiene discriminante n, si $n \equiv 1 \mod 4$, o $4n$, si $n \equiv 2, 3 \mod 4$).

□

2. Teorema de Hermite: *Solo hay un número finito de extensiones de $\mathbb{Q}$ de grado y discriminantes dados.*

Demostración. Sea K una extensión de discriminante Δ y grado d.

Supongamos que $i \in K$ (luego $r = 0$). Consideremos en el infinito el divisor

$$D' := (d + \ln \sqrt{|\Delta_K|}) \cdot [\sigma_1] - [\sigma_2] - \ldots - [\sigma_s]$$

El teorema de Riemann-Roch débil afirma que $\bar{I}_{-D'} \neq 0$, es decir, existe $f \in A$ no nula tal que $|\sigma_i(f)| \leq e^{-1} < 1$, para todo $i > 1$ (y $|\sigma_1(f)| \leq e^d \cdot \sqrt{|\Delta_K|}$) . Podemos pensar $\sigma_1 \colon K \hookrightarrow \mathbb{C}$ como una inclusión. Como $N(f)$ es un número entero, se sigue $|\sigma_1(f)| = |f| > 1$. Tomando $i \cdot f$ en vez de f, si es necesario, puedo suponer que f no es un número real. Sea $H = \{\sigma \in \operatorname{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) \colon \sigma(f) = f\}$, tendremos que $|\sigma(f)| = |f| > 1$, para todo $\sigma \in H$. Por tanto, $H = \{\sigma_1\}$. Por la Teoría de Galois sabemos que $\mathbb{Q}[f] = \mathbb{Q}[x]/(q(x))$, con $q(x) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})}(x - \sigma(f))$. Luego, $K = \mathbb{Q}[f]$. Los coeficientes de $q(x)$ están acotados, pues sus raíces $\sigma_i(f)$ lo están, y como son números enteros solo hay un número finito de tales polinomios. Por tanto, salvo isomorfismos solo hay un número finito de extensiones K posibles.

Si $i \notin K$, entonces $|\Delta_{K[i]}| \leq |\Delta_{A[i]}| \overset{6.3.11}{=} 4^d|\Delta_A|^2 = 4^d|\Delta_K|^2$. El número de cuerpos cuyo valor absoluto del discriminante es menor que $4^d|\Delta^2|$ y grado $2d$, que contienen a i, es finito. Cada uno de estos cuerpos contiene un número finito de subextensiones. En conclusión, el número de cuerpos de discriminante Δ y grado d es finito.

□

3. La cota de Minkowski: *Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Dado un ideal fraccionario $I \subset K$, existe $f \in I$ no nula, de modo que*

$$|N(f)| \leq c|N(I)|, \text{ con } c = d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|}.$$

Tomando $I = A$, obtenemos que $d < \sqrt{|\Delta_K|}$ ó $d < 3$.

Demostración. Consideremos el compacto

$$C = \{(\lambda_1, \ldots, \lambda_r, \ldots, \lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i \leq r} |\lambda_i| + \sum_{j > r} 2|\lambda_j| \leq t\}.$$

Se cumple[4] que $Vol(C) = 2^r(\frac{\pi}{2})^s t^d/d!$. Sea t, de modo que $Vol(C) = 2^d Vol(\mathbb{R}^r \times \mathbb{C}^s/I)$. Entonces, por el teorema del punto de la red de Minkowski existe $f \in I$ no nula, de modo que $\sum_i |\sigma_i(f)| \leq t$. Como la media geométrica está acotada por la media aritmética,

$$\begin{aligned} |N(f)| = \prod_i |\sigma_i(f)| \leq (\sum_i |\sigma_i(f)|/d)^d \leq t^d/d^d = d!d^{-d}(8/\pi)^s \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I) \\ = d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot |N(I)|. \end{aligned}$$

Consideremos $I = A$, entonces existe $f \in A$ de modo que $|N(f)| \leq c$, luego $c \geq 1$. Para todo número natural $m \geq u, 4$ $(u \geq 0)$, se cumple que $m!m^{-m}(4/\pi)^{\frac{m}{2}} \cdot u < 1$. Se sigue que si $d \geq 4$ entonces $d < \sqrt{|\Delta_K|}$. Además, no es posible $d = 3$ y $3 \geq \sqrt{|\Delta_K|}$. Luego, $d < 3$ ó $d < \sqrt{|\Delta_K|}$.

□

4. Ejercicio : Sea K un cuerpo de números de discriminante -4. Prueba que $\dim_{\mathbb{Q}} K = 2$. Prueba que $K = \mathbb{Q}[i]$.

5. Corolario : *Sea A el anillo de enteros de un cuerpo de números K. Sea $I \subseteq A$ un ideal. Existe un ideal $I' \subset A$ isomorfo a I, de modo que $N(I') \leq d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|}$.*

Demostración. Existe $f \in I^{-1}$ tal que $|N(f)| \leq d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot N(I^{-1})$, por 6.11.3. $I' := f \cdot I \subset A$ es un ideal isomorfo a I. Tomando normas, obtenemos que

$$N(I') = |N(f)| \cdot N(I) \leq d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|}.$$

□

[4] Véase el problema 13.

6.12. Invertibles. Elementos de norma 1

Queremos estudiar el grupo de invertibles de un anillo de enteros A, que coincide con el grupo de los enteros de K de norma ± 1.

Sea $\mathrm{Div}_\infty = \oplus_{y\in X_\infty}\mathbb{R}\cdot y = \mathbb{R}^{r+s}$ el espacio vectorial de los divisores completos con soporte en el infinito. El espacio vectorial Div^0_∞ de los divisores completos con soporte en el infinito de grado 0 es un hiperplano de Div_∞.

Sea A^* el conjunto de todos los invertibles de A y $\mathrm{Pic}^0_\infty := \mathrm{Div}^0_\infty/\sim = \mathrm{Div}^0_\infty/\bar{D}(A^*)$. Consideremos la sucesión exacta

$$1 \to \mu_K \to A^* \xrightarrow{\bar{D}} \mathrm{Div}^0_\infty \to \mathrm{Pic}^0_\infty \to 0$$

1. Proposición: Pic^0_∞ *es compacto.*

Demostración. Fijemos un divisor de grado $c := \ln\sqrt{|\Delta_K|}$, $D'_\infty = \frac{c}{\mathrm{gr}\, y_1}\cdot y_1 \in \mathrm{Div}_\infty$. Sea Div^c_∞ el conjunto de los divisores con soporte en el infinito de grado c. Obviamente, $\mathrm{Div}^0_\infty = \mathrm{Div}^c_\infty$, $\bar{D} \mapsto \bar{D} + D'_\infty$, $\mathrm{Pic}^0_\infty = \mathrm{Div}^0_\infty/\bar{D}(A^*) = \mathrm{Div}^c_\infty/\bar{D}(A^*) =: \mathrm{Pic}^c_\infty$ y basta demostrar que Pic^c_∞ es compacto.

Dado $\bar{D} \in \mathrm{Div}^c_\infty$, por el teorema de Riemann-Roch débil existe $f \in K$ tal que

$$\bar{D} + \bar{D}(f) \geq 0.$$

La parte afín de $\bar{D} + \bar{D}(f)$ es igual a $D(f) \geq 0$ y sea $c' = \mathrm{gr}(D(f))$. La parte del infinito de $\bar{D} + \bar{D}(f)$ es $\bar{D} + \bar{D}(f)_\infty \geq 0$, que tiene grado $c - c'$ y está en el compacto

$$C_{c-c'} := \{D'' \in \mathrm{Div}^{c-c'}_\infty : D'' \geq 0\} \subset \mathrm{Div}^{c-c'}_\infty .$$

Es decir, $\bar{D}$ pertenece al compacto $C_f := C_{c-c'} - \bar{D}(f)_\infty \subset \mathrm{Div}^c_\infty$. Observemos que $f \in A$, porque $D(f) \geq 0$ y que $\mathrm{gr}(D(f)) = c' \leq c$. El conjunto de los divisores $D(f)$, con $f \in A$, tales que $\mathrm{gr}D(f) \leq c$ es finito, digamos que es $\{D(f_1), \ldots, D(f_n)\}$. Entonces,

$$\mathrm{Div}^c_\infty = \bigcup_{g \in \bigcup_{i=1}^n f_i \cdot A^*} C_g \text{ y por tanto } \mathrm{Pic}^c_\infty = \cup_i \overline{C_{f_i}},$$

que es unión de un número finito de compactos, luego compacto.

□

2. Lema: *Sea* Γ *un subgrupo discreto de* $\mathbb{R}^d$. *Entonces, existen* $r \leq d$ *vectores linealmente independientes* $e_1, \ldots, e_r \in \mathbb{R}^d$ *de modo que* $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$.

Demostración. Γ es un cerrado de $\mathbb{R}^d$: Si una sucesión $\{v_n \in \Gamma\}$ converge a $v \in \mathbb{R}^d$, entonces $v_n - v_m \to 0$, para $n, m >> 0$. Como Γ es discreto $v_n - v_m = 0$ para todo $n, m >> 0$. Luego, $v_n = v_m$ para todo $n, m >> 0$ y $v = v_n \in \Gamma$, para $n >> 0$.

Sustituyendo $\mathbb{R}^d$ por el subespacio vectorial que genera Γ, podemos suponer que Γ contiene una base de $\mathbb{R}^d$. Podemos suponer que Γ contiene la base estándar de $\mathbb{R}^d$, es decir, que $\mathbb{Z}^d \subseteq \Gamma$. Consideremos la proyección $\pi\colon \mathbb{R}^d \to \mathbb{R}^d/\mathbb{Z}^d = S_1^d$, que es una aplicación continua abierta luego la topología de S_1^d coincide con la topología final de π. $\pi(\Gamma)$ es un cerrado, porque $\pi^{-1}(\pi(\Gamma)) = \Gamma + \mathbb{Z}^d = \Gamma$ es un cerrado, luego es compacto. Además, $\pi(\Gamma)$ es discreto: sea U un abierto tal que $U \cap \Gamma = \mathbb{Z}^d$, entonces $\pi(U) \cap \pi(\Gamma) = \bar{0}$ es un abierto de $\pi(\Gamma)$. Por tanto, $\pi(\Gamma)$ es finito y obtenemos que Γ es finito generado. Como carece de torsión, pues está incluido en $\mathbb{R}^d$, es un grupo libre de rango d. Existen, $e_1, \ldots, e_d \in \Gamma$ tales que $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_d$ y como $e_1, \ldots, e_d$ generan $\mathbb{R}^d$, han de ser linealmente independientes en $\mathbb{R}^d$. □

3. Teorema de Dirichlet: Pic_∞^0 *es un toro de dimensión* $r+s-1$. A^* *es un grupo finito generado de rango* $r+s-1$ *y de torsión el grupo de las raíces de la unidad contenidas en* K.

Demostración. A es un subconjunto discreto de $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$, luego A^* es un subgrupo discreto de $(\mathbb{R}^r \times \mathbb{C}^s)^*$. Consideremos el epimorfismo de grupos (que tiene sección)

$$(\mathbb{R}^r \oplus \mathbb{C}^s)^* \xrightarrow{\ln||} \mathrm{Div}_\infty,\ (\lambda_i) \mapsto \sum_i -(\ln|\lambda_i|) \cdot y_i,$$

que es una aplicación abierta de núcleo un campacto que denotamos C. La imagen de A^* es $\bar{D}(A^*)$. El núcleo del epimorfismo $A^* \to \bar{D}(A^*)$, $f \mapsto \bar{D}(f)$ es el conjunto de las raíces de la unidad contenidas en K, μ_K.

$\bar{D}(A^*) \subset \mathrm{Div}_\infty$ es discreto: sea U un abierto de $(\mathbb{R}^r \times \mathbb{C}^s)^*$ que contenga a C y tal que $U \cap A^* = \mu_K$ y W un abierto de $(\mathbb{R}^r \times \mathbb{C}^s)^*$ que contenga a 1 y tal que $C \cdot W \subseteq U$, entonces $\ln|W| \cap \bar{D}(A^*) = \{0\}$.

Por el lema anterior $\bar{D}(A^*) \subset \mathrm{Div}_\infty^0 \simeq \mathbb{R}^{r+s-1}$ es un grupo libre de rango $\leq r+s-1$. La compacidad de Pic_∞^0 implica que el rango de $\bar{D}(A^*)$ es $r+s-1$ y que Pic_∞^0 es un toro de dimensión $r+s-1$. Por tanto,

$$A^* \simeq \mu_K \oplus \mathbb{Z}^{r+s-1}.$$

□

4. Ejercicio: Prueba que existen $\xi_1, \ldots, \xi_{r+s-1} \in A^*$, de modo que $a \in A^*$ si y solo si

$$a = \mu \cdot \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos) y una raíz n-ésima de la unidad $\mu\in\mu_K$ (única).

5. Proposición: *El subgrupo de enteros de K de norma 1, $\{a\in A: N(a)=1\}$, es un grupo abeliano libre de rango $r+s-1$ si $\dim_{\mathbb{Q}}K$ es impar, y es un grupo abeliano finito generado de rango $r+s-1$ y torsión μ_K si $\dim_{\mathbb{Q}}K$ es par.*

Demostración. Como $G:=\{a\in A: N(a)=1\}$ es un subgrupo de índice finito (1 ó 2) de A^*, concluimos que es un grupo abeliano finito generado de rango $r+s-1$.

Si $\dim_{\mathbb{Q}}K$ es impar, entonces $r>0$, luego $K\subset\mathbb{R}$ y $\mu_K=\{\pm1\}$. Obviamente $N(-1)=-1$, por tanto la parte de torsión de G es igual a $\mu_K\cap G=\{1\}$. Si $\dim_{\mathbb{Q}}K$ es par, entonces $N(\xi)=1$ para todo $\xi\in\mu_K$: Obviamente $N(\pm1)=1$. Si $\xi\in\mu_K$ es imaginaria entonces $r=0$. Entonces, $N(a)=\prod_{i=1}^{s}\sigma_i(a)\bar{\sigma}_i(a)>0$, para todo $a\in A\setminus\{0\}$. Por tanto la parte de torsión de G es igual a $\mu_K\cap G=\mu_K$.

□

6. Ejercicio: Prueba que existen $\xi_1,\dots,\xi_{r+s-1}\in A$ de norma 1, de modo que $a\in A$ es de norma 1, si y solo

$$a=\begin{cases}\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_{\mathbb{Q}}K \text{ impar.}\\ \mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu\in\mu_K, \text{ si } \dim_{\mathbb{Q}}K \text{ es par.}\end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos). Prueba que existen además $\mu_1,\dots,\mu_i\in A$ de norma $c\in\mathbb{Z}$, de modo que $N(a)=c\in\mathbb{Z}$ si y solo

$$a=\begin{cases}\mu_i\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_{\mathbb{Q}}K \text{ impar.}\\ \mu_i\cdot\mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu\in\mu_K, \text{ si } \dim_{\mathbb{Q}}K \text{ es par.}\end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos), para un i único (recordar el ejercicio 6.7.9).

7. Ejemplo: Sea $n>1$ un entero sin factores cuadráticos y $K=\mathbb{Q}[\sqrt{n}]$, $A=\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$ el anillo de enteros de K. A^* es un grupo abeliano de rango 1 y parte de torsión ±1. Obviamente $A^*\subseteq\{\frac{a+b\sqrt{\Delta}}{2}: a,b\in\mathbb{Z}\}$ y si $N(\frac{a+b\sqrt{\Delta}}{2})=\pm1$ entonces $\frac{a+b\sqrt{\Delta}}{2}\in A^*$, porque su polinomio anulador sería $x^2-ax\pm1$. Por tanto,

$$A^*=\{\frac{a+b\sqrt{\Delta}}{2}, a,b\in\mathbb{Z}: a^2-b^2\Delta=\pm4\}=\{\pm\xi^n, \forall n\in\mathbb{Z}\}.$$

Para calcular $\xi=\frac{a+b\sqrt{\Delta}}{2}$, que es único salvo toma de inverso y multiplicación por -1, podemos suponer que $a,b>0$ y ha de ser aquel que cumpla además que a y b son mínimos.

8. Ejercicio: Calcula los invertibles de los anillos de enteros de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ y $\mathbb{Q}[\sqrt{6}]$.

9. Sea $\mathrm{Div}^0(\bar{X})$ el conjunto de los divisores completos de grado cero. Consideremos el morfismo natural $\mathrm{Div}(\bar{X}) \to \mathrm{Div}(X)$, $\bar{D} \mapsto \bar{D}_{|X}$ y la sucesión exacta,

$$0 \to \mathrm{Div}^0_\infty \to \mathrm{Div}^0(\bar{X}) \to \mathrm{Div}(X) \to 0$$

Sea $\mathrm{Pic}^0(\bar{X})$ el grupo de las clases de equivalencia de los divisores completos de grado 0. La sucesión exacta

$$0 \to \mathrm{Pic}^0_\infty \to \mathrm{Pic}^0(\bar{X}) \to \mathrm{Pic}(X) \to 0$$

relaciona el grupo de Picard completo (de divisores de grado cero) con el grupo de Picard de A y Pic^0_∞.

6.13. Número de ideales de norma acotada

1. Teorema: *Sea $S(n)$ el número de ideales de A de norma $\le n$. Existe una constante no nula v tal que*

$$S(n) = vn + O(n^{1-1/d})$$

(donde entendemos que $\lim_{x\to\infty} \frac{O(x)}{x} = cte$).

Demostración. En virtud de la finitud de $\mathrm{Pic}A$, basta probar el teorema para el número $T(n)$ de ideales de norma $\le n$ en una clase de isomorfismos dada. El conjunto de ideales de A está en correspondencia biunívoca con el conjunto de divisores afines efectivos y recordemos que si I es un ideal de norma n, entonces $D(I)$ es un divisor de grado $\ln n$. Por tanto, $T(n)$ es el número de divisores afines efectivos, D', de grado $\le \ln n$, afínmente equivalentes a un divisor afín efectivo dado (que es equivalente a un divisor $-D(\mathfrak{a})$, para cierto ideal $\mathfrak{a} \subset A$). Sea $m = \mathrm{gr}D(\mathfrak{a})$. La condición $D' = D(f) - D(\mathfrak{a}) \ge 0$ significa que $f \in \mathfrak{a}$, y la condición $\mathrm{gr}(D(f) - D(\mathfrak{a})) = \mathrm{gr}(D(f)) - \mathrm{gr}D(\mathfrak{a}) \le \ln n$ significa $-\mathrm{gr}(\bar{D}(f)_\infty) = \mathrm{gr}(D(f)) \le \ln n + m$. Es decir,

$$T(n) = \text{Nº de conjuntos } fA^* \text{ tales que } fA^* \subset \mathfrak{a} \text{ y } -\mathrm{gr}(\bar{D}(f)_\infty) \le \ln n + m.$$

(observemos que $-\mathrm{gr}(\bar{D}(g)_\infty) = \mathrm{gr}(D(g)) = \mathrm{gr}(D(f))$ para toda $g \in f \cdot A^*$).

Consideremos los morfismos

$$\begin{array}{ccccc} (\mathbb{R}^r \oplus \mathbb{C}^s)^* & \overset{\bar{D}_\infty}{\to} & \mathrm{Div}_\infty & \overset{-\mathrm{gr}}{\to} & \mathbb{R} \\ (\lambda_1, \ldots, \lambda_{r+s}) & \mapsto & -\sum_i (\ln|\lambda_i|) \cdot y_i & & \end{array}$$

Observemos que $\mathrm{Ker}\bar{D}_{\infty\,|A} = \{a \in A : \bar{D}(a)_\infty = 0\} = \{a \in A : \bar{D}(a) = 0\} = \mu_K$. Por lo tanto, $fA^* \subset \mathfrak{a}$ si y solo si $\bar{D}_\infty(fA^*) \subset \bar{D}_\infty(\mathfrak{a})$.
Consideremos el divisor de grado 1 con soporte en el infinito, $F = \frac{1}{d}\cdot(y_1 + \cdots + y_{r+s})$, entonces $\mathrm{Div}_\infty = \mathrm{Div}^0_\infty \oplus \mathbb{R}\cdot F$. Sea $P \subset \mathrm{Div}^0_\infty$ un paralelepípedo fundamental de la red $\bar{D}(A^*) = \bar{D}_\infty(A^*)$ en Div^0_∞, luego $\mathrm{Div}^0_\infty = \bar{D}_\infty(A^*) \oplus P$ y

$$\mathrm{Div}_\infty = \bar{D}_\infty(A^*) \oplus P \oplus \mathbb{R}\cdot F.$$

Dado $f\cdot A^*$, entonces existe un único $p \in P$ de modo que $\bar{D}_\infty(fA^*) = \bar{D}_\infty(A^*) + p + \lambda\cdot F$ (donde $\lambda = \mathrm{gr}(\bar{D}_\infty(f))$). Luego, $\bar{D}_\infty(fA^*) \subset \bar{D}_\infty(\mathfrak{a})$ si y solo si $(P\oplus\mathbb{R}\cdot F)\cap\bar{D}_\infty(\mathfrak{a}) = \{p+\lambda\cdot F\}$. Por tanto, $T(n) = |(P \oplus [-\ln n - m, \infty)\cdot F)\cap\bar{D}_\infty(\mathfrak{a})|$. Luego,

$$T(n) = \frac{|\bar{D}_\infty^{-1}(P \oplus [-\ln n - m, \infty)\cdot F)\cap\mathfrak{a}|}{|\mu_K|} = \frac{|(n^{\frac{1}{d}}\cdot\bar{D}_\infty^{-1}(P \oplus [-m, \infty)\cdot F)\cap\mathfrak{a}|}{|\mu_K|}.$$

Por el lema[5] 6.13.2, hemos concluido.

□

2. Lema: *Sea U un recinto acotado y limitado por un número finito de hipersuperficies diferenciables en un espacio vectorial real E de dimensión d y sea $\Gamma \subset E$ una red. Si $P(\lambda)$ denota el número de puntos de $\lambda\cdot U\cap\Gamma$, existe una constante no nula v tal que*

$$P(\lambda) = v\lambda^d + O(\lambda^{d-1}).$$

Demostración. Podemos suponer que $E = \mathbb{R}^d$ y $\Gamma = \mathbb{Z}^d$. Observemos que el número de puntos de $\lambda U\cap\Gamma$ es el mismo que el de $U\cap\lambda^{-1}\Gamma$. Sea $C = \{x \in \mathbb{R}^d : 0 \le x_i \le \lambda^{-1}, \forall i\}$. Considerando la unión $\bigcup_{p\in U\cap\lambda^{-1}\Gamma} p + C$, obtenemos una figura que casi coincide con U, pues le faltan algunos puntos de U y le sobran otros, pero tales puntos están en el compacto C_ϵ de los puntos que distan $\le \epsilon = \sqrt{d}/\lambda$ del borde de U. Luego,

$$Vol(U) - Vol(C_\epsilon) \le P(\lambda)Vol(C) \le Vol(U) + Vol(C_\epsilon).$$

Como $Vol(C) = \lambda^{-d}$ y $Vol(C_\epsilon) = O(\epsilon) = O(\lambda^{-1})$ se concluye que

$$P(\lambda) = \lambda^d\cdot Vol(U) + \lambda^d O(\lambda^{-1}) = \lambda^d\cdot Vol(U) + O(\lambda^{d-1}).$$

□

[5] Donde $E = \mathbb{R}^r\times\mathbb{C}^s$, $\Gamma = \mathfrak{a}$ y $U = \bar{D}_\infty^{-1}(P\oplus[-m,\infty)\cdot F)\coprod\{0\} = (0, e^m]\cdot\bar{D}_\infty^{-1}(P)\coprod\{0\}$.

6.14. La función zeta

Veamos la demostración de Euler de que el número de números primos es infinito: Dado un número finito de primos distintos $\{p_1,\dots,p_r\}$ observemos que

$$(1-\frac{1}{p_1})^{-1}\cdots(1-\frac{1}{p_r})^{-1}=(1+p_1^{-1}+p_1^{-2}+\cdots)\cdots(1+p_r^{-1}+p_r^{-2}+\cdots)=\sum_{n\in P}\frac{1}{n}$$

donde P es el conjunto de números naturales que se pueden expresar como producto de potencias de $p_1,\dots,p_r$. Denotemos $S=\sum_{n=1}^{\infty}\frac{1}{n}$. Tenemos que $S-1\le\int_1^{\infty}\frac{1}{t}dt\le S$. Como $\int_1^{\infty}\frac{1}{t}dt=\ln t]_1^{\infty}=\infty$ tenemos que $S=\infty$. Si existiese un número finito de números primos, $\{p_1,\dots,p_r\}$, entonces

$$(1-\frac{1}{p_1})^{-1}\cdot\dots\cdot(1-\frac{1}{p_r})^{-1}=\sum_{n=1}^{\infty}\frac{1}{n}=\infty$$

y hemos llegado a contradicción.

Para cada $x>1$ consideremos la serie $S(x)=\sum_{n=1}^{\infty}\frac{1}{n^x}$. Tenemos las desigualdades $S(x)-1\le\int_1^{\infty}\frac{1}{t^x}dt\le S(x)$. Como $\int_1^{\infty}\frac{1}{t^x}dt=\frac{t^{1-x}}{1-x}]_1^{\infty}=\frac{1}{x-1}$, la serie $S(x)$ converge. Es más, como los sumandos n^{-x} son funciones continuas en x decrecientes, la serie de funciones $S(x)$ es uniformemente convergente (en los intervalos $[a,\infty)$) y converge a una función continua. Además, $\lim_{x\to 1}(x-1)\cdot S(x)=1$. Observemos que

$$(1-\frac{1}{p_1^x})^{-1}\cdots(1-\frac{1}{p_r^x})^{-1}=(1+p_1^{-x}+p_1^{-2x}+\cdots)\cdots(1+p_r^{-x}+p_r^{-2x}+\cdots)=\sum_{n\in P}\frac{1}{n^x}.$$

Por tanto[6], $S(x)=\prod_{p\text{ primo}}(1-\frac{1}{p^x})^{-1}$.

1. Teorema: *La serie* $\zeta(x):=\sum_{n=1}^{\infty}n^{-x}$ *es una función continua en* $(1,\infty)$ *tal que*

$$\lim_{x\to 1}(x-1)\cdot\zeta(x)=1\quad y\quad \zeta(x)=\prod_{p\ primo}(1-\frac{1}{p^x})^{-1}.$$

Tratemos de generalizar todas estas definiciones y resultados a los anillos de números.

2. Definición: Sea K un cuerpo de números y A el anillo de enteros de K. Se dice que

$$\zeta_K(x):=\sum_{0\neq\mathfrak{a}\subseteq A}N(\mathfrak{a})^{-x}$$

es la función zeta (de Dedekind) de K.

[6]Recuerde el lector que toda serie de números complejos absolutamente convergente es incodicionalmente convergente.

3. Ejercicio: Prueba que $\zeta(x) = \zeta_{\mathbb{Q}}(x)$.

4. Teorema: *La función $\zeta_K(x)$ es continua en la semirecta $x > 1$,*

$$\lim_{x\to 1}(x-1)\cdot\zeta_K(x) = v \quad y \quad \zeta_K(x) = \prod_{\mathfrak{p}}(1-\frac{1}{N(\mathfrak{p})^x})^{-1}.$$

Demostración. Por el teorema 6.13.1 el número de ideales de norma n es $v + a_n$, donde $b_n := a_1 + \cdots + a_n = O(n^{1-\frac{1}{d}})$. Por tanto, $\zeta_K(x) = v\cdot\zeta(x) + \sum_n a_n n^{-x}$ y el siguiente lema permite concluir que $\sum_n a_n n^{-x}$ es una función continua en $x > 1 - \frac{1}{d}$. Luego, $\zeta_K(x)$ lo es en $x > 1$ y

$$\lim_{x\to 1}(x-1)\cdot\zeta_K(x) = v\cdot\lim_{x\to 1}(x-1)\cdot\zeta(x) = v.$$

La igualdad $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-x} = \prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-x})^{-1}$ expresa la unicidad de la descomposición de cada ideal no nulo de A en producto de ideales primos. □

5. Lema: *Sea (a_n) una sucesión de números reales y sea $b_n := a_1+\cdots+a_n$. Si $b_n = O(n^\epsilon)$ entonces la serie $\sum_n a_n n^{-x}$ converge uniformemente en los compactos de la semirrecta (ϵ,∞).*

Demostración. Para cada pareja de números naturales $m < r$,

$$\sum_{n=m}^{r} a_n\cdot n^{-x} = \sum_{n=m}^{r}(b_n - b_{n-1})\cdot n^{-x} = b_r r^{-x} - b_{m-1}m^{-x} + \sum_{n=m}^{r-1} b_n\cdot(n^{-x} - (n+1)^{-x}).$$

Por hipótesis existe una constante $c > 0$ tal que $|b_n| < cn^\epsilon$, para todo n. Luego,

$$|b_r r^{-x} - b_{m-1}m^{-x}| \le |b_r r^{-x}| + |b_{m-1}m^{-x}| \le cr^{-x+\epsilon} + c(m-1)^\epsilon\cdot m^{-x} \le 2cm^{-x+\epsilon}$$
$$|b_n\cdot(n^{-x} - (n+1)^{-x})| \le cn^\epsilon\cdot x\int_n^{n+1} t^{-x-1}dt \le c\cdot x\int_n^{n+1} t^{-x-1+\epsilon}dt.$$

Por tanto,

$$|\sum_{n=m}^{r} a_n\cdot n^{-x}| \le 2cm^{-x+\epsilon} + c\cdot x\int_m^\infty t^{-x-1+\epsilon}dt \le (2 + \frac{x}{-x+\epsilon})\cdot cm^{-x+\epsilon},$$

que tiende a cero para $m >> 0$ (fijado el compacto de la semirrecta (ϵ,∞)). □

6.15. Raíces modulares y la función zeta

1. Definición: Sea A un anillo de enteros, $\mathfrak{p}_x \subset A$ un ideal maximal y $\mathfrak{m}_p = (p) := \mathfrak{p}_x \cap \mathbb{Z}$. Llamaremos grado de x sobre $\mathbb{Z}$, que denotaremos $\mathrm{gr}_{\mathbb{Z}}\, x$, a

$$\mathrm{gr}_{\mathbb{Z}}\, x := l_{\mathbb{Z}}(A/\mathfrak{p}_x) = \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{p}_x = \mathrm{gr}_p\, x.$$

2. Ejemplo: Sea $A = \mathbb{Z}[x]/(q(x))$. Los primos de A de grado 1 sobre $\mathbb{Z}$ se corresponden con las raíces de $\overline{q(x)}$ en $\mathbb{Z}/p\mathbb{Z}$, variando p (llamadas raíces modulares de $q(x)$): Dada $y \in \mathrm{Spec}\, A$, con $\mathrm{gr}_{\mathbb{Z}}\, y = 1$ tenemos que $A/\mathfrak{p}_y = \mathbb{Z}/p\mathbb{Z}$ y si $\bar{x} \mapsto \bar{n}$ entonces $0 = \overline{q(x)} \mapsto q(\bar{n}) = 0$, es decir, $\bar{n}$ es una raíz modular de $q(x)$. Recíprocamente, si $\bar{n} \in \mathbb{Z}/p\mathbb{Z}$ es una raíz de $\overline{q(x)}$, entonces el núcleo del morfismo $A \to \mathbb{Z}/p\mathbb{Z}$, $\overline{p(x)} \mapsto p(\bar{n})$ es un ideal primo de A de grado 1 sobre $\mathbb{Z}$.

3. Recordemos (proposición 3.8.10) que si $\mathrm{Spec}\, A/pA = \{x_1, \ldots, x_r\}$ entonces

$$d = \mathrm{gr}_{\mathbb{Z}}\, x_1 \cdot m_{x_1} + \cdots + \mathrm{gr}_{\mathbb{Z}}\, x_r \cdot m_{x_r} \geq \mathrm{gr}_{\mathbb{Z}}\, x_1 + \cdots + \mathrm{gr}_{\mathbb{Z}}\, x_r.$$

Por tanto, $\mathrm{gr}_{\mathbb{Z}}\, x_i \leq d$ y el número de puntos x_i de grado m es menor o igual que d/m.

4. Notación: Dadas dos funciones continuas $f(x)$ y $g(x)$ en la semirrecta $x > 1$, escribiremos $f(x) \sim g(x)$ cuando $\lim_{x\to 1} \frac{f(x)}{g(x)}$ existe, es finito y no nulo.

Tenemos que $\zeta_K(x) \sim \frac{1}{x-1}$.

5. Lema: *Sea $m \geq 2$ un número natural y P cualquier conjunto de números primos. El producto $\prod_{p\in P}(1 - \frac{1}{p^{mx}})^{-1}$ define una función continua en la semirrecta $x > 1/2$.*

Demostración. La serie $\zeta(mx) = \sum_n (n^m)^{-x}$ es uniformemente convergente en los compactos de la semirrecta $x > 1/m$, por tanto la subserie formada por los términos correspondientes a los números n con todos sus factores primos en P es uniformemente convergente en los compactos de la semirrecta $x > 1/m$ y coincide con el productorio considerado. □

6. Teorema: *Se cumple que*

$$\zeta_K(x) \sim \prod_{\mathrm{gr}_{\mathbb{Z}}\, y = 1} (1 - \frac{1}{N(\mathfrak{p}_y)^x})^{-1}.$$

Demostración. Sea $P_{m,r} := \{\text{primos } p \in \mathbb{Z}, \text{ tales que el número de ideales primos de } A \text{ de grado } m \text{ sobre } \mathbb{Z} \text{ en la fibra de } (p) \text{ es } r\}$. Observemos que si $P_{m,r} \neq \emptyset$ entonces $m \cdot r \leq d$. Para cada $p \in P_{m,r}$ existen r ideales primos $\mathfrak{p}_y \subset A$ en la fibra de (p) de grado m sobre $\mathbb{Z}$ (observemos que $N(\mathfrak{p}_y) = |A/\mathfrak{p}_y| = p^m$).

Como

$$\begin{aligned}\zeta_K(x) &= \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \cdot \prod_{\mathrm{gr}_{\mathbb{Z}}\, y>1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \\ &= \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \cdot \prod_{m>1, mr\leq d} \prod_{p\in P_{m,r}} (1-\frac{1}{(p^m)^x})^{-r}\end{aligned}$$

y $\prod_{p\in P_{m,r}}(1-\frac{1}{(p^m)^x})^{-r}$ definen funciones continuas en la semirrecta $x > 1/2$ según 6.15.5, hemos concluido.

□

7. Notación: Sea K un cuerpo de números y A el anillo de enteros de K. Con abuso de notación, diremos que un ideal primo $\mathfrak{p} \subset A$ es un ideal primo de K.

8. Teorema: *Todo cuerpo de números tiene infinitos ideales primos de grado* 1 *sobre* $\mathbb{Z}$.

Demostración. Sigamos el argumento de Euler. Si K solo tuviera un número finito de primos de grado 1, entonces

$$\frac{1}{x-1} \sim \zeta_K(x) \sim \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1}$$

y $\lim_{x\to 1} \frac{\prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1}}{1/(x-1)} = \lim_{x\to 1} (x-1) \cdot \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} = 0$, lo que es contradictorio.

□

9. Nota Todo anillo de enteros A tiene un número infinito de ideales primos de grado 1 sobre $\mathbb{Z}$. Si $a \in A$ es no nulo, entonces A_a tiene un número infinito de ideales primos de grado 1 sobre $\mathbb{Z}$.

6.15.1. Aplicaciones

10. Corolario: *Todo polinomio no constante con coeficientes enteros* $q(x)$ *tiene infinitas raíces modulares. Más aún, hay infinitos números primos* p *en los que* $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ *tiene todas sus raíces en* $\mathbb{Z}/p\mathbb{Z}$.

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $q(x)$. La existencia de infinitos primos en $\mathbb{Q}[\alpha_1]$ de grado 1 sobre $\mathbb{Z}$, muestra que $q(x)$ tiene infinitas raíces raíces modulares. La existencia de infinitos primos en $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ de grado 1 sobre $\mathbb{Z}$, muestra que hay infinitos primos p en los que la reducción $\overline{q(x)}$ tiene todas sus raíces en $\mathbb{Z}/p\mathbb{Z}$. □

11. Corolario: *Dado $0 \neq n \in \mathbb{N}$, en la lista $\{1+mn, m \in \mathbb{N}\}$ existen infinitos números primos.*

Demostración. Tenemos que probar que existen infinitos primos p (podemos suponer que no dividen a n), tales que $p = 1 \in (\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$. Ahora bien, $p = 1 \mod n$ si y solo si el automorfismo de Fröbenius en p, F_p, de $\mathbb{Q}[e^{2\pi i/n}]$ es igual al morfismo Id, es decir, $\overline{x^n - 1} \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene todas sus raíces en $\mathbb{Z}/p\mathbb{Z}$ (y son distintas). □

12. Corolario: *Sea G un grupo abeliano finito. Existe una extensión de Galois $\mathbb{Q} \hookrightarrow K$ de grupo de Galois G.*

Demostración. Como G es un grupo finito abeliano entonces $G \simeq \overset{r}{\underset{i=1}{\oplus}} \mathbb{Z}/n_i\mathbb{Z}$. Por el corolario 6.15.11, existen números primos distintos $p_1, \ldots, p_r$ tales que $p_i = 1 \mod n_i$, para todo i, luego $p_i - 1 = m_i \cdot n_i$. Sea $n = p_1 \cdots p_r$. El grupo de Galois de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^* = \prod_i (\mathbb{Z}/p_i\mathbb{Z})^*$. Recordemos que $(\mathbb{Z}/p_i\mathbb{Z})^*$ es un grupo cíclico (ver 2.4.8). Sea $H_i = \langle \bar{n}_i \rangle \subset \mathbb{Z}/(p_i - 1)\mathbb{Z} \simeq (\mathbb{Z}/p_i\mathbb{Z})^*$ y $H = \prod_i H_i \subset (\mathbb{Z}/n\mathbb{Z})^*$. Entonces,

$$(\mathbb{Z}/n\mathbb{Z})^*/H = \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^*/H_i = \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \simeq G$$

y por la teoría de Galois, el grupo de Galois de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]^H$ es $(\mathbb{Z}/n\mathbb{Z})^*/H \simeq G$.

□

El teorema de Kronecker-Weber afirma que toda extensión finita de Galois de $\mathbb{Q}$ de grupo de Galois conmutativo es una subextensión de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$, para cierto n.

13. Lema: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q_1(x_1, \ldots, x_n) \\ &\cdots\cdots \\ 0 &= q_r(x_1, \ldots, x_n) \end{aligned}$$

tenga alguna solución compleja es que admita soluciones $\mathbb{Q}$-algebraicas

Demostración. Las soluciones complejas del sistema de ecuaciones diofánticas se corresponden biunívocamente, por el teorema de los ceros de Hilbert, con los ideales maximales de $\mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$. El sistema no tiene soluciones complejas si y solo si $0 = \mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$.

Igualmente, por el teorema de los ceros de Hilbert, el sistema no tiene soluciones algebraicas si y solo si $\mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$ no tiene ideales maximales, es decir, $0 = \mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$.

Concluimos porque $\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$ si y solo si $\mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$, ya que $\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=\mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)\otimes_{\mathbb{Q}}\mathbb{C}$.

□

14. Proposición: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0&=q_1(x_1,\ldots,x_n)\\ &\cdots\cdots\\ 0&=q_r(x_1,\ldots,x_n)\end{aligned}$$

tenga alguna solución compleja es que admita soluciones modulares en infinitos primos

Demostración. Si el sistema de ecuaciones diofánticas no tiene soluciones complejas, entonces $\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$, luego $\mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$. Es decir, existen polinomios $h_1,\ldots,h_r\in\mathbb{Q}[x_1,\ldots,x_n]$ tales que $\sum_i h_i q_i=1$. Multiplicando por $N\in\mathbb{N}$ conveniente tenemos que $\sum_i h_i' q_i=N$, con $h_1',\ldots,h_r'\in\mathbb{Z}[x_1,\ldots,x_n]$. Ahora es evidente que, salvo en los primos que dividan a N, la reducción $\bar{q}_1=0,\ldots,\bar{q}_r=0$ módulo p del sistema dado carece de soluciones en $\mathbb{Z}/p\mathbb{Z}$.

Recíprocamente, si el sistema considerado tiene alguna raíz compleja, entonces el sistema admite alguna solución en una extensión finita K de $\mathbb{Q}$. Sea A el anillo de enteros de K. Como $K=A\otimes_{\mathbb{Z}}\mathbb{Q}$, tal solución será

$$x_1=\frac{a_1}{m_1},\ldots,x_n=\frac{a_n}{m_n}$$

con $a_i\in A$ y $m_i\in\mathbb{Z}$. Sea $m=\prod_i m_i$, entonces $x_i=\frac{a_i}{m_i}\in A_m$, para todo i. Como el teorema 6.15.8 afirma la existencia de infinitos primos $\mathfrak{p}$ de grado 1 en A_m, se concluye la existencia de infinitos primos p, tales que el sistema considerado tiene solución en $\mathbb{Z}/p\mathbb{Z}=A/\mathfrak{p}$.

□

15. Definición: Sea K un cuerpo de números y A el anillo de enteros de K. Diremos que un ideal $\mathfrak{a}$ descompone totalmente en A (o con abuso de notación, en K) si $\mathfrak{a}=\mathfrak{p}_{x_1}\cdots\mathfrak{p}_{x_n}$ con $\mathrm{gr}_{\mathbb{Z}}\,x_i=1$, para todo i.

Observemos que $\mathfrak{a}$ descompone totalmente en A si y solo si todos los puntos de $(\mathfrak{a})_0$ son de grado 1. Sea $p(x)\in\mathbb{Z}[x]$ un polinomio, $K=\mathbb{Q}[x]/(p(x))$, p un número primo y supongamos que $\overline{p(x)}\in\mathbb{F}_p[x]$ no tiene raíces múltiples. Si A es el anillo de enteros de K, se cumple que $A/(p)=\mathbb{F}_p[x]/(\overline{p(x)})$. Entonces, (p) descompone totalmente en K si y solo si todas las raíces de $\overline{p(x)}\in\mathbb{F}_p[x]$ pertenecen a $\mathbb{F}_p$.

16. Teorema: *Sea K un cuerpo de números y $K \hookrightarrow L$ una extensión finita. Si casi todo primo de grado* 1 *sobre $\mathbb{Z}$ de K descompone totalmente en L, entonces $K = L$.*

Demostración. Sea $t = \dim_K L$. Por hipótesis, la fibra de casi todos los primos de grado 1 sobre $\mathbb{Z}$ de K está formada por t primos de L, de grado 1 sobre $\mathbb{Z}$. Además, cada primo de L de grado 1 sobre $\mathbb{Z}$, está sobre un primo de K de grado 1 sobre $\mathbb{Z}$. Luego,

$$\frac{1}{x-1} \sim \zeta_L(x) \sim \zeta_K(x)^t \sim (\frac{1}{x-1})^t$$

y $t = 1$. □

17. Corolario: *Si la reducción de $q(x) \in \mathbb{Z}[x]$ módulo p descompone totalmente en casi todo p, entonces $q(x)$ descompone totalmente en $\mathbb{Q}[x]$.*

Demostración. Podemos suponer que $q(x)$ es irreducible. Sea $K = \mathbb{Q}[x]/(q(x))$ y $A = \mathbb{Z}[x]/(q(x))$. Observemos que un primo $p \in \mathbb{Z}$ descompone totalmente en A si y solo si $\overline{q(x)}$ descompone totalmente en $\mathbb{Z}/p\mathbb{Z}[x]$. Por hipótesis, casi todo primo $p \in \mathbb{Z}$ descompone totalmente en K, luego por el teorema anterior, $\mathbb{Q} = K$ y $q(x) = \lambda \cdot (x - \alpha)$ en $\mathbb{Q}[x]$. □

18. Corolario: *Si un número entero es resto cuadrático módulo casi todo primo, entonces es un cuadrado perfecto.*

Demostración. Considérese en el corolario anterior $q(x) = x^2 - n$. □

19. Corolario: *Sea K un cuerpo de números y $K \to L, L'$ dos K-extensiones de Galois. Si casi todos los primos de K de grado* 1 *sobre $\mathbb{Z}$ que descomponen totalmente en L también descomponen totalmente en L', entonces $L' \subseteq L$. Sean $q_1(x), q_2(x) \in \mathbb{Z}[x]$. La condición necesaria y suficiente para que todas las raíces de $q_2(x)$ sean expresiones racionales de las raíces de $q_1(x)$ es que en casi todos los primos p en los que el automorfismo de Fröbenius de $q_1(x)$ sea trivial lo sea el automorfismo de Fröbenius de $q_2(x)$.*

Demostración. Dado un cuerpo de números Σ denotemos A_Σ el anillo de enteros de Σ.

Sea $\mathfrak{q} \subset A_L$ un ideal primo, que no sea de ramificación sobre A_K, que sea de grado 1 sobre $\mathbb{Z}$. Entonces, $\mathfrak{p} = \mathfrak{q} \cap A_K$ es de grado 1 sobre $\mathbb{Z}$. Al ser $K \to L$ de Galois, tenemos que $\mathfrak{p}$ descompone totalmente en L; luego también en L' (casi siempre) por hipótesis. Es decir, $A_L/\mathfrak{p}A_L$ y $A_{L'}/\mathfrak{p}A_{L'}$ son $A_K/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$-álgebras triviales.

El morfismo natural $A_L \otimes_{A_K} A_{L'} \to A_{LL'}$ es epiyectivo en casi todo punto, porque al localizar en el punto genérico de A_K, tenemos el epimorfismo $L \otimes_K L' \to LL'$. Por tanto, (casi siempre) $A_{LL'}/\mathfrak{p}A_{LL'}$ es una $\mathbb{Z}/p\mathbb{Z}$-álgebra trivial porque tenemos el epimorfismo

$$(A_L/\mathfrak{p}A_L) \otimes_{A_K/\mathfrak{p}} (A_{L'}/\mathfrak{p}A_{L'}) \to A_{LL'}/\mathfrak{p}A_{LL'}$$

Por tanto, $\mathfrak{q}$ descompone totalmente en LL', y el corolario anterior permite concluir que $L = LL'$, es decir, $L' \subseteq L$.

□

6.16. Problemas

1. Calcula el cierre entero de $\mathbb{Z}[\sqrt[2]{5}]$.

2. Prueba que el discriminante de todo cuerpo de números es congruente con $0, 1$ mód 4.

   Pista: El determinante $\det(\sigma_i(a_j))$, como todo determinante, es una suma de términos, cada uno afectado de un signo positivo o negativo. Sea P (resp. N) la suma de los términos positivos (resp. la suma de los términos negativos), entonces $\Delta = (P-N)^2 = (P+N)^2 - 4PN$.

3. Sea $\{e_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{R}^n\}_{i=1,\ldots,n}$ una base y $c_1, \ldots, c_n$ números reales positivos tales que $c_1 \cdots c_n > |\det((a_{ij}))|$. Prueba que existe $(m_1 \ldots, m_n) \in \mathbb{Z}^n \setminus \{0\}$ tal que

   $$|\sum_j a_{ij} m_j| < c_i, \ \forall i$$

4. Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Prueba que para todo ideal fraccionario I de K, existe $f \in I$ tal que $|\sigma(f)| < (N(I) \cdot \sqrt{\Delta_k} \cdot (\frac{2}{\pi})^s)^{1/d}$, para toda $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$.

5. Sea K un cuerpo de números de anillo e $I \subset K$ un ideal fraccionario. Sean $c_y > 0$, con $y \in X_\infty$ tales que

   $$\prod_{y \in X_\infty} c_y^{\mathrm{gr}\, y} > (\frac{2}{\pi})^s \cdot Vol(\mathcal{O}_\infty / I)$$

   Prueba que existe $0 \neq f \in I$, tal que $|f|_y < c_y$ para todo $y \in X_\infty$.

6. Sea K un cuerpo de números de anillo de enteros A. Prueba que existe un ideal $\mathfrak{a} \subseteq A$ tal que $N(\mathfrak{a}) \leq \frac{d!}{d^d} \cdot (\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

7. Prueba que el anillo de enteros de $\mathbb{Q}[\sqrt{n}]$ es un anillo de ideales principales, para $n = 5, 8, 11, -3, -4, -7, -8, -11$.

8. Prueba que si $\dim_{\mathbb{Q}} K >> 0$ entonces $|\Delta_K| >> 0$.

9. **La batalla de Hastings** (14 de octubre de 1066). "Los hombres de Harold permanecían bien juntos, como solían hacer, y formaban 13 escuadrones, con el mismo número de hombres en cada escuadrón, y hostigaban a los esforzados normandos que se aventuraban entrar en sus reductos; porque un único golpe de un hacha de guerra sajona podía romper sus lanzas y cortar sus mayas... Cuando Harold se lanzó el mismo al ataque, los sajones formaban una poderoso escuadrón de hombres, gritando las exclamaciones de guerra..." ¿Cuántos sajones había en la batalla de Hastings?

10. Sea K un cuerpo de números y $P \subset \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$ un subconjunto propio, tal que si $\sigma \in P$, y c es el automorfismo conjugar de $\mathbb{C}$, entonces $c \circ \sigma \in P$. Prueba que existe una unidad ϵ en el anillo de enteros de K, tal que $|\sigma(\epsilon)| < 1$, para todo $\sigma \in P$ y $|\sigma(\epsilon)| > 1$, para todo $\sigma \notin P$.

11. Prueba que $\mathbb{R}[x.y]/(x^2 + y^2 + 1)$ es un dominio de ideales principales y que no es un anillo euclídeo.

    Resolución: $A = \mathbb{R}[x, y]/(x^2 + y^2 + 1)$ es un anillo íntegro de dimensión de krull 1. Para ver que es d.i.p. basta ver que los ideales maximales $\mathfrak{m}$ son principales. Ahora bien, $A/\mathfrak{m}$ es una $\mathbb{R}$-extensión finita de $\mathbb{R}$ (teorema de los ceros de Hilbert) y no puede ser $\mathbb{R}$ (pues $x^2 + y^2 + 1 = 0$ no tiene soluciones reales), luego $A/\mathfrak{m} = \mathbb{C}$. Por tanto, $\bar{1}, \bar{x}, \bar{y}$ son linealmente dependientes en $A/\mathfrak{m}$, luego existen $a, b, c \in \mathbb{R}$ (no todos nulos simultáneamente) tales que $a + bx + cy \in \mathfrak{m}$, es fácil ver que $\dim_{\mathbb{R}} A/(a + bx + cy) = 2$, luego $\mathfrak{m} = (a + bx + cy)$.

    Veamos que A no es euclídeo:

    a. $\mathbb{R} - \{0\}$ son los invertibles de A: Sea $\tau : A \to A$ el automorfismo de $\mathbb{R}$-álgebras definido por $\tau(\bar{x}) = \bar{x}$ y $\tau(\bar{y}) = -\bar{y}$. $A = \mathbb{R}[x] \oplus \mathbb{R}[x] \cdot \bar{y}$ y $A^{\langle \tau \rangle} = \mathbb{R}[x]$. Dado $a \in A$ definimos $N : A \to \mathbb{R}[x]$, $N(a) := a \cdot \tau(a) \in A^{\langle \tau \rangle} = \mathbb{R}[x]$, que cumple que $N(ab) = N(a)N(b)$. Si a es invertible en A entonces $N(a)$ es invertible en $\mathbb{R}[x]$. Sea $p(x) + q(x) \cdot \bar{y} \in A$ invertible, tenemos que $N(p(x) + q(x) \cdot \bar{y}) = p(x)^2 - q(x)^2 \bar{y}^2 = p(x)^2 + q(x)^2(1 + x^2)$ es invertible, luego es un polinomio de grado cero. Esto solo es cierto si $p(x) \in \mathbb{R}$ y $q(x) = 0$.

    b. Supongamos que A es euclídeo y sea $c \in A - \mathbb{R}$ un elemento de grado mínimo. Podemos suponer que c es irreducible.

c. Todo elemento de A módulo (c) es igual a un elemento de $\mathbb{R}$, es decir, el morfismo $\mathbb{R} \to A/(c)$ es epiyectivo, es decir, $\mathbb{R} = A/(c)$ lo cual es imposible.

12. Prueba que $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es dip pero no es un anillo euclídeo.

Resolución: $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es el anillo de enteros de $K = \mathbb{Q}[\sqrt{-19}]$. Tenemos que comprobar que los ideales $\mathfrak{p}_x \subset A$ tales que $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|} = \sqrt{19}$ son principales. Sea $\mathfrak{p}_x$ tal que $\mathfrak{p}_x \cap \mathbb{Z} = (2)$. Como $A = \mathbb{Z}[x]/(x^2+x+5)$, entonces $\mathfrak{p}_x = (2)$ porque $A/(2) = \mathbb{F}_2[x]/(x^2+x+1)$ es un cuerpo. Sea $\mathfrak{p}_x$ tal que $\mathfrak{p}_x \cap \mathbb{Z} = (3)$. Se cumple que $\mathfrak{p}_x = (3)$, porque $A/(3) = \mathbb{F}_3[x]/(x^2+x+2)$ es un cuerpo. Con todo A es dip.

Supongamos que A es euclídeo. Por el teorema de Dirichlet, los invertibles, A^*, es el conjunto de las raíces de la unidad incluidas en $\mathbb{Q}[\sqrt{-19}]$, es decir, $\{\pm 1\}$. Sea $c \in A \setminus \{0,1,-1\}$ de grado mínimo. Podemos suponer que c es irreducible. Dado $z \in A \setminus \{0,1,-1\}$ tenemos que $z = z' \cdot c + r$, con $r \in \{0,1,-1\}$. Es decir, $A/(c) = \mathbb{F}_2$ ó $A = \mathbb{F}_3$. Por tanto, $A/(c)$ es un cociente de $A/(2)$ ó $A/(3)$, pero éstos son cuerpos de orden 4 y 9, luego es imposible.

13. Sea $C = \{(\lambda_i) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i \leq r} |\lambda_i| + \sum_{j>r} 2|\lambda_j| \leq t\}$. Prueba que

$$Vol(C) = 2^r \cdot (\frac{\pi}{2})^s \cdot \frac{t^{r+2s}}{(r+2s)!}.$$

Resolución: $Vol(C) = \int_C dx_1 \cdots dx_r \cdot dy_1 \cdot dz_1 \cdots dy_s \cdot dz_s$.. Cambiando a coordenadas polares $y_i = u_i \cdot \cos\theta_i, z_i = u_i \operatorname{sen}\theta_i$, tenemos

$$Vol(C) = \int_D u_1 \cdots u_s dx_1 \cdots dx_r \cdot du_1 \cdots du_s \cdot d\theta_1 \cdots d\theta_s,$$

Donde $D = \{(x,u,\theta) \in \mathbb{R}^{r+2s} : 0 \leq \theta_i \leq 2\pi, u_i \geq 0, |x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s \leq t\}$. Hagamos el cambio de coordenadas $2u_i = w_i$. Entonces, $Vol(C) = 2^r 4^{-s} (2\pi)^s I_{r,s}(t)$, donde

$$I_{r,s}(t) = \int_E w_1 \cdots w_s dx_1 \cdots dx_r \cdot dw_1 \cdots dw_s,$$

donde $E = \{(x,w) \in \mathbb{R}^{r+s} : x_i, w_i \geq 0,\ x_1 + \cdots + x_r + w_1 + \cdots + w_s \leq t\}$.. Tenemos que $I_{r,s}(t) = t^{r+2s} I_{r,s}(1)$. Reescribiendo el dominio como $x_2 + \cdots + x_r + w_1 + \cdots + w_s \leq t - x_1$, tenemos por el teorema de Fubini

$$I_{r,s}(1) = \int_0^1 I_{r-1,s}(1-x_1)dx_1 = \int_0^1 (1-x_1)^{r+2s-1} dx_1 \cdot I_{r-1,s}(1) = \frac{1}{r+2s} I_{r-1,s}(1),$$

y entonces por inducción $I_{r,s}(1) = \frac{1}{(r+2s)\cdots(2s+1)} \cdot I_{0,s}(1)$. De la misma manera

$$I_{0,s}(1) = \int_0^1 w_1 (1-w_1)^{2s-2} dw_1 \cdot I_{0,s-1}(1) = \frac{1}{2s \cdot (2s-1)} \cdot I_{0,s-1}(1),$$

de donde por inducción $I_{0,s}(1) = \frac{|}{(2s)!} I_{0,0}(1) = \frac{1}{(2s)!}$ y $I_{r,s}(1) = \frac{1}{(r+2s)!}$. Por tanto,

$$Vol(C) = 2^r \cdot (\frac{\pi}{2})^s \cdot \frac{t^{r+2s}}{(r+2s)!}.$$

Capítulo 7

Álgebra Conmutativa Homológica

7.1. Introducción

En este capítulo se aplican "técnicas homológicas" en el estudio de los anillos regulares, Cohen-Macaulay y Gorenstein y en el estudio de los morfismos planos y formalmente lisos.

Veamos cómo aparecen técnicas homológicas en Álgebra Conmutativa jugando con un ejemplo. Consideremos la sucesión de morfismos de $k[x_1,\ldots,x_n]$-módulos libres

$$0 \to k[x_1,\ldots,x_n]\cdot \mathbf{x_1}\wedge\ldots\wedge\mathbf{x_n} \xrightarrow{d_n} \cdots \to \bigoplus_{i_1<\cdots<i_r} k[x_1,\ldots,x_n]\cdot \mathbf{x_{i_1}}\wedge\ldots\wedge\mathbf{x_{i_r}} \xrightarrow{d_r} \cdots$$
$$\to k[x_1,\ldots,x_n]\cdot \mathbf{x_1}\oplus\cdots\oplus k[x_1,\ldots,x_n]\cdot \mathbf{x_n} \xrightarrow{d_1} k[x_1,\ldots,x_n] \to k[x_1,\ldots,x_n]/(x_1,\ldots,x_n)\to 0$$

con $d_r(\mathbf{x_{i_1}}\wedge\ldots\wedge\mathbf{x_{i_r}}) = \sum(-1)^{j-1}x_{i_j}\cdot\mathbf{x_{i_1}}\wedge\ldots\wedge\widehat{\mathbf{x_{i_j}}}\wedge\ldots\wedge\mathbf{x_{i_r}}$. No es difícil comprobar que esta sucesión de morfismos es exacta. Si $\mathcal{O}$ es un anillo local de ideal maximal $\mathfrak{m}$, $f_1,\ldots,f_n$ es un sistema mínimo generador de $\mathfrak{m}$ y en la sucesión anterior sustituimos $k[x_1,\ldots,x_n]$ por $\mathcal{O}$ y los x_i por los f_i, obtenemos una sucesión de morfismos (complejo de Koszul) de modo que $\operatorname{Im} d_r \subseteq \operatorname{Ker} d_{r-1}$. Probamos que la sucesión es exacta (es decir, $\operatorname{Ker} d_{r-1}/\operatorname{Im} d_r = 0$) si y solo si el anillo es regular (observemos que si $\mathcal{O}$ es regular completando por el ideal maximal obtendremos la sucesión escrita para el anillo de polinomios, completada). Así pues, en los anillos locales regulares $\mathcal{O}/\mathfrak{m}$ "se resuelve" por una sucesión finita de módulos libres y, como probaremos, todo módulo finito generado también es resoluble por una sucesión finita de módulos libres. Esta propiedad caracteriza a los anillos locales regulares y es el criterio de Serre de regularidad. Sea ahora $\{f_1,\ldots,f_n\}$ un sistema mínimo de parámetros (es decir, $(f_1,\ldots,f_n)_0 = \{\mathfrak{m}\}$ y $n = \dim\mathcal{O}$), si la sucesión considerada asociada es exacta se dice que $\mathcal{O}$ es un anillo de Cohen-Macaulay. Si además $\mathcal{O}/(f_1,\ldots,f_n)$ es un $\mathcal{O}/(f_1,\ldots,f_n)$-módulo inyectivo se dice que $\mathcal{O}$ es un anillo de Gorenstein. Probamos que dados $f_1,\ldots,f_n\in\mathfrak{m}$, la condición

necesaria y suficiente para que la sucesión de morfismos asociada sea exacta es que "formen una sucesión regular de funciones", es decir, que $\bar{f}_i$ no sea un divisor de cero en $\mathcal{O}/(f_1,\ldots,f_{i-1})$, para todo i.

El estudio de la deficiencia en la exactitud de las resoluciones de los módulos por módulos libres al tensarlas por un módulo, o al tomar homomorfismos en un módulo, constituye la base de la teoría homológica de los tores y extens.

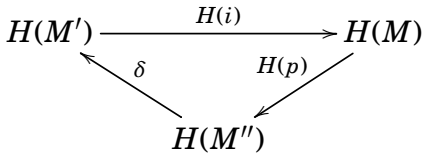
7.2. Módulos diferenciales. Homología

1. Definición: Un módulo diferencial es un A-módulo M dotado de un endomorfismo A-lineal $\mathrm{d}\colon M \to M$ de cuadrado nulo, $\mathrm{d}^2 = 0$. El morfismo d se denomina diferencial. Denotaremos $Z(M) = \operatorname{Ker}\mathrm{d}$, $B(M) = \operatorname{Im}\mathrm{d}$, los elementos de $Z(M)$ se denominan ciclos y los de $B(M)$ bordes. El cociente $H(M) = Z(M)/B(M)$ se denomina *grupo de cohomología* del módulo diferencial. Diremos que un módulo diferencial es acíclico si $H(M) = 0$.

2. Definición: Sean M y M' dos A-módulos diferenciales, de diferenciales respectivas d y d$'$. Un morfismo diferencial $\phi\colon M \to M'$ es un morfismo de A-módulos que conmuta con las diferenciales: $\phi \circ \mathrm{d} = \mathrm{d}' \circ \phi$.

Todo morfismo diferencial $\phi\colon M \to M'$ transforma ciclos en ciclos y bordes en bordes, luego induce un morfismo en cohomología, $H(\phi)\colon H(M) \to H(M')$, $\bar{c} \mapsto \overline{\phi(c)}$.

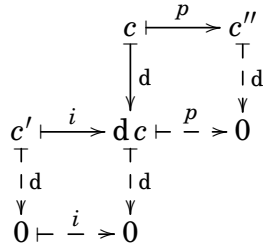
3. Proposición: *Sea* $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *una sucesión exacta de módulos, entre módulos diferenciales y morfismos diferenciales. Existe un morfismo de A-módulos* $\delta\colon H(M'') \to H(M)$ *tal que el triángulo*



es exacto. El morfismo δ se denomina morfismo de conexión.

Demostración. Comencemos definiendo δ. Dado un ciclo $c'' \in M''$, sea $c \in M$ una antimagen por p. Como p es un morfismo diferencial, $p(\mathrm{d}\,c) = \mathrm{d}(p(c)) = \mathrm{d}(c'') = 0$. Por tanto, existe $c' \in M'$ tal que $i(c') = d\,c$. Además, c' es un ciclo: $i(\mathrm{d}\,c') = \mathrm{d}(i(c')) = \mathrm{d}(\mathrm{d}\,c) = 0$, luego

$\mathrm{d}\,c' = 0$, porque i es inyectiva. Gráficamente hemos escrito



Con estas notaciones, definimos $\delta(\bar{c''}) := \bar{c'}$. Es fácil ver que no depende del c tomado ni del representante de $\bar{c''}$ considerado.

Tenemos que $H(i)(\delta(\bar{c''})) = H(i)(\bar{c'}) = \overline{\mathrm{d}\,c} = 0$. Además, dado $\bar{a} \in H(M')$, si $H(i)(\bar{a}) = \overline{i(a)} = 0$, entonces $i(a) = \mathrm{d}\,b$, luego $0 = p(\mathrm{d}(b)) = \mathrm{d}(p(b))$ y $\delta(\overline{p(b)}) = \bar{a}$. Con todo, hemos probado que $\mathrm{Im}\,\delta = \mathrm{Ker}\,H(i)$.

Dejamos como ejercicio probar el resto de la exactitud del triángulo.

□

4. Definición: Un *complejo* de A-módulos es un A-módulo graduado

$$K = \bigoplus_{i\in\mathbb{Z}} K^i$$

(K^i es un A-módulo, para todo i) diferencial, cuya diferencial cumple que $\mathrm{d}K^i \subseteq K^{i+1}$ (si la diferencial baja el grado en uno en vez de subirlo, se denota $K = \oplus K_i$).

La restricción de la diferencial a K^i, esto es, $\mathrm{d}\colon K^i \to K^{i+1}$, se denota d^i (o d_i si baja el grado en vez de subirlo).

Si K es un complejo, denotaremos $Z^i(K)$ al A-módulo de ciclos homogéneos de grado i y $B^i(K)$ al A-módulo de bordes homogéneos de grado i. El cociente $H^i(K) = Z^i(K)/B^i(K)$ se denomina i-ésimo grupo de cohomología (si la diferencial baja el grado en vez de subirlo, se denomina homología en vez de cohomología, y se denota $H_i(K)$). Como es obvio, se cumple que $Z(K) = \bigoplus_i Z^i(K)$, $B(K) = \bigoplus_i B^i(K)$ y $H(K) = \bigoplus_i H^i(K)$.

Un complejo K equivale a dar una sucesión de módulos y morfismos de módulos

$$\cdots \to K^{i-1} \xrightarrow{\mathrm{d}^{i-1}} K^i \xrightarrow{\mathrm{d}^i} K^{i+1} \xrightarrow{\mathrm{d}^{i+1}} \cdots$$

tal que la imagen de cada morfismo está contenido en el núcleo del siguiente. Los grupos de cohomología $H^i(K)$ miden la deficiencia en la exactitud y su anulación equivale a la exactitud de la sucesión.

5. Ejemplo: Consideremos un poliedro (no precisamos una definición) r-dimensional de n vértices $\{a_1,\dots,a_n\}$. Una arista viene definida por un par de vértices $l^{ij}=\{a_i,a_j\}$, una cara por tres vértices $C^{ijk}=\{a_i,a_j,a_k\}$, y en general, un símplice de orden p por $p+1$ vértices $S_p^\alpha=\{a_{i_0},\dots,a_{i_p}\}$, con $\alpha=\{i_0,\dots,i_p\}$. Denotemos por $M_p=\sum\limits_\alpha \mathbb{Q}\cdot S_p^\alpha$ el $\mathbb{Q}$-módulo libre generado por todos los símplices S_p^α de orden p del poliedro. El módulo

$$M=\bigoplus_{p=0}^{r} M_p$$

es el *módulo graduado diferencial de cadenas sobre el poliedro*, con la diferencial de grado -1 definida como sigue

$$\mathrm{d}_p\{a_{i_0},\dots,a_{i_p}\}=\sum_{j=0}^{p}(-1)^j\{a_{i_0},\dots,\widehat{a_{i_j}},\dots,a_{i_p}\}$$

Se cumple que $\mathrm{d}_p\circ\mathrm{d}_{p+1}=0$. La homología del complejo de cadenas sobre el poliedro es por definición, $H(M)=\bigoplus\limits_{p=0}^{p}\mathrm{Ker}\,\mathrm{d}_p/\mathrm{Im}\,\mathrm{d}_{p+1}$.

La dimensión de los grupos de homología de M son invariantes topológicos esenciales del poliedro. Se llama característica del poliedro a $\chi(M):=\sum\limits_{i=0}^{r}(-1)^i\dim_{\mathbb{Q}}H_i(M)$ y se verifica

$$\chi(M)=n^0\text{ vértices }-n^0\text{ aristas }+n^0\text{ caras }+\dots+(-1)^r n^0\text{ r-símplices}$$

Por ejemplo, si un poliedro está inscrito en una esfera, entonces

$$\chi(M)=n^0\text{ vértices }-n^0\text{ aristas }+n^0\text{ caras }=2$$

Si el poliedro está inscrito en un toro de g asas, entonces $\chi(M)=2-2g$.

6. Definición: Un morfismo de complejos $f:K\to L$ es un morfismo diferencial y graduado (es decir, $f(K^n)\subset L^n$). Se dice que un morfismo de complejos es un cuasi-isomorfismo si el morfismo inducido en cohomología es un isomorfismo.

Se dice que una sucesión de morfismos de complejos $0\to K'\to K\to K''\to 0$ es exacta si es exacta como sucesión de morfismos de A-módulos. Si es exacta el triángulo de cohomología define la siguiente sucesión exacta larga de cohomología:

$$\cdots\to H^i(K'')\xrightarrow{\delta}H^{i+1}(K'')\to H^{i+1}(K)\to H^{i+1}(K'')\xrightarrow{\delta}H^{i+2}(K')\to\cdots$$

7. Lema de la serpiente: *Sea*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N'' & \longrightarrow & 0 \end{array}$$

un diagrama conmutativo de morfismos de A-módulos, de filas exactas. Existe un morfismo

$$\delta\colon \operatorname{Ker} f'' \to \operatorname{Coker} f'$$

tal que la sucesión de morfismos

$$0 \to \operatorname{Ker} f' \xrightarrow{i} \operatorname{Ker} f \xrightarrow{p} \operatorname{Ker} f'' \xrightarrow{\delta} \operatorname{Coker} f' \xrightarrow{j} \operatorname{Coker} f \xrightarrow{q} \operatorname{Coker} f'' \to 0$$

es exacta.

Demostración. Sea $L = L^0 \oplus L^1$, donde $L^0 = M$, $L^1 = N$, y $\mathrm{d}\colon L \to L$ el morfismo definido por $d(m,n) := (0, f(m))$. Es de inmediata comprobación que (L,d) es un complejo diferencial y que $H(L) = \operatorname{Ker} f \oplus \operatorname{Coker} f$. De modo análogo definimos los módulos diferenciales L' y L''. Las hipótesis nos dicen que

$$0 \to L' \xrightarrow{i \oplus j} L \xrightarrow{p \oplus q} L'' \to 0$$

es una sucesión exacta de complejos. La sucesión exacta larga de cohomología es justamente la sucesión exacta requerida. □

8. Definiciones: Dado un complejo K denotaremos por $K[n]$ el complejo definido por: $K[n]^p := K^{n+p}$ y $d_{K[n]} := (-1)^n d_K$.

Si $\{M_i, \mathrm{d}_i\}_{i \in I}$ son complejos, podemos definir la suma directa $\underset{i \in I}{\oplus} M_i$, que es un complejo con la graduación

$$(\underset{i}{\oplus} M_i)^n = \underset{i}{\oplus} M_i^n$$

y con la diferencial $\mathrm{d} = \oplus\, \mathrm{d}_i$.

Bicomplejos

9. Definición: Un bicomplejo de A-módulos es un A-módulo bigraduado

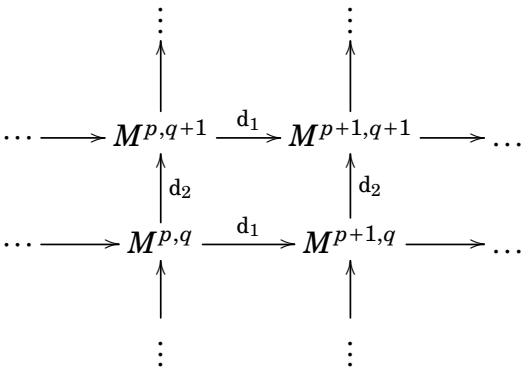
$$M = \underset{p,q \in \mathbb{Z}}{\oplus} M^{p,q}$$

dotado de dos diferenciales: una diferencial "horizontal" $\mathrm{d}_1 \colon M^{p,q} \to M^{p+1,q}$ y otra "vertical" $\mathrm{d}_2 \colon M^{p,q} \to M^{p,q+1}$ tales que:

$$\mathrm{d}_1^2 = 0, \quad \mathrm{d}_2^2 = 0, \quad \mathrm{d}_1 \circ \mathrm{d}_2 = \mathrm{d}_2 \circ \mathrm{d}_1 .$$

Por tanto, dar un bicomplejo equivale a dar un diagrama conmutativo

$(*)$



de filas y columnas complejos.

Si M es un bicomplejo, tiene dos estructuras naturales de complejo: por columnas y por filas. Con más precisión, si denotamos $M^{p,\cdot} = \oplus_q M^{p,q}$, entonces M es un complejo con la graduación $M = \oplus_p M^{p,\cdot}$ y la diferencial d_1. Análogamente, si denotamos $M^{\cdot,q} = \oplus_p M^{p,q}$, entonces M es un complejo con la graduación $M = \oplus_q M^{\cdot,q}$ y la diferencial d_2. Denotaremos por (M, d_1) y (M, d_2) estas dos estructuras de complejo de M, y por $H^n_{\mathrm{d}_1}(M)$, $H^n_{\mathrm{d}_2}(M)$ a sus cohomologías respectivas. Obsérvese además que $M^{p,\cdot}$ es un complejo con la diferencial d_2, de modo que (M, d_2) es la suma directa de los complejos $M^{p,\cdot}$. Igualmente, $M^{\cdot,q}$ es un complejo con la diferencial d_1, de modo que (M, d_1) es la suma directa de los complejos $M^{\cdot,q}$. $H^n_{d_1}(M)$ es un complejo con la graduación

$$H^n_{\mathrm{d}_1}(M) = \oplus_q H^n_{\mathrm{d}_1}(M^{\cdot,q})$$

y la diferencial d_2. Análogamente, $H^n_{\mathrm{d}_2}(M)$ es un complejo con la graduación

$$H^n_{\mathrm{d}_2}(M) = \oplus_p H^n_{\mathrm{d}_2}(M^{p,\cdot})$$

y la diferencial d_1. Veamos ahora una estructura de complejo en M que implica a ambas diferenciales.

10. Definición: Llamaremos complejo simple asociado a un bicomplejo M, al complejo $M^{\cdot}$ cuya graduación es

$$M^n = \bigoplus_{p+q=n} M^{p,q}$$

y cuya diferencial $\mathrm{d}\colon M^n \to M^{n+1}$ es $\mathrm{d} = \mathrm{d}_1 + (-1)^p \mathrm{d}_2$ sobre $M^{p,q}$. Obsérvese que los M^n son las diagonales (de pendiente -1) del diagrama $(*)$.

Si bien la diferencial del complejo simple depende en su definición del orden en el que se consideran d_1 y d_2, si definimos $\mathrm{d}' = \mathrm{d}_2 + (-1)^q \mathrm{d}_1$ sobre $M^{p,q}$, se verifica que el morfismo $(M,\mathrm{d}) \to (M,\mathrm{d}')$, $m_{p,q} \mapsto (-1)^{pq} m_{p,q}$ es un morfismo de complejos y es un cuasi-isomorfismo.

11. Ejemplos:

1. Sean (M,d_M) y (N,d_N) dos complejos. Entonces $\bigoplus_{p,q} (M^p \otimes N^q)$ es un bicomplejo, con las diferenciales $\mathrm{d}_1 = \mathrm{d}_M \otimes 1$, $\mathrm{d}_2 = 1 \otimes \mathrm{d}_N$. Llamaremos complejo producto tensorial, $M \otimes N$, al complejo simple asociado al bicomplejo anterior.

2. También $\bigoplus_{p,q} \mathrm{Hom}(M^{-q}, N^p)$ es un bicomplejo, con las diferenciales

$$\mathrm{d}_1\colon \mathrm{Hom}(M^{-q},N^p) \to \mathrm{Hom}(M^{-q},N^{p+1}), \quad f \mapsto \mathrm{d}_N \circ f$$
$$\mathrm{d}_2\colon \mathrm{Hom}(M^{-q},N^p) \to \mathrm{Hom}(M^{-q-1},N^p), \quad f \mapsto (-1)^q f \circ \mathrm{d}_M$$

   Se denota $\mathrm{Hom}^n(M,N) = \prod_i \mathrm{Hom}(M^i, N^{i+n})$. Llamaremos complejo de homomorfismos, $\mathrm{Hom}^{\cdot}(M,N)$, al complejo cuya graduación es

$$\mathrm{Hom}^{\cdot}(M,N) = \bigoplus_n \mathrm{Hom}^n(M,N)$$

   y cuya diferencial es $\mathrm{d} = \mathrm{d}_1 + (-1)^p \mathrm{d}_2$ sobre $\mathrm{Hom}(M^{-q},N^p)$. Este complejo coincide con el complejo simple asociado al bicomplejo $\bigoplus_{p,q} \mathrm{Hom}(M^{-q},N^p)$ cuando la suma directa $\bigoplus_i \mathrm{Hom}(M^i,N^{i+n})$ coincida con el producto directo $\prod_i \mathrm{Hom}(M^i,N^{i+n})$, por ejemplo si M está acotado por la derecha y N está acotado por la izquierda (ver definición 7.2.14).

3. Un morfismo de complejos $f\colon M \to N$ se puede pensar como un bicomplejo con dos columnas, la columna -1 es M y la columna 0 es N, de diferencial horizontal f y diferencial vertical las diferenciales que tenemos en M y N. El complejo simple asociado se denomina el cono de f.

12. Definición: Dado un morfismo de complejos $f\colon K \to L$, llamaremos cono de f al complejo $\mathrm{Cono}(f)$ cuya graduación es $\mathrm{Cono}(f)^n = K^{n+1} \oplus L^n$ y cuya diferencial es

$$\mathrm{d}_{\mathrm{Cono}(f)} = \begin{pmatrix} -\mathrm{d}_K & 0 \\ f & \mathrm{d}_L \end{pmatrix}$$

El cono de f está dotado de morfismos de complejos naturales:

$$\mathrm{Cono}(f) \to K[1],\ (k,l) \mapsto k \qquad L \to \mathrm{Cono}(f),\ l \mapsto (l,0),$$

y se tiene una sucesión exacta de complejos

$$0 \to L \to \mathrm{Cono}(f) \to K[1] \to 0,$$

13. Proposición: *Un morfismo de complejos $f : K \to L$ es cuasi-isomorfismo si y solo si su cono es acíclico.*

Demostración. Se deduce de la sucesión exacta larga de cohomología asociada a la sucesión exacta de complejos $0 \to L \to \mathrm{Cono}(f) \to K[1] \to 0$, teniendo en cuenta que el morfismo de conexión de dicha sucesión exacta coincide con $H(f)$. □

14. Definición: Se dice que un bicomplejo M es de diagonales acotadas por la izquierda (respectivamente, por la derecha) si para cada n existe un p_n tal que $M^{p,n-p} = 0$ para todo $p < p_n$ (respectivamente, $p > p_n$).

15. Teorema: *Sea M un bicomplejo de diagonales acotadas por la izquierda (respectivamente por la derecha). Si $H_{\mathrm{d}_2}(H_{\mathrm{d}_1}(M)) = 0$ (respectivamente $H_{\mathrm{d}_1}(H_{\mathrm{d}_2}(M)) = 0$), entonces el complejo simple asociado es acíclico, i.e., $H(M) = 0$.*

Demostración. Consideremos la sucesión exacta de complejos simples obvia

$$0 \to \mathrm{Ker}\,\mathrm{d}_1 \to M \xrightarrow{\mathrm{d}_1} \mathrm{Im}\,\mathrm{d}_1[1] \to 0$$

Hay que probar que el morfismo de conexión

$$\delta : H^n(\mathrm{Im}\,\mathrm{d}_1) \to H^n(\mathrm{Ker}\,\mathrm{d}_1),\ \delta(\overline{\mathrm{d}_1 m_{p,q}}) = \overline{\mathrm{d}_1 m_{p,q} + (-1)^p \mathrm{d}_2 m_{p,q}}$$

es isomorfismo.

Como $\mathrm{Im}\,\mathrm{d}_1$ y $\mathrm{Ker}\,\mathrm{d}_1$ tienen diferencial horizontal nula, se cumple que

$$H^n(\mathrm{Im}\,\mathrm{d}_1) = \underset{p}{\oplus} H^{n-p}_{\mathrm{d}_2}((\mathrm{Im}\,\mathrm{d}_1)^{p,\cdot}), \qquad H^n(\mathrm{Ker}\,\mathrm{d}_1) = \underset{p}{\oplus} H^{n-p}_{\mathrm{d}_2}((\mathrm{Ker}\,\mathrm{d}_1)^{p,\cdot}).$$

Consideremos en ambos los submódulos

$$F_r := \underset{p \le r}{\oplus} H^{n-p}_{\mathrm{d}_2}((\mathrm{Im}\,\mathrm{d}_1)^{p,\cdot}), \qquad F'_r := \underset{p \le r}{\oplus} H^{n-p}_{\mathrm{d}_2}((\mathrm{Ker}\,\mathrm{d}_1)^{p,\cdot}).$$

Por ser M de diagonales acotadas por la izquierda, se obtiene que $F_r = F'_r = 0$ para $r << 0$. F_s y F'_s son completos y separados con las filtraciones $\{F_i\}_{i \le s}$ y $\{F'_i\}_{i \le s}$, para

todo $s \geq r$. Tenemos que $H^n(\operatorname{Im} \mathrm{d}_1) = \bigcup_{s=r}^{\infty} F_s$ y $H^n(\operatorname{Ker} \mathrm{d}_1) = \bigcup_{s=r}^{\infty} F'_s$. El morfismo δ es compatible con las filtraciones, luego para que sea isomorfismo basta que lo sea el morfismo inducido en los graduados,

$$G(H^n(\operatorname{Im} \mathrm{d}_1)) \xrightarrow{G(\delta)} G(H^n(\operatorname{Ker} \mathrm{d}_1))$$

que viene dado por $G(\delta)(\overline{\mathrm{d}_1 m}) = \overline{\mathrm{d}_1 m}$, luego coincide con el morfismo inducido en los graduados por el morfismo $H(i)\colon H^n(\operatorname{Im} \mathrm{d}_1) \to H^n(\operatorname{Ker} \mathrm{d}_1)$ asociado a la inclusión $i\colon \operatorname{Im} \mathrm{d}_1 \to \operatorname{Ker} \mathrm{d}_1$. Este último es isomorfismo, como se deduce de la sucesión exacta

$$0 \to \operatorname{Im} \mathrm{d}_1 \xrightarrow{i} \operatorname{Ker} \mathrm{d}_1 \to H_{\mathrm{d}_1}(M) \to 0$$

ya que $H_{\mathrm{d}_1}(M)$ es acíclico por hipótesis. □

16. Teorema: *Sea $f\colon M \to N$ un morfismo de bicomplejos. Supongamos que M y N son de diagonales acotadas por la izquierda. Si el morfismo inducido*

$$H_{\mathrm{d}_2}(H_{\mathrm{d}_1}(M)) \to H_{\mathrm{d}_2}(H_{\mathrm{d}_1}(N))$$

es isomorfismo entonces el morfismo $M^{\cdot} \to N^{\cdot}$ entre los complejos simples asociados es un cuasi-isomorfismo.

Análogamente, supongamos que M y N son de diagonales acotadas por la derecha. Si el morfismo inducido

$$H_{\mathrm{d}_1}(H_{\mathrm{d}_2}(M)) \to H_{\mathrm{d}_1}(H_{\mathrm{d}_2}(N))$$

es isomorfismo entonces el morfismo $M^{\cdot} \to N^{\cdot}$ entre los complejos simples asociados es un cuasi-isomorfismo.

Demostración. Podemos considerar $f\colon M^{\cdot,\cdot} \to N^{\cdot,\cdot}$ como un tricomplejo de diferenciales, con las notaciones obvias, $\mathrm{d}_1, \mathrm{d}_2, \mathrm{d}_3 = f$. Cuando consideremos la diferencial simple asociada a dos diferenciales la denotaremos como la suma de las dos diferenciales. Ahora ya, como el morfismo $H_{\mathrm{d}_1}(f)\colon H_{\mathrm{d}_1}(M) \to H_{\mathrm{d}_1}(N)$ es un cuasi-isomorfismo $\overset{7.2.13}{\Rightarrow} 0 = H_{\mathrm{d}_3+\mathrm{d}_2}(\operatorname{Cono}(H_{\mathrm{d}_1}(f))) = H_{\mathrm{d}_3+\mathrm{d}_2}(H_{\mathrm{d}_1}(\operatorname{Cono}(f))) \overset{7.2.15}{\Rightarrow} 0 = H_{(\mathrm{d}_3+\mathrm{d}_2)+\mathrm{d}_1}(\operatorname{Cono}(f)) = H_{\mathrm{d}_3+(\mathrm{d}_2+\mathrm{d}_1)}(\operatorname{Cono}(f)) \overset{7.2.13}{\Rightarrow} f\colon M \to N$ es un cuasi-isomorfismo. □

17. Corolario: *Sea M un bicomplejo de diagonales acotadas por la izquierda (respectivamente, de diagonales acotadas por la derecha). Si existe un n tal que*

$$H^i_{\mathrm{d}_1}(M) = 0, \text{ para todo } i \neq n$$

(respectivamente, $H^i_{\mathrm{d}_2}(M)=0$*, para todo* $i\neq n$*), entonces*

$$H^{i+n}(M^{\cdot})=H^i_{\mathrm{d}_2}(H^n_{\mathrm{d}_1}(M))$$

(respectivamente, $H^{i+n}(M^{\cdot})=H^i_{\mathrm{d}_1}(H^n_{\mathrm{d}_2}(M))$*).*

Demostración. Sea $M^{\leq n,\cdot}$ el bicomplejo

$$M^{\leq n,\cdot}=\cdots\to M^{n-2,\cdot}\to M^{n-1,\cdot}\to \operatorname{Ker}\mathrm{d}_1^n\to 0\cdots$$

Es inmediato que $H^i_{\mathrm{d}_1}(M^{\leq n,\cdot})=\begin{cases}H^i_{\mathrm{d}_1}(M^{\cdot}) & \text{para } i\leq n.\\ 0 & \text{para } i>n.\end{cases}$

Por las hipótesis y el teorema 7,2,15, los morfismos

$$H^n_{\mathrm{d}_1}(M)[-n]\leftarrow M^{\leq n,\cdot}\to M^{\cdot}$$

son cuasi-isomorfismos, luego $H^i(M^{\cdot})=H^i(H^n_{\mathrm{d}_1}(M)[-n])=H^{i-n}_{\mathrm{d}_2}(H^n_{\mathrm{d}_1}(M))$. □

7.3. Tores y Extens

1. Definición: Sea A un A-módulo. Diremos que una sucesión exacta de A-módulos

$$\cdots\to L_n\to L_{n-1}\to\cdots\to L_1\to L_0\to N\to 0,$$

siendo L_i módulos libres, para todo i, es una resolución de N por módulos libres. La denotaremos $L_{\cdot}\to N$.

2. Definición: Sean M y N dos A-módulos. Sea $L_{\cdot}\to N$ una resolución de N por módulos libres. Denotaremos $\operatorname{Tor}_i(N,M)=H_i(L_{\cdot}\otimes M)$, y se denomina i-ésimo módulo de torsión de N y M. Cuando queramos explicitar el anillo, escribiremos $\operatorname{Tor}_i=\operatorname{Tor}_i^A$.

3. Proposición: $\operatorname{Tor}_i(N,M)$ *no depende de la resolución por libres de* N *escogida y* $\operatorname{Tor}_i(N,M)=\operatorname{Tor}_i(M,N)$.

Demostración. Sean $L_{\cdot}\to N$ y $L'_{\cdot}\to M$, resoluciones por libres. Consideremos el bicomplejo $L_{\cdot}\otimes L'_{\cdot}$. Observemos que $H_{i,d_2}(L_{\cdot}\otimes L'_{\cdot})=L_{\cdot}\otimes H_{i,d_2}(L'_{\cdot})=0$, para todo $i\neq 0$, y $H_{0,d_2}(L_{\cdot}\otimes L'_{\cdot})=L_{\cdot}\otimes M$. Igualmente, $H_{i,d_1}(L_{\cdot}\otimes L'_{\cdot})=0$, para $i\neq 0$ y $H_{0,d_1}(L_{\cdot}\otimes L'_{\cdot})=N\otimes L'_{\cdot}$. Por tanto,

$$\operatorname{Tor}_i(N,M)=H_i(L_{\cdot}\otimes M)\overset{7.2.17}{=}H_i(L_{\cdot}\otimes L'_{\cdot})\overset{7.2.17}{=}H_i(N\otimes L'_{\cdot})=\operatorname{Tor}_i(M,N).$$

□

4. Proposición: $\mathrm{Tor}_0(N,M) = M \otimes N$.

Demostración. Es consecuencia inmediata de la exactitud del producto tensorial por la derecha. □

Dada una sucesión exacta de A-módulos $0 \to N_1 \to N_2 \to N_3 \to 0$ y una resolución por libres $L'_\cdot \to M$, tenemos la sucesión exacta de complejos

$$0 \to N_1 \otimes L'_\cdot \to N_2 \otimes L'_\cdot \to N_3 \otimes L'_\cdot \to 0$$

que define la sucesión exacta larga de homología de los tores

$$\cdots \to \mathrm{Tor}_i(N_1,M) \to \mathrm{Tor}_i(N_2,M) \to \mathrm{Tor}_i(N_3,M) \to \mathrm{Tor}_{i-1}(N_1,M) \to \cdots$$
$$\to \mathrm{Tor}_1(N_1,M) \to \mathrm{Tor}_1(N_2,M) \to \mathrm{Tor}_1(N_3,M) \to N_1 \otimes M \to N_2 \otimes M \to N_3 \otimes M \to 0$$

De esta sucesión se deduce fácilmente la siguiente proposición.

5. Proposición: *M es plano* $\Leftrightarrow \mathrm{Tor}_i(M,-) = 0$ *para todo* $i > 0 \Leftrightarrow \mathrm{Tor}_1(M,-) = 0$.

Como todo módulo N es límite inductivo de sus submódulos finito generados y la toma de límites inductivos es exacta, para ver que M es plano basta ver que $\mathrm{Tor}_1(M,N) = 0$ cuando N es finito generado. Por inducción sobre el número mínimo de generadores y la sucesión exacta larga de los tores, podemos suponer que N es monógeno. Es decir, M es plano si y solo si $\mathrm{Tor}_1(M,A/I) = 0$ para todo ideal I. Por último, $\mathrm{Tor}_1(M,A/I) = 0$ si y solo si $I \otimes_A M = I \cdot M$, como se deduce de la sucesión exacta larga de tores obtenida al tensar la sucesión exacta $0 \to I \to A \to A/I \to 0$ por M. Hemos obtenido por tanto la siguiente proposición:

6. Proposición: *Un A-módulo M es plano si y solo si $I \otimes_A M = I \cdot M$, para todo ideal $I \subset A$.*

7. Proposición: *Sea $A \to B$ un morfismo de anillos plano y M, N dos A-módulos. Entonces,*

$$\mathrm{Tor}_i^A(M,N) \otimes_A B = \mathrm{Tor}_i^B(M \otimes_A B, N \otimes_A B)$$

Demostración. Sea $L_\cdot$ una resolución por A-módulos libres de M. Entonces, $L_\cdot \otimes_A B$ es una resolución por B-módulos libres de $M \otimes_A B$ y

$$\mathrm{Tor}_i^A(M,N) \otimes_A B = H_i(L_\cdot \otimes_A N) \otimes_A B = H_i(L_\cdot \otimes_A N \otimes_A B) = H_i((L_\cdot \otimes_A B) \otimes_B (N \otimes_A B))$$
$$= \mathrm{Tor}_i^B(M \otimes_A B, N \otimes_A B).$$

□

Dado un A-módulo M, existe un morfismo inyectivo $M \to I^0$, para cierto A-módulo inyectivo I^0. Sea $M_1 := I^0/M$ y sea $M_1 \to I^1$ un morfismo inyectivo en un cierto módulo inyectivo I^1. Sea $M_2 := I^1/M_1$ y sea $M_2 \to I^2$ un morfismo inyectivo en un cierto módulo inyectivo I^2. Así sucesivamente vamos definiendo los módulos inyectivos I^n, $n \in \mathbb{N}$. Si consideremos el morfismo composición $I^n \to I^n/M_n \to I^{n+1}$, para todo n, se cumple que

$$M \to I^0 \to I^1 \to \cdots \to I^n \to \cdots$$

es acíclico y diremos que $M \to I^{\cdot}$ es una resolución de M por módulos inyectivos.

Sea $P_{\cdot} \to N$ una resolución de N por módulos proyectivos y $M \to I^{\cdot}$ una resolución de M por módulos inyectivos. Se verifica que

$$H^i(\mathrm{Hom}(P_{\cdot}, M)) \overset{7.2.17}{=} H^i(\mathrm{Hom}^{\cdot}(P_{\cdot}, I^{\cdot})) \overset{7.2.17}{=} H^i(\mathrm{Hom}(N, I^{\cdot}))$$

En particular, podemos definir

$$\mathrm{Ext}^i(N,M) := H^i(\mathrm{Hom}(P_{\cdot}, M)) \quad \text{ó} \quad \mathrm{Ext}^i(N,M) := H^i(\mathrm{Hom}(N, I^{\cdot}))$$

y la definición no depende de las resoluciones escogidas. De la exactitud de $\mathrm{Hom}(N,-)$ por la izquierda se deduce que $\mathrm{Ext}^0(N,M) = \mathrm{Hom}(N,M)$.

Una sucesión exacta de módulos $0 \to M_1 \to M_2 \to M_3 \to 0$ induce una sucesión exacta de complejos $0 \to \mathrm{Hom}(P_{\cdot}, M_1) \to \mathrm{Hom}(P_{\cdot}, M_2) \to \mathrm{Hom}(P_{\cdot}, M_3) \to 0$, que induce la sucesión exacta larga de los extens

$$\cdots \to \mathrm{Ext}^i(N,M_1) \to \mathrm{Ext}^i(N,M_2) \to \mathrm{Ext}^i(N,M_3) \to \mathrm{Ext}^{i+1}(N,M_1) \to \cdots$$

Análogamente, una sucesión exacta $0 \to N_1 \to N_2 \to N_3 \to 0$ induce una sucesión exacta de complejos $0 \to \mathrm{Hom}(N_3, I^{\cdot}) \to \mathrm{Hom}(N_2, I^{\cdot}) \to \mathrm{Hom}(N_1, I^{\cdot}) \to 0$, que induce la sucesión exacta larga de los extens

$$\cdots \to \mathrm{Ext}^i(N_3,M) \to \mathrm{Ext}^i(N_2,M) \to \mathrm{Ext}^i(N_1,M) \to \mathrm{Ext}^{i+1}(N_3,M) \to \cdots$$

8. Proposición: *Sea M un A-módulo. Las siguientes condiciones son equivalentes:*

1. *M es un A-módulo inyectivo.*
2. *$\mathrm{Ext}^i_A(N,M) = 0$, para todo $i > 0$ y todo A-módulo N.*
3. *$\mathrm{Ext}^1_A(N,M) = 0$, para todo A-módulo N.*
4. *$\mathrm{Ext}^1_A(A/I,M) = 0$, para todo ideal $I \subseteq A$. Si A es noetheriano, basta tomar como ideales los ideales primos de A.*

Demostración. 1. $\Rightarrow$ 2. Sea $L_\cdot \to N \to 0$ una resolución por A-módulos libres de N. Entonces, $\mathrm{Ext}^i_A(N,M) = H^i(\mathrm{Hom}_A(L_\cdot,N)) = 0$, para todo $i>0$.

2. $\Rightarrow$ 3. y 3. $\Rightarrow$ 4. son obvios.

4. $\Rightarrow$ 1. La primera parte es consecuencia del criterio del ideal 0.12.3 y de la sucesión exacta larga de extens. Si A es un anillo noetheriano, A/I admite una cadena $0 \subset N_0 \subset \cdots \subset N_r = A/I$ tal que $N_i/N_{i-1} \simeq A/\mathfrak{p}_i$, con $\mathfrak{p}_i$ primo. De la sucesión exacta larga de los extens se deduce fácilmente que si $\mathrm{Ext}^1_A(A/\mathfrak{p}_i,M)=0$ para todo i, entonces $\mathrm{Ext}^1_A(A/I,M)=0$, con lo que se concluye. □

9. Proposición: *Sea A un anillo noetheriano y $A \to B$ un morfismo de anillos plano. Sea M un A-módulo finito generado y N un A-módulo. Entonces,*

$$\mathrm{Ext}^i_A(M,N)\otimes_A B = \mathrm{Ext}^i_B(M\otimes_A B, N\otimes_A B), \text{ para todo } i.$$

Demostración. Sea $L_\cdot \to M$ una resolución de M por A-módulos libres finito generados. Entonces,

$$\begin{aligned}\mathrm{Ext}^i_A(M,N)\otimes_A B &= H^i(\mathrm{Hom}_A(L_\cdot,N))\otimes_A B = H^i(\mathrm{Hom}_A(L_\cdot,N)\otimes_A B)\\ &= H^i(\mathrm{Hom}_B(L_\cdot\otimes_A B, N\otimes_A B)) = \mathrm{Ext}^i_B(M\otimes_A B, N\otimes_A B).\end{aligned}$$

□

10. Corolario: *Sea A un anillo noetheriano y $S\subset A$ un sistema multiplicativo. Si E es un A-módulo inyectivo, entonces E_S es un A_S-módulo inyectivo.*

Demostración. Se deduce de que todo ideal de A_S es la localización de un ideal de A y de que $\mathrm{Ext}^1_A(A/I,E)$ localiza por la proposición anterior. □

7.4. Complejo de Koszul

Sea $\mathscr{O}$ un anillo local y $a_1,\ldots,a_r$ elementos no invertibles de $\mathscr{O}$. Sea L un $\mathscr{O}$-módulo libre de base $e_1,\ldots,e_r$, y $w: L\to\mathscr{O}$ el morfismo $w(e_i)=a_i$.

1. Definición: Llamaremos complejo de Koszul respecto de $a_1,\ldots,a_r$ al complejo de $\mathscr{O}$-módulos

$$K_\cdot(a_1,\ldots,a_r,\mathscr{O}) := \bigoplus_{i=0}^{r}\Lambda^i L,$$

cuya diferencial $d\colon \Lambda^j L \to \Lambda^{j-1}L$, de grado -1, es la contracción interior con w, es decir,

$$d(e_{i_1}\wedge\cdots\wedge e_{i_p}) := \sum_{j=1}^{p}(-1)^{j-1}a_{i_j}e_{i_1}\wedge\cdots\wedge\widehat{e_{i_j}}\wedge\cdots\wedge e_{i_p}$$

Observemos que

$$H_0(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) = \mathcal{O}/(a_1\ldots,a_r).$$
$$H_r(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) = \{a\in\mathcal{O} : a\cdot a_i = 0 \text{ para todo } i\}.$$

Dado un complejo $M_\cdot$ de $\mathcal{O}$-módulos, $M_\cdot(a_1,\ldots,a_r)$ denotará el complejo de $\mathcal{O}$-módulos $M_\cdot \otimes_{\mathcal{O}} K_\cdot(a_1,\ldots,a_r,\mathcal{O})$. Obsérvese que $K_\cdot(a_1,\ldots,a_r,\mathcal{O}) = K_\cdot(a_1,\mathcal{O})\otimes_{\mathcal{O}}\cdots\otimes_{\mathcal{O}} K_\cdot(a_r,\mathcal{O})$.

2. Teorema : *Sea $M_\cdot$ un complejo de $\mathcal{O}$-módulos y $x\in\mathcal{O}$. Entonces, la sucesión de complejos:*

$$0\to M_\cdot \xrightarrow{i} M_\cdot(x) \xrightarrow{\pi} M_\cdot[-1]\to 0, \quad i(m)=m,\ \pi(m+n\mathbf{x})=n,$$

es exacta ($M_\cdot(x) = M\otimes_{\mathcal{O}} K\cdot(x,\mathcal{O}) = M\oplus M\cdot\mathbf{x}$). Por tanto, se tiene un triángulo exacto de homología

$$\begin{array}{ccc} H_\cdot(M_\cdot) & \longrightarrow & H_\cdot(M_\cdot(x)) \\ & {\scriptstyle\delta}\nwarrow \quad \swarrow & \\ & H_\cdot(M_\cdot) & \end{array}$$

donde $\delta\colon H_p(M_\cdot)\to H_p(M_\cdot)$ es multiplicar por $(-1)^p x$.

Demostración. Veamos que δ es multiplicar por $(-1)^p x$. Dado $n\in M_p$ tal que $dn=0$, tenemos

$$\begin{array}{ccccc} & & m+n\mathbf{x} & \overset{\pi}{\relbar\!\!\!\rightarrow} & n \\ & & \downarrow & & \downarrow \\ dm+(-1)^p xn & \relbar\!\!\!\rightarrow & dm+(-1)^p xn & \longmapsto & 0 \end{array}$$

luego $\delta(\bar{n}) = (-1)^p x\bar{n}$. □

3. Definición : Sean $a_1,\ldots,a_r$ elementos no invertibles de un anillo local $\mathcal{O}$. Diremos que $a_1,\ldots,a_r$ es una sucesión regular si a_i no divide al cero en $\mathcal{O}/(a_1,\ldots,a_{i-1})$, para todo i.

4. Teorema : *Sea $\mathcal{O}$ local y noetheriano y $a_1,\ldots,a_r$ elementos no invertibles de $\mathcal{O}$. Las siguientes condiciones son equivalentes:*

1. *$a_1,\ldots,a_r$ es una sucesión regular.*
2. *$H_i(K_\cdot(a_1,\ldots,a_r)) = 0$, para todo $i>0$.*
3. *$H_1(K_\cdot(a_1,\ldots,a_r)) = 0$.*

Demostración. 1. ⇒ 2. Procedemos por inducción sobre r. Si $r = 1$, entonces se cumple que $H_1(K_\cdot(a_1,\mathcal{O})) = \{a \in \mathcal{O} : a \cdot a_1 = 0\} = 0$ y concluimos. Sea $r > 1$. Por el teorema anterior, y por inducción, tenemos

$$\begin{array}{ccccc} H_p(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) & \to & H_p(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) & \to & H_{p-1}(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) \\ \| & & & & \| \\ 0 & & & & 0 \end{array}$$

para $p > 1$, luego $H_p(K_\cdot(a_1,\ldots,a_r,\mathcal{O}) = 0$ para $p > 1$. Para $p = 1$ tenemos

$$\begin{array}{cccccc} & 0 \to H_1(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) & \to & H_0(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) & \xrightarrow{\cdot a_r} & H_0(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) \\ (*) & & & \| & & \| \\ & & & \mathcal{O}/(a_1,\ldots,a_{r-1}) & & \mathcal{O}/(a_1,\ldots,a_{r-1}) \end{array}$$

luego $H_1(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) = 0$, por la regularidad de la sucesión.

2. ⇒ 3. Evidente

3. ⇒ 1. Por el teorema anterior tenemos la sucesión

$$\begin{array}{ccccc} H_1(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) & \xrightarrow{\cdot -a_r} & H_1(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) & \to & H_1(K_\cdot(a_1,\ldots,a_r,\mathcal{O})) \\ & & & & \| \\ & & & & 0 \end{array}$$

Por el lema de Nakayama, $H_1(K_\cdot(a_1,\ldots,a_{r-1},\mathcal{O})) = 0$. Por inducción sobre r, $a_1,\ldots,a_{r-1}$ es una sucesión regular. Para concluir que $a_1,\ldots,a_r$ es regular basta observar la sucesión $(*)$. □

Dado que $K_\cdot(a_1,\ldots,a_r,\mathcal{O}) = K_\cdot(a_1,\mathcal{O}) \otimes \cdots \otimes K_\cdot(a_r,\mathcal{O})$, se obtiene como corolario de este teorema que el que $a_1,\ldots,a_r$ sea una sucesión regular no depende del orden en que sean escritos $a_1,\ldots,a_r$.

5. Proposición: *Si $\{a_1,\ldots,a_r\}$ es una sucesión regular del anillo local noetheriano $\mathcal{O}$ e $I = (a_1,\ldots,a_r)$, entonces I/I^2 es un $\mathcal{O}/I$-módulo libre de rango r.*

Demostración. El complejo de Koszul asociado a $\{a_1,\ldots,a_r\}$ es acíclico en grado mayor que cero, luego tenemos la sucesión exacta

$$\Lambda^2 L \to L \to I \to 0$$

Tensando por $\otimes_{\mathcal{O}} \mathcal{O}/I$, como el morfismo $(\Lambda^2 L) \otimes_{\mathcal{O}} \mathcal{O}/I \to L \otimes_{\mathcal{O}} \mathcal{O}/I$ es nulo obtenemos que $L \otimes_{\mathcal{O}} \mathcal{O}/I \simeq I/I^2$. □

6. Observación: En las hipótesis de la proposición 7.4.5, se puede demostrar que el graduado $G_I\mathcal{O}$ es un anillo de polinomios con coeficientes en $\mathcal{O}/I$.

7. Observación: Sea $\mathcal{O}$ e un anillo local regular de ideal maximal $\mathfrak{m}_x$. Si las diferenciales de $f_1,\dots,f_r \in \mathfrak{m}_x$ en x son linealmente independientes, sabemos por 4.3.10 que $\mathcal{O}/(f_1,\dots,f_i)$ es un anillo local regular (luego íntegro), para todo i, y por tanto $\{f_1,\dots,f_r\}$ es una sucesión regular en $\mathcal{O}$. Si $I \subset \mathcal{O}$ es un ideal de modo que $\mathcal{O}/I$ es un anillo regular, sabemos, por 4.3.10, que existen $\{f_1,\dots,f_r\}$ tales que $I = (f_1,\dots,f_r)$ y $\{d_x f_i\}$ son linealmente independientes en $\mathfrak{m}_x/\mathfrak{m}_x^2$, luego $\{f_1,\dots,f_r\}$ es una sucesión regular en $\mathcal{O}$.

Decimos que un morfismo $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una inmersión cerrada, si existe un isomorfismo $B \simeq A/I$, de modo que f es igual a la composición $\operatorname{Spec} B \simeq \operatorname{Spec}(A/I) \hookrightarrow \operatorname{Spec} A$.

8. Definición: Se dice que una inmersión cerrada $Y = \operatorname{Spec} A/I \hookrightarrow X = \operatorname{Spec} A$ es regular si I está localmente generado por una sucesión regular. Se dice que es una intersección completa si está globalmente generado (en un abierto U que contenga a Y) por una sucesión regular.

9. Proposición: *Sea $Y = \operatorname{Spec} A/I \hookrightarrow X = \operatorname{Spec} A$ una inmersión cerrada. Si X e Y son regulares entonces la inmersión cerrada es regular.*

Demostración. Es consecuencia de la observación 7.4.7. □

Sabemos por 4.4.26 que las variedades lisas son regulares. Demostremos, de nuevo, que las variedades algebraicas regulares sobre un cuerpo algebraicamente cerrado son lisas.

10. Proposición: *Si $X = \operatorname{Spec} A$ es una k-variedad algebraica regular sobre un cuerpo algebraicamente cerrado, entonces es lisa.*

Demostración. $X \times X$ es regular. Luego, la diagonal $X \hookrightarrow X \times X$ es una inmersión cerrada regular. Sea $\Delta \subset A \otimes_k A$ el ideal de funciones de $X \times X$ que se anulan en la diagonal $X \hookrightarrow X \times X$. Por 7.4.5, $(\Delta/\Delta^2)_x = (\Omega_{A/k})_x$ es un A_x-módulo localmente libre de rango $\dim(A \times A)_{(x,x)} - \dim A_x = \dim A_x$, para todo punto cerrado $x \in X$. Por tanto, X es lisa. □

7.5. Teorema de Serre para los anillos regulares

En toda la sección, $\mathcal{O}$ denota un anillo local noetheriano de maximal $\mathfrak{m}$.

1. Proposición: *Sea M un $\mathcal{O}$-módulo finito generado. Entonces,*

$$\operatorname{Tor}_1(M, \mathcal{O}/\mathfrak{m}) = 0 \Leftrightarrow M \text{ es libre}.$$

Demostración. Sean L un módulo libre y $\pi: L \to M$ un morfismo de $\mathcal{O}$-módulos tal que $\bar{\pi}: L \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}$ sea un isomorfismo. Por el lema de Nakayama, π es epiyectivo. Sea $N = \operatorname{Ker}\pi$. Tensando la sucesión exacta $0 \to N \to L \to M \to 0$ por $\mathcal{O}/\mathfrak{m}$ obtenemos una sucesión exacta

$$0 \to \operatorname{Tor}_1(M, \mathcal{O}/\mathfrak{m}) \to N \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to L \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \xrightarrow{\sim} M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to 0$$

Luego $N \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = 0$, y por el lema de Nakayama $N = 0$ y $L \simeq M$. □

2. Corolario: *Sea M un $\mathcal{O}$-módulo finito generado. Si $\operatorname{Tor}_{n+1}(M, \mathcal{O}/\mathfrak{m}) = 0$, para toda resolución de M*

$$L_{n-1} \xrightarrow{d_{n-1}} L_{n-2} \xrightarrow{d_{n-2}} \cdots \xrightarrow{d_1} L_0 \xrightarrow{d_0} M \to 0$$

por libres finito generados, se cumple que $\operatorname{Ker} d_{n-1}$ es libre, y obtenemos una resolución finita por $n+1$ libres finito generados

$$0 \to \operatorname{Ker} d_{n-1} \to L_{n-1} \xrightarrow{d_{n-1}} L_{n-2} \xrightarrow{d_{n-2}} \cdots \xrightarrow{d_1} L_0 \xrightarrow{d_0} M \to 0$$

Demostración. De las sucesiones exactas

$$0 \to \operatorname{Ker} d_j \to L_j \to \operatorname{Ker} d_{j-1} \to 0$$

se deduce que $\operatorname{Tor}_i(\operatorname{Ker} d_j, \mathcal{O}/\mathfrak{m}) = \operatorname{Tor}_{i+1}(\operatorname{Ker} d_{j-1}, \mathcal{O}/\mathfrak{m})$, para $i > 0$. Por tanto,

$$\operatorname{Tor}_1(\operatorname{Ker} d_{n-1}, \mathcal{O}/\mathfrak{m}) = \operatorname{Tor}_2(\operatorname{Ker} d_{n-2}, \mathcal{O}/\mathfrak{m}) = \cdots = \operatorname{Tor}_n(\operatorname{Ker} d_0, \mathcal{O}/\mathfrak{m}) = \operatorname{Tor}_{n+1}(M, \mathcal{O}/\mathfrak{m}) = 0$$

luego se concluye por la proposición anterior. □

3. Definición: Sea M un A-módulo. Diremos que la dimensión proyectiva de M, que denotaremos $\operatorname{dimpro} M$, es $n < \infty$, si existe una resolución de M por $n+1$ libres

$$0 \to L_n \to L_{n-1} \to \cdots \to L_0 \to M \to 0$$

y no existe una de longitud más corta.

4. Proposición: *Sea M un $\mathcal{O}$-módulo finito generado. Se cumple que*

1. $\operatorname{dimpro} M = \sup\{i : \operatorname{Tor}_i(M, \mathcal{O}/\mathfrak{m}) \neq 0\}$.
2. $\operatorname{dimpro} M = \sup\{i : \operatorname{Tor}_i(M, N) \neq 0, \text{ para algún } N\}$.

Demostración. Obviamente, $\mathrm{Tor}_i(M,N)=0$, para todo $i>\mathrm{dimpro}\,M$. Por otra parte, sea $n=\sup\{i:\mathrm{Tor}_i(M,\mathscr{O}/\mathfrak{m})\neq 0\}$. Por 7.5.2, sabemos que existe una resolución por $n+1$ libres $0\to L_n\to L_{n-1}\to\cdots\to L_0\to M\to 0$, por tanto, $\mathrm{dimpro}\,M\leq n$. Entonces,

$$\sup\{i:\mathrm{Tor}_i(M,N)\neq 0,\ \text{para algún } N\}\leq \mathrm{dimpro}\,M\leq \sup\{i:\mathrm{Tor}_i(M,\mathscr{O}/\mathfrak{m})\neq 0\}.$$

Como el primer término de las desigualdades es mayor o igual que el tercer término obtenemos la igualdad de todos ellos. □

5. Definición: Llamaremos dimensión global de $\mathscr{O}$, y lo denotaremos $\mathrm{dimglo}\,\mathscr{O}$, a

$$\mathrm{dimglo}\,\mathscr{O}:=\sup\{\mathrm{dimpro}\,M,\ M \text{ finito generado}\}.$$

Como $\mathrm{dimpro}\,M=\sup\{i:\mathrm{Tor}_i(M,\mathscr{O}/\mathfrak{m})\neq 0\}\leq \mathrm{dimpro}\,\mathscr{O}/\mathfrak{m}$, entonces $\mathrm{dimglo}\,\mathscr{O}=\mathrm{dimpro}\,\mathscr{O}/\mathfrak{m}$.

6. Definición: Sea M un A-módulo. Diremos que $x\in A$ es M-regular si el morfismo $M\to M$, $m\mapsto xm$ es inyectivo.

7. Lema: *Sea A un anillo, M un A-módulo y $x\in A$ un elemento A-regular y M-regular. Para todo A/xA-módulo N se cumple que*

$$\mathrm{Tor}_n^A(M,N)=\mathrm{Tor}_n^{A/xA}(M/xM,N),$$

para todo $n\geq 0$.

Demostración. Los cuasi-isomorfismos los escribiremos $\equiv$. Cuando una sucesión de morfismos la consideremos como un complejo de módulos la escribiremos entre corchetes. Sea $L_\cdot\to M$ una resolución de M por módulos libres. Entonces,

$$M/xM[-1]\equiv[M\overset{x\cdot}{\hookrightarrow}M]\overset{7.2.17}{\equiv}[L_\cdot\overset{x\cdot}{\hookrightarrow}L_\cdot]\overset{7.2.17}{\equiv}[L_\cdot/xL_\cdot][-1].$$

Luego, $L_\cdot/xL_\cdot$ es una resolución por A/xA-módulos libres de M/xM y

$$\mathrm{Tor}_n^A(M,N)=H_n(L_\cdot\otimes_A N)=H_n(L_\cdot/xL_\cdot\otimes_{A/xA}N)=\mathrm{Tor}_n^{A/xA}(M/xM,N).$$

□

8. Teorema de Serre: *Sea $\mathscr{O}$ un anillo local noetheriano. $\mathscr{O}$ es regular si y solo si tiene dimensión global finita. Además, si $\mathscr{O}$ es regular, su dimensión global coincide con su dimensión de Krull.*

Demostración. Sea $\mathcal{O}$ regular de ideal maximal $\mathfrak{m}$, y $x_1,\dots,x_n$ un sistema mínimo de parámetros que generen $\mathfrak{m}$. El complejo de Koszul asociado, $K_\cdot$, es una resolución de $\mathcal{O}/\mathfrak{m}$ por $n+1$ libres. Además, $\mathrm{Tor}_n(\mathcal{O}/\mathfrak{m},\mathcal{O}/\mathfrak{m}) = H_n(K_\cdot \otimes \mathcal{O}/\mathfrak{m})$ y es fácil ver que éste último vale $\mathcal{O}/\mathfrak{m}$. En conclusión, $\mathrm{dimglo}\,\mathcal{O} = \mathrm{dimpro}\,\mathcal{O}/\mathfrak{m} = n = \dim \mathcal{O}$.

Veamos el recíproco. Lo vamos a demostrar por inducción sobre $\dim\mathcal{O}$.

Si $\mathrm{dimglo}\,\mathcal{O} = 0$, entonces todo $\mathcal{O}$-módulo es libre y por tanto $\mathcal{O} = \mathcal{O}/\mathfrak{m}$ y es regular. Podemos suponer que $\mathrm{dimglo}\,\mathcal{O} = n > 0$. Veamos que existe $f \in \mathfrak{m}$ no divisor de cero. En efecto, si todos los $x \in \mathfrak{m}$ fuesen divisores de cero, existiría $a \in \mathcal{O}$ no nulo tal que $a\cdot\mathfrak{m} = 0$. Sea $L_{n-2} \xrightarrow{d_{n-2}} L_{n-3}\cdots \to L_0 \to \mathcal{O}/\mathfrak{m} \to 0$ una resolución de $\mathcal{O}/\mathfrak{m}$ por módulos libres finito generados. Sean L_{n-1} un libre finito generado y $L_{n-1} \xrightarrow{d_{n-1}} \mathrm{Ker}\, d_{n-2}$ una epiyección que sea isomorfismo al tensar por $\otimes_{\mathcal{O}}\mathcal{O}/\mathfrak{m}$. Entonces la sucesión exacta de $\mathcal{O}$-módulos $0 \to \mathrm{Ker}\, d_{n-1} \to L_{n-1} \to L_{n-2} \to \cdots \to L_0 \to \mathcal{O}/\mathfrak{m} \to 0$ es una resolución por libres de $\mathcal{O}/\mathfrak{m}$ (por 7.5.2, ya que $\mathrm{Tor}_1(\mathrm{Ker}\, d_{n-1},\mathcal{O}/\mathfrak{m}) = \mathrm{Tor}_{n+1}(\mathcal{O}/\mathfrak{m},\mathcal{O}/\mathfrak{m}) = 0$) y $\mathrm{Ker}\, d_{n-1} \subset \mathfrak{m}L_{n-1}$. Pero $0 \neq a\cdot\mathrm{Ker}\, d_{n-1} \subset a\cdot\mathfrak{m}L_{n-1} = 0$ y hemos llegado a contradicción.

Existe $x \in \mathfrak{m}\backslash\mathfrak{m}^2$ no divisor de cero: Sean $\mathfrak{p}_1,\dots,\mathfrak{p}_r$, los ideales maximales entre los primos asociados a una descomposición primaria reducida del cero. Por tanto, los divisores del cero son $\bigcup_{i=1}^{r}\mathfrak{p}_i$. Buscamos $x \in \mathfrak{m}\backslash(\bigcup_{i=1}^{r}\mathfrak{p}_i \cup \mathfrak{m}^2)$. Sabemos que $\mathfrak{p}_i \subsetneq \mathfrak{m}$, para todo i, y que $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ si $i \neq j$. Por inducción sobre r, podemos suponer que existe $f_1 \in \mathfrak{m}\backslash(\bigcup_{i=2}^{r}\mathfrak{p}_i \cup \mathfrak{m}^2)$. Si $f_1 \notin \mathfrak{p}_1$, sea $x := f_1$. Si $f_1 \in \mathfrak{p}_1$, sea $f_2 \in (\bigcap_{i=2}^{r}\mathfrak{p}_i \cap \mathfrak{m}^2)\backslash\mathfrak{p}_1$, y sea $x := f_1 + f_2$.

Basta demostrar que $\mathcal{O}/x\mathcal{O}$ es regular, porque como $x \in \mathfrak{m}\backslash\mathfrak{m}^2$, entonces $\mathcal{O}$ sería regular. Por la hipótesis de inducción sobre $\dim\mathcal{O}$, basta demostrar que $\mathcal{O}/x\mathcal{O}$ tiene dimensión global finita. Tenemos que probar que $\mathcal{O}/\mathfrak{m}$ es un $\mathcal{O}/x\mathcal{O}$-módulo de dimensión proyectiva finita, que equivale a decir que $\mathfrak{m}/x\mathcal{O}$ tiene dimensión proyectiva finita, como se deduce de la sucesión exacta $0 \to \mathfrak{m}/x\mathcal{O} \to \mathcal{O}/x\mathcal{O} \to \mathcal{O}/\mathfrak{m} \to 0$. Ahora bien, $\mathfrak{m}/x\mathcal{O}$ es un sumando directo de $\mathfrak{m}/x\mathfrak{m}$: en efecto, la sucesión exacta $0 \to (\bar{x}) \xrightarrow{i} \mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/x\mathcal{O} \to 0$ rompe, pues un retracto de i es la composición de los morfismos obvios $\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2 = (\bar{x}) \oplus N \to (\bar{x})$, siendo N un subespacio complementario cualquiera de $(\bar{x})$ en $\mathfrak{m}/\mathfrak{m}^2$. Por tanto, basta ver que $\mathfrak{m}/x\mathfrak{m}$ tiene dimensión proyectiva finita y esto es consecuencia de que $\mathrm{Tor}_i^{\mathcal{O}}(\mathfrak{m},\mathcal{O}/\mathfrak{m}) = \mathrm{Tor}_i^{\mathcal{O}/x\mathcal{O}}(\mathfrak{m}/x\mathfrak{m},\mathcal{O}/\mathfrak{m})$, por el lema anterior.

□

9. Corolario: *Si $\mathcal{O}$ es regular e $y \in \mathrm{Spec}\,\mathcal{O}$, entonces $\mathcal{O}_y$ es regular.*

Demostración. Es consecuencia del teorema de Serre y de que los tores localizan por 7.3.7. □

10. Definición: Un anillo noetheriano se dice que es regular si es localmente regular.

11. Corolario: *Sea A un anillo noetheriano de dimensión de Krull finita. Entonces, A es regular si y solo si existe un $n >> 0$ de modo que $\mathrm{Tor}_n(M,N) = 0$, para todo módulo M y N.*

12. Corolario: *Una variedad algebraica es regular si por cambio del cuerpo base es regular. En particular, las variedades algebraicas lisas son regulares.*

Demostración. Es consecuencia del teorema de Serre y de que los tores son estables por cambios de base planos. □

13. Definición: Diremos que un ideal primo $\mathfrak{p}_x \subset A$ es de altura r, si $\dim A_x = r$.

14. Lema: *Un anillo íntegro y noetheriano es DFU si y solo si los ideales primos de altura 1 son principales.*

Demostración. Sea A DFU y $\mathfrak{p} \subset A$ un ideal de altura 1. Sea $a \in \mathfrak{p}$ un elemento irreducible. El ideal (a) es primo, luego $\mathfrak{p} = (a)$.

Veamos el recíproco. Por noetherianidad, todo $a \in A$ se escribe como producto de elementos irreducibles. Para la unicidad, basta probar que los elementos irreducibles son primos. Sea a un elemento irreducible y $\mathfrak{p}_x$ un ideal primo mínimo conteniéndolo. Entonces $\mathfrak{p}_x$ es de altura 1, pues $\dim A_x/aA_x = 0$, luego $\dim A_x = 1$. Por tanto, $\mathfrak{p}_x = (b)$, luego $a = b \cdot c$ y por ser a irreducible, c ha de ser invertible. Por consiguiente $\mathfrak{p}_x = (a)$. □

15. Teorema: *Si $\mathcal{O}$ es un anillo local y regular, entonces es DFU.*

Demostración. Procedemos por inducción sobre la dimensión de Krull de $\mathcal{O}$. Si $\dim \mathcal{O} = 0$ entonces $\mathcal{O} = \mathcal{O}/\mathfrak{m}$ que es DFU. Podemos suponer que $\dim \mathcal{O} > 0$.

Sea $f \in \mathfrak{m} \setminus \mathfrak{m}^2$. Se cumple que (f) es un ideal primo, pues $\mathcal{O}/f\mathcal{O}$ es regular.

1) Probemos que $\mathcal{O}_f$ es DFU. Por el lema 7.5.14, tenemos que probar que los ideales primos de altura 1 de $\mathcal{O}_f$ son principales. Sea $\mathfrak{p} \subset \mathcal{O}$ un ideal primo de altura 1 tal que $f \notin \mathfrak{p}$. Como $\mathcal{O}_f$ es un anillo localmente regular de dimensión menor que $\mathcal{O}$, por inducción $\mathfrak{p}\mathcal{O}_f$ es localmente principal. Sea $0 \to L_m \to L_{m-1} \to \cdots \to L_0 \to \mathfrak{p} \to 0$ una resolución por libres de $\mathfrak{p}$. Localizando por f, obtenemos una resolución por libres de $\mathfrak{p}\mathcal{O}_f$, $0 \to L_{m,f} \to L_{m-1,f} \to \cdots \to L_{0,f} \to \mathfrak{p}\mathcal{O}_f \to 0$. Si probamos que todo A-módulo M localmente libre de rango n que se resuelva por libres cumple que $\Lambda^n M \simeq A$, concluiremos que $\mathfrak{p}\mathcal{O}_f$ es principal. Sea pues $0 \to L_m \to \cdots \to L_0 \to M \to 0$ una resolución libre de un módulo localmente libre M. Como M es proyectivo, $L_0 = M \oplus N$, donde N es

localmente libre y $0 \to L_n \to \cdots \to L_1 \to N \to 0$ es una resolución por libres de N. Por inducción sobre la longitud de la cadena, $\Lambda^{\mathrm{rg}N} N \simeq A$. Como

$$A = \Lambda^{\mathrm{rg}L_0} L_0 = \Lambda^{\mathrm{rg}M} M \otimes \Lambda^{\mathrm{rg}N} N,$$

se concluye que $\Lambda^{\mathrm{rg}M} M \simeq A$.

2) Ahora ya, probemos que $\mathscr{O}$ es DFU. En efecto, sea $\mathfrak{p}$ un ideal primo de altura 1 de $\mathscr{O}$. Si $f \in \mathfrak{p}$, entonces $\mathfrak{p} = (f)$. Si $f \notin \mathfrak{p}$, entonces $\mathfrak{p}\mathscr{O}_f$ es principal (pues $\mathscr{O}_f$ es DFU). Escribamos $\mathfrak{p}\mathscr{O}_f = a \cdot \mathscr{O}_f$, con $a \in \mathscr{O}$. Por noetherianidad podemos escoger a de modo que no sea divisible por f en $\mathscr{O}$. Si $b \in \mathfrak{p}$, entonces para cierto $n \in \mathbb{N}$ y $s \in \mathscr{O}$, $b \cdot f^n = a \cdot s$. Ahora bien, como a no es divisible por f, que es primo, se tendrá que $\frac{s}{f^n} \in \mathscr{O}$ y $b = a \cdot \frac{s}{f^n}$. En conclusión, $\mathfrak{p} = (a)$ es principal, luego $\mathscr{O}$ es DFU por 7.5.14.

□

7.6. Anillos de Cohen-Macaulay y Gorenstein

Supondremos en toda la sección que los anillos son anillos noetherianos.

1. Definición: Sea M un A-módulo. Diremos que $a_1, \ldots, a_n \in A$ es una sucesión M-regular si a_{i+1} no es divisor de cero en $M/(a_1, \ldots, a_i)M$.

2. Lema: *Si un ideal de un anillo está incluido en la unión de un número finito de ideales primos, entonces el ideal está incluido en alguno de los ideales primos.*

Demostración. Ver 0.5.37. □

3. Proposición: *Sea A un anillo noetheriano, $I \subset A$ un ideal y M un A-módulo finito generado. Entonces,* $\mathrm{Hom}_A(A/I, M) = 0$ *si y solo si existe algún elemento M-regular en I.*

Demostración. $\mathrm{Hom}_A(A/I, M) = \{m \in M : I \cdot m = 0\}$. Si existe un elemento M-regular en I, entonces $\mathrm{Hom}_A(A/I, M) = 0$. Recíprocamente, supongamos $\mathrm{Hom}_A(A/I, M) = 0$. Si todos los elementos de I son divisores de cero en M, entonces $I \subseteq \bigcup_j \mathfrak{p}_j$, donde $\mathfrak{p}_j$ son los ideales primos asociados a la descomposición primaria del cero en M. Por tanto, $I \subseteq \mathfrak{p}_j$ para algún j. Sea $0 \neq m \in M$ tal que $\mathfrak{p}_j \cdot m = 0$. Entonces $I \cdot m = 0$ y $\mathrm{Hom}_A(A/I, M) \neq 0$. Hemos llegado a contradicción por suponer que no existen elementos M-regulares en I. □

4. Teorema: *En las hipótesis de la proposición anterior, la condición necesaria y suficiente para que exista una sucesión M-regular $a_1,\dots,a_r \in I$ es que* $\operatorname{Ext}^i_A(A/I,M) = 0$, *para* $0 \le i < r$.

Demostración. Supongamos que $\operatorname{Ext}^i_A(A/I,M) = 0$, para todo $0 \le i < r$. Para $i = 0$ tenemos que $\operatorname{Hom}_A(A/I,M) = 0$, y por la proposición anterior existe $a_1 \in I$ no divisor de cero en M. De la sucesión exacta

$$0 \to M \xrightarrow{a_1\cdot} M \to M/a_1M \to 0$$

se sigue

$$0 = \operatorname{Ext}^i_A(A/I,M) \to \operatorname{Ext}^i_A(A/I,M/a_1M) \to \operatorname{Ext}^{i+1}_A(A/I,M) = 0$$

para todo $i+1 < r$. Por lo tanto $\operatorname{Ext}^i_A(A/I,M/a_1M) = 0$ para $0 \le i < r-1$. Por inducción, existe una sucesión $a_2,\dots,a_r \in I$ que es (M/a_1M)-regular, luego $a_1,\dots,a_r$ es M-regular.

Recíprocamente, sea $a_1,\dots,a_r \in I$ una sucesión M-regular. De la sucesión exacta

$$0 \to M \xrightarrow{a_1\cdot} M \to M/a_1M \to 0$$

y por inducción sobre r, se obtienen sucesiones exactas

$$0 = \operatorname{Ext}^j_A(A/I,M/a_1M) \to \operatorname{Ext}^{j+1}_A(A/I,M) \xrightarrow{a_1\cdot} \operatorname{Ext}^{j+1}_A(A/I,M)$$

para $-1 \le j < r-1$. Por tanto, la aplicación $\operatorname{Ext}^{j+1}_A(A/I,M) \xrightarrow{a_1\cdot} \operatorname{Ext}^{j+1}_A(A/I,M)$ es inyectiva para $0 \le j+1 < r$. Ahora bien, $\operatorname{Ext}^{j+1}_A(A/I,M)$ está anulado por I (como se observa al calcular los extens resolviendo M por inyectivos) y $a_1 \in I$, luego $\operatorname{Ext}^j_A(A/I,M) = 0$ para $0 \le j < r$. □

5. Definición: Se llama profundidad de un módulo M al supremo de las longitudes de las sucesiones $a_1,\dots,a_n$ M-regulares tales que $M/(a_1,\dots,a_n)M \neq 0$.

6. Observación: Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y M un $\mathcal{O}$-módulo finito generado. Entonces, $\operatorname{prof} M = n$ si y solo si $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},M) = 0$ para $0 \le i < n$ y $\operatorname{Ext}^n_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},M) \neq 0$. En la demostración del teorema anterior hemos visto que toda sucesión regular de un módulo M de profundidad n se puede ampliar a una sucesión regular maximal de longitud n. Por lo tanto toda sucesión regular maximal tiene la misma longitud.

7. Definición: Sea $\mathcal{O}$ un anillo local noetheriano y M un $\mathcal{O}$-módulo finito generado. Llamaremos dimensión de M, que denotaremos $\dim M$, a la dimensión de su soporte.

8. Teorema de Ischebeck: *Sea $\mathcal{O}$ un anillo noetheriano local de ideal maximal $\mathfrak{m}$, M y N $\mathcal{O}$-módulos finito generados distintos de cero. Supongamos que* $\operatorname{prof} M = n$ *y* $\dim N = r$. *Entonces,*

$$\operatorname{Ext}^i_{\mathcal{O}}(N, M) = 0 \text{ para } i < n - r.$$

Demostración. Sea $N = N_0 \supset N_1 \supset \cdots \supset N_n = (0)$ una cadena con $N_j/N_{j+1} \simeq \mathcal{O}/\mathfrak{p}_j$, y $\mathfrak{p}_j$ primo. Es fácil ver que si $\operatorname{Ext}^i_{\mathcal{O}}(N_j/N_{j+1}, M) = 0$ para todo j, entonces $\operatorname{Ext}^i_{\mathcal{O}}(N, M) = 0$.

Procedamos por inducción sobre $\dim N$. Si $\dim N = 0$, como $\dim N_j/N_{j+1} \leq \dim N = 0$, entonces $N_j/N_{j+1} = \mathcal{O}/\mathfrak{m}$ y concluimos porque $\operatorname{prof} M = n$ si y solo si $\operatorname{Ext}^i(\mathcal{O}/\mathfrak{m}, M) = 0$, para $i < n$.

Supongamos $\dim N = r > 0$. Tenemos que probar que $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) = 0$ para $i < n - r$, cuando $\dim \mathcal{O}/\mathfrak{p} = r$. Sea $a \in \mathfrak{m} \setminus \mathfrak{p}$ y consideremos la sucesión exacta

$$0 \to \mathcal{O}/\mathfrak{p} \xrightarrow{a\cdot} \mathcal{O}/\mathfrak{p} \to \mathcal{O}/(\mathfrak{p}, a) \to 0$$

Como $\dim \mathcal{O}/(\mathfrak{p}, a) < \dim \mathcal{O}/\mathfrak{p} = r$, por inducción $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}, a), M) = 0$ para $i < n - r + 1$. Así pues, para $i < n - r$ tenemos las sucesiones exactas

$$\underset{\|}{\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}, a), M)_0} \to \operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) \xrightarrow{a\cdot} \operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) \to \underset{\|}{\operatorname{Ext}^{i+1}_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}, a), M)_0}$$

Como $a \in \mathfrak{m}$, $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) = 0$, por el lema de Nakayama. □

9. Definición: Se dice que un anillo local noetheriano $\mathcal{O}$ es de Cohen-Macaulay si su profundidad es igual a su dimensión.

Obsérvese que la profundidad es siempre menor o igual que la dimensión. Por tanto, $\mathcal{O}$ es de Cohen-Macaulay si y solo si $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = 0$, para $0 \leq i < \dim \mathcal{O}$.

10. Ejemplo: Los anillos locales regulares son de Cohen-Macaulay.

11. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$.*

1. *Si $\mathcal{O}$ es de Cohen-Macaulay, entonces no tiene componentes sumergidas; y si $\mathfrak{p}$ es un ideal primo minimal entonces* $\dim \mathcal{O} = \dim \mathcal{O}/\mathfrak{p}$.

2. *Sea $a_1, \ldots, a_r \in \mathfrak{m}$ es una sucesión regular. Entonces, $\mathcal{O}$ es un anillo de Cohen-Macaulay si y solo si $\mathcal{O}/(a_1, \ldots, a_r)$ es de Cohen-Macaulay.*

3. *Sea $x \in \operatorname{Spec} \mathcal{O}$. Si $\mathcal{O}$ es de Cohen-Macaulay, entonces $\mathcal{O}_x$ es de Cohen-Macaulay.*

4. *Si $\mathcal{O}$ es de Cohen-Macaulay, entonces es catenario.*

Demostración. 1. Si $\mathfrak{p}$ es divisor de cero, entonces $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \neq 0$. Por el teorema anterior, $0 \geq \mathrm{prof}\mathcal{O} - \dim\mathcal{O}/\mathfrak{p} = \dim\mathcal{O} - \dim\mathcal{O}/\mathfrak{p}$ y concluimos.

2. En primer lugar, observemos que $\dim\mathcal{O}/(a_1,\ldots,a_r) = \dim\mathcal{O} - r$. Si $\mathcal{O}$ es de Cohen-Macaulay, entonces $a_1,\ldots,a_r$ se puede ampliar a una sucesión regular maximal $a_1,\ldots,a_n$ ($n = \dim\mathcal{O}$), luego $a_{r+1},\ldots,a_n$ es una sucesión regular de $\mathcal{O}/(a_1,\ldots,a_r)$ de longitud $\dim\mathcal{O}/(a_1,\ldots,a_r)$, luego el anillo $\mathcal{O}/(a_1,\ldots,a_r)$ es de Cohen-Macaulay. Para el recíproco se argumenta equivalentemente.

3. Si $\mathfrak{p}_x$ es divisor de cero, entonces es minimal, por 1., luego $\mathcal{O}_x$ tiene dimensión cero y es de Cohen-Macaulay. Si $\mathfrak{p}_x$ no es divisor de cero, sea $a_1 \in \mathfrak{p}_x$ no divisor de cero. Por 2., $\mathcal{O}/(a_1)$ es de Cohen-Macaulay, luego, por inducción sobre la dimensión de $\mathcal{O}$, $(\mathcal{O}/(a_1))_x$ es de Cohen-Macaulay. Por 2., $\mathcal{O}_x$ es de Cohen-Macaulay.

4. Procedemos por inducción sobre $\dim\mathcal{O}$. Sea $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_m = \mathfrak{m}$ una cadena maximal de ideales primos. Por 1., existe $a \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$ que no es divisor de cero. Entonces $\bar{\mathfrak{p}}_1 \subset \cdots \subset \bar{\mathfrak{p}}_m = \bar{\mathfrak{m}}$ es una cadena maximal de $\mathcal{O}/(a_1)$, que es de Cohen-Macaulay, luego catenario por inducción. Por tanto, $m - 1 = \dim\mathcal{O}/(a_1)$, luego $\dim\mathcal{O} = m$.

□

12. Observación: Si $\mathcal{O}$ es Cohen-Macaulay, entonces $a \in \mathcal{O}$ no es divisor de cero si y solo si $(a)_0 \subset \mathrm{Spec}\mathcal{O}$ no es un divisor topológico, es decir, no existe un cerrado propio $C \subset \mathrm{Spec}A$ tal que $(a)_0 \cup C = \mathrm{Spec}\mathcal{O}$.

13. Corolario: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull n, de ideal maximal $\mathfrak{m}_x$. $\mathcal{O}$ es Cohen-Macaulay si y solo si todo sistema de parámetros $\{f_1,\ldots,f_n\}$ ($(f_1,\ldots,f_n)_0 = \{x\}$) es una sucesión regular.*

Demostración. Como $\mathcal{O}/(f_1,\ldots,f_n)$ es de dimensión cero es de Cohen-Macaulay. Por tanto, si $\{f_1,\ldots,f_n\}$ es una sucesión regular $\mathcal{O}$ es de Cohen-Macaulay.

Supongamos ahora que $\mathcal{O}$ es Cohen-Macaulay. Como $\dim\mathcal{O} = n$ y $\dim\mathcal{O}/(f_1,\ldots,f_n) = 0$, entonces $\dim\mathcal{O}/(f_1,\ldots,f_i) = \dim\mathcal{O} - i$. Por tanto, f_1 no es divisor de cero y $\mathcal{O}/(f_1)$ es Cohen-Macaulay. Luego, f_2 no es divisor de cero en $\mathcal{O}/(f_1)$ y $\mathcal{O}/(f_1,f_2)$ es Cohen-Macaulay, etc. □

14. Definición: Se dice que A es un anillo de Cohen-Macaulay (o que $\mathrm{Spec}A$ es Cohen-Macaulay) si A es noetheriano y A_x es Cohen-Macaulay para todo $x \in \mathrm{Spec}A$.

15. Ejemplos: Las curvas planas $p(x,y) = 0$ son variedades de Cohen-Macaulay. Las subvariedades de $\mathbb{A}^n$ que son localmente intersección completa son variedades de Cohen-Macaulay.

16. Proposición: *Sea $f: A \to B$ un morfismo finito fielmente plano. Entonces, A es Cohen-Macaulay si y solo si B es de Cohen-Macaulay.*

Demostración. Observemos que A es noetheriano si y solo si B es noetheriano. Sea $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido por f. Las fibras de f^* son de dimensión cero y los ideales primos que están en la fibra de un ideal primo de A tienen la misma altura que éste (por 3.3.42).

Sea $x \in \operatorname{Spec} A$ y $f^{*-1}(x) = \{y_1, \ldots, y_r\}$. Los extens son estables por cambio de base plano, luego

$$\operatorname{Ext}^i_{A_x}((A/\mathfrak{p}_x)_x, A_x) \underset{A_x}{\otimes} B_x = \operatorname{Ext}^i_{B_x}((B/\mathfrak{p}_x B)_x, B_x) = \prod_j \operatorname{Ext}^i_{B_{y_j}}((B/\mathfrak{p}_x B)_{y_j}, B_{y_j})$$

Ahora, por el teorema de Ischebeck, es fácil concluir que A_x es de Cohen-Macaulay si y solo si los B_{y_j} son de Cohen-Macaulay. □

17. Teorema: *Sea A un anillo regular y B un anillo de Cohen-Macaulay. Todo morfismo $A \to B$ finito e inyectivo es plano (supongamos que todos los puntos cerrados de* $\operatorname{Spec} B$ *tienen la misma altura).*

Demostración. Podemos suponer que A es un anillo local de dimensión de Krull n, de ideal maximal $\mathfrak{m}$. Sea $t_1, \ldots, t_n$ un sistema mínimo de parámetros que generen $\mathfrak{m}$. Por ser $A \to B$ finito, $\dim B/(t_1, \ldots, t_n) = 0$, y por tanto $t_1, \ldots, t_n$ es una sucesión regular en B, por ser B Cohen-Macaulay. Entonces,

$$\operatorname{Tor}^A_1(A/\mathfrak{m}, B) = H_1(K_\cdot(t_1, \ldots, t_n, A) \otimes_A B) = H_1(K_\cdot(t_1, \ldots, t_n, B)) = 0$$

luego B es un A-módulo libre. □

18. Observación: Sea $X = \operatorname{Spec} A$ una k-variedad algebraica afín conexa. Por el teorema de Noether, existe una proyección finita $X \to \mathbb{A}^n_k$. El teorema anterior y 7.6.16 nos dice que X es Cohen-Macaulay si y solo si dicha proyección es un revestimiento. En conclusión, las variedades afines de Cohen-Macaulay son los revestimientos del espacio afín.

Nuestro objetivo ahora es el estudio de los anillos de Gorenstein, más adelante definidos. Su conocimiento será necesario en la teoría de dualidad y de hecho creemos que los anillos de Gorenstein son mejor comprendidos dentro de la teoría de la dualidad local.

19. Definición: Se dice que un anillo es artiniano si es un anillo noetheriano de dimensión cero.

Los anillos artinianos son de longitud finita, luego toda cadena descendente de ideales estabiliza. Esta propiedad los caracteriza (véase el libro de Atiyah y Macdonald [2]).

20. Proposición: *Sea $\mathcal{O}$ un anillos local noetheriano de ideal maximal $\mathfrak{m}$. $\mathcal{O}$ es un módulo inyectivo $\Leftrightarrow$ $\mathcal{O}$ es un anillo artiniano y* $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \mathcal{O}/\mathfrak{m}$.

Demostración. Sea N un $\mathcal{O}$-módulo finito generado. Denotemos $N^* = \mathrm{Hom}_{\mathcal{O}}(N,\mathcal{O})$ y $k = \mathcal{O}/\mathfrak{m}$. Veamos el recíproco:

1) $l(N^*) \leq l(N)$: Procedemos por inducción sobre la longitud del módulo N. Sea $0 \to k \to N \to N/k = N' \to 0$ una sucesión exacta. Tomando duales se obtiene la sucesión exacta $k^* \leftarrow N^* \leftarrow N'^* \leftarrow 0$, luego $l(N^*) \leq l(N'^*) + 1 \underset{\text{Ind.}}{\leq} l(N') + 1 = l(N)$.

2) Consideremos la sucesión exacta $0 \to \mathfrak{m} \to \mathcal{O} \to \mathcal{O}/\mathfrak{m} \to 0$. Tenemos que $l(\mathfrak{m}^*) \leq l(\mathfrak{m}) = l(\mathcal{O}) - 1$. Tomando duales y por la hipótesis tenemos

$$0 \to k \to \mathcal{O} \to \mathfrak{m}^* \to \mathrm{Ext}^1_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) \to 0$$

luego, $l(\mathrm{Ext}^1_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O})) = l(\mathfrak{m}^*) - l(\mathcal{O}) + 1 \leq 0$, y $\mathrm{Ext}^1_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = 0$. Por la proposición 7.3.8, $\mathcal{O}$ es inyectivo.

Probemos el directo. Dado un ideal primo $\mathfrak{p} \underset{\neq}{\subset} \mathfrak{m}$, sea $x \in \mathfrak{m}\backslash\mathfrak{p}$ y consideremos el morfismo $\mathcal{O}/\mathfrak{p} \xhookrightarrow{x\cdot} \mathcal{O}/\mathfrak{p}$. Entonces el morfismo $(\mathcal{O}/\mathfrak{p})^* \xrightarrow{x\cdot} (\mathcal{O}/\mathfrak{p})^*$ es epiyectivo y por el lema de Nakayama, $(\mathcal{O}/\mathfrak{p})^* = 0$, luego $(\mathcal{O}/\mathfrak{p})^{**} = 0$. $(\mathcal{O}/\mathfrak{m})^{**}$ es un $\mathcal{O}/\mathfrak{m}$-módulo, luego contiene una cadena de $\mathcal{O}$-módulos de factores isomorfos a $\mathcal{O}/\mathfrak{m}$. Existe una cadena de $\mathcal{O}$-módulos $0 = N_0 \subset \cdots \subset N_r = \mathcal{O}$, de factores $N_i/N_{i-1} \simeq \mathcal{O}/\mathfrak{p}_i$, entonces $\mathcal{O} = \mathcal{O}^{**}$ contiene una cadena de factores isomorfos a $\mathcal{O}/\mathfrak{m}$, luego existe n tal que $\mathfrak{m}^n \cdot \mathcal{O} = 0$ y $\dim \mathcal{O} = 0$. Sea $l((\mathcal{O}/\mathfrak{m})^*) = n$. Por inducción sobre la longitud, se prueba que $l(N^*) = n \cdot l(N)$. Como $l(\mathcal{O}^*) = l(\mathcal{O})$, habrá de ser $n = 1$. Por tanto $(\mathcal{O}/\mathfrak{m})^* \simeq \mathcal{O}/\mathfrak{m}$. □

21. Definición: Llamaremos dimensión inyectiva de M, y lo denotaremos $\mathrm{diminy}\, M$, a la longitud mínima de las resoluciones por inyectivos

$$0 \to M \to I_0 \to \cdots \to I_n \to 0$$

Si no existe ninguna resolución finita por inyectivos, decimos que la dimensión inyectiva es infinita.

22. Corolario: *Se cumple que* $\mathrm{diminy}\, M \leq n \Leftrightarrow \mathrm{Ext}^{n+1}_A(A/I, M) = 0$ *para todo ideal I. En caso noetheriano, basta tomar como ideales los ideales primos.*

Demostración. El directo es obvio. Veamos el recíproco. Sea

$$0 \to M \to I_0 \to I_1 \to \cdots \to I_{n-1} \to C \to 0$$

una sucesión exacta, con I_i inyectivos. Es fácil ver que $\operatorname{Ext}_A^1(A/I, C) = \operatorname{Ext}_A^{n+1}(A/I, M) = 0$. Por la proposición 7.3.8 concluimos que C es un A-módulo inyectivo y $\operatorname{diminy} M \leq n$. □

23. Lema : *Sea A un anillo, M un A-módulo y $x \in A$ un elemento A-regular y M-regular. Para todo A/xA-módulo N se cumple que*

$$\operatorname{Ext}_A^{n+1}(N, M) = \operatorname{Ext}_{A/xA}^n(N, M/xM).$$

Demostración. Sea I un A-módulo inyectivo. Como sabemos si tomamos $\operatorname{Hom}_A(-, I)$ en la inyección $A \xhookrightarrow{x\cdot} A$, obtenemos el epimorfismo $I \xrightarrow{x\cdot} I$. Además, el núcleo K de este último morfismo es un A/xA-módulo y $\operatorname{Hom}_{A/xA}(N, K) = \operatorname{Hom}_A(N, I)$ para todo A/xA-módulo N, luego K es un A/xA-módulo inyectivo.

Sea $M \to I^\cdot$ una resolución de M por módulos inyectivos y $K^\cdot$ el núcleo del morfismo $I^\cdot \xrightarrow{x\cdot} I^\cdot$. Entonces,

$$M/xM[-1] \equiv [M \xhookrightarrow{x\cdot} M] \overset{7.2.17}{\equiv} [I^\cdot \xrightarrow{x\cdot} I^\cdot] \overset{7.2.17}{\equiv} K^\cdot.$$

Sea $L_\cdot \to N$ una resolución de N por A/xA-módulos libres. Entonces,

$$\operatorname{Ext}_A^i(N, M) = H^i(\operatorname{Hom}_A(N, I^\cdot)) = H^i(\operatorname{Hom}_{A/xA}(N, K^\cdot)) \overset{7.2.17}{=} H^i(\operatorname{Hom}_{A/xA}(L_\cdot, K^\cdot))$$
$$\overset{7.2.17}{=} H^i(\operatorname{Hom}_{A/xA}(L_\cdot, M/xM[-1])) = \operatorname{Ext}_{A/xA}^{i-1}(N, M/xM).$$

□

24. Teorema : *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión n e ideal maximal $\mathfrak{m}$. Las siguientes condiciones son equivalentes:*

1. $\operatorname{diminy} \mathcal{O} < \infty$.
2. $\operatorname{diminy} \mathcal{O} = \dim \mathcal{O}$.
3. *$\mathcal{O}$ es de Cohen-Macaulay y* $\operatorname{Ext}_{\mathcal{O}}^n(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = \mathcal{O}/\mathfrak{m}$.
4. $\operatorname{Ext}_{\mathcal{O}}^r(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = 0$, *para un $r > \dim \mathcal{O}$ cualquiera.*

Demostración. 1. $\Rightarrow$ 3. Sea $\operatorname{diminy}\mathcal{O} = s$, es decir, $\operatorname{Ext}^{s+1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) = 0$ para todo ideal primo $\mathfrak{p}$ y $s+1$ es el mínimo número natural con esta propiedad.

Si $s = 0$, entonces $\mathcal{O}$ es un $\mathcal{O}$-módulo inyectivo. Luego, $\mathcal{O}$ es de Cohen-Macaulay porque $\dim\mathcal{O} = 0$, por 7.6.20 y $\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \mathcal{O}/\mathfrak{m}$, por 7.6.20.

Supongamos ahora que $s > 0$. Dado un ideal primo $\mathfrak{p}$ distinto de $\mathfrak{m}$, sea $x \in \mathfrak{m}\backslash\mathfrak{p}$; de la sucesión exacta $0 \to \mathcal{O}/\mathfrak{p} \xrightarrow{x\cdot} \mathcal{O}/\mathfrak{p}$ obtenemos $\operatorname{Ext}^s_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^s_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \to 0$, luego por Nakayama $\operatorname{Ext}^s_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) = 0$.

Si $\mathfrak{m}$ es divisor de cero, existe un morfismo $k = \mathcal{O}/\mathfrak{m} \hookrightarrow \mathcal{O}$, que induce un morfismo $0 = \operatorname{Ext}^s_{\mathcal{O}}(\mathcal{O},\mathcal{O}) \to \operatorname{Ext}^s_{\mathcal{O}}(k,\mathcal{O}) \to 0$, luego $\operatorname{Ext}^s_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = 0$ y llegamos a contradicción con $\operatorname{diminy}\mathcal{O} = s$. Así pues, $\mathfrak{m}$ no es divisor de cero. Sea $x \in \mathfrak{m}$ un elemento $\mathcal{O}$-regular. Por el lema anterior, $\operatorname{Ext}^i_{\mathcal{O}/x\mathcal{O}}(N,\mathcal{O}/x\mathcal{O}) = \operatorname{Ext}^{i+1}_{\mathcal{O}}(N,\mathcal{O})$, para todo $\mathcal{O}/x\mathcal{O}$-módulo N, luego $\mathcal{O}/x\mathcal{O}$ tiene dimensión inyectiva menor que s. Por inducción sobre s, obtenemos que $\mathcal{O}/x\mathcal{O}$ es Cohen-Macaulay y que $\mathcal{O}/\mathfrak{m} = \operatorname{Ext}^{\dim\mathcal{O}/x\mathcal{O}}_{\mathcal{O}/x\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}/x\mathcal{O})$. Luego $\mathcal{O}$ es Cohen-Macaulay y de nuevo por el lema $\mathcal{O}/\mathfrak{m} = \operatorname{Ext}^{\dim\mathcal{O}}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O})$.

3. $\Rightarrow$ 2. Si $\dim\mathcal{O} = 0$, entonces $\operatorname{diminy}\mathcal{O} = 0$ por la proposición 7.6.20. Sea $\dim\mathcal{O} = n > 0$. Sea $x \in \mathfrak{m}$ un elemento $\mathcal{O}$-regular. Probemos que $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\quad,\mathcal{O}) = 0$ para todo $i > 0$. Por el lema,

$$\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \operatorname{Ext}^{n+i-1}_{\mathcal{O}/x\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}/x\mathcal{O}) \overset{\text{Ind.}}{=} 0.$$

Sea $\mathfrak{p}$ un ideal primo de altura máxima tal que $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \neq 0$, para algún $i > 0$. Sea $x \in \mathfrak{m}\backslash\mathfrak{p}$. De la sucesión exacta $0 \to \mathcal{O}/\mathfrak{p} \xrightarrow{x\cdot} \mathcal{O}/\mathfrak{p} \to \mathcal{O}/(\mathfrak{p},x) \to 0$ obtenemos la sucesión exacta $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \to \operatorname{Ext}^{n+i+1}_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p},x),\mathcal{O}) = 0$ (donde éste último es cero ya que existe una resolución $0 \subset N_0 \subset \cdots \subset N_r = \mathcal{O}/(\mathfrak{p},x)$ con $N_i/N_{i-1} \simeq \mathcal{O}/\mathfrak{p}_i$ y $\mathfrak{p}_i$ de altura mayor que la de $\mathfrak{p}$). Por el lema de Nakayama concluimos que $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) = 0$, llegando a contradicción. Luego $\dim\mathcal{O} = \operatorname{diminy}\mathcal{O}$

2. $\Rightarrow$ 1. Es inmediato.

Hemos probado la equivalencia de 1.,2. y 3.

1. $\Leftrightarrow$ 4. El directo es obvio. Para el recíproco sabemos que $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = 0$, luego $\operatorname{Ext}^r_{\mathcal{O}}(M,\mathcal{O}) = 0$ para todo $\mathcal{O}$-módulo M finito generado concentrado en $\mathfrak{m}$. Si $\dim\mathcal{O} = 0$ hemos terminado. Sea $\mathfrak{p}_y$ un ideal primo, maximal cumpliendo $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) \neq 0$. Sea $x \in \mathfrak{m}\backslash\mathfrak{p}_y$ y consideremos la sucesión exacta $0 \to \mathcal{O}/\mathfrak{p}_y \xrightarrow{x\cdot} \mathcal{O}/\mathfrak{p}_y \to \mathcal{O}/(\mathfrak{p}_y,x) \to 0$. $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}_y,x),\mathcal{O}) = 0$ porque existe una cadena de submódulos de $\mathcal{O}/(\mathfrak{p}_y,x)$ de factores $\mathcal{O}/\mathfrak{p}_z$, con $\mathfrak{p}_y \underset{\neq}{\subset} \mathfrak{p}_z$ y $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_z,\mathcal{O}) = 0$. De la sucesión exacta larga de $\mathcal{O}$-módulos inducida $\operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) \to 0$, deducimos que $\operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) = 0$, por el lema de Nakayama. Luego, $\operatorname{Ext}^{r-1}_{\mathcal{O}_y}((\mathcal{O}/\mathfrak{p}_y)_y,\mathcal{O}_y) = 0$, y por inducción sobre la dimensión del anillo obtenemos que $\operatorname{diminy}\mathcal{O}_y = \dim\mathcal{O}_y < r-1$. Observemos que para todo ideal primo $\mathfrak{p}_y \underset{\neq}{\subset} \mathfrak{p}_z \underset{\neq}{\subset} \mathfrak{m}$, se cumple que $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_z,\mathcal{O}) = 0$, luego $\operatorname{Ext}^r_{\mathcal{O}_z}(\mathcal{O}_z/\mathfrak{p}_z\mathcal{O}_z,\mathcal{O}_z) = 0$ y por hipótesis de inducción $\operatorname{diminy}\mathcal{O}_z = \dim\mathcal{O}_z < r-1$. Por tanto, $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O})$ es

un $\mathcal{O}$-módulo concentrado en $\mathfrak{m}$, luego de longitud finita. Tenemos la sucesión exacta $0 \to \mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y, \mathcal{O}) \xrightarrow{x\cdot} \mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y, \mathcal{O})$. Por toma de longitudes, se deduce que $x\cdot$ ha de ser un isomorfismo y por el lema de Nakayama $\mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y, \mathcal{O}) = 0$ y llegamos a contradicción. En conclusión, $\mathrm{Ext}^r_{\mathcal{O}}(-, \mathcal{O}) = 0$ y $\mathrm{diminy}\,\mathcal{O} < r$. □

25. Definición: Diremos que un anillo $\mathcal{O}$ local noetheriano es de Gorenstein si verifica cualquiera de las condiciones equivalentes del teorema anterior.

Diremos que un anillo noetheriano A es de Gorenstein (o que $\mathrm{Spec}\,A$ es de Gorenstein) si A_x es de Gorenstein para todo $x \in \mathrm{Spec}\,A$.

26. Ejemplo: Los anillos locales regulares son de Gorenstein, porque son de dimensión global finita por el teorema de Serre y la condicón 4. del teorema anterior.

27. Proposición: *Sea $\mathcal{O}$ un anillo local noetheriano y $x \in \mathcal{O}$ un elemento regular. Se verifica que $\mathcal{O}$ es de Gorenstein si y solo si $\mathcal{O}/x\mathcal{O}$ es de Gorenstein.*

Demostración. Es consecuencia de la igualdad $\mathrm{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = \mathrm{Ext}^{i-1}_{\mathcal{O}/x\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}/x\mathcal{O})$. □

28. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$ y $x \in \mathrm{Spec}\mathcal{O}$. Se verifica:*

a) Si $\mathcal{O}$ es de Gorenstein, entonces $\mathcal{O}_x$ es de Gorenstein.

b) $\mathcal{O}$ es de Gorenstein si y solo si $\widehat{\mathcal{O}}$ es de Gorenstein.

Demostración. *a*) Si $\mathcal{O}$ es Gorenstein entonces tiene una resolución por $\mathcal{O}$-módulos inyectivos finita. Localizando en x obtenemos una resolución de $\mathcal{O}_x$ por $\mathcal{O}_x$-módulos inyectiva finita, luego $\mathcal{O}_x$ es de Gorestein.

b) $\mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O})$ está anulado por $\mathfrak{m}$, luego $\mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = \mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) \underset{\mathcal{O}}{\otimes} \widehat{\mathcal{O}}$. Además, como $\mathcal{O} \to \widehat{\mathcal{O}}$ es plano, $\mathrm{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) \underset{\mathcal{O}}{\otimes} \widehat{\mathcal{O}} = \mathrm{Ext}^r_{\widehat{\mathcal{O}}}(\widehat{\mathcal{O}}/\mathfrak{m}\widehat{\mathcal{O}}, \widehat{\mathcal{O}})$. Se concluye. □

29. Teorema: *Sea $\mathcal{O}$ un anillo local de Gorenstein de dimensión n y $\bar{\mathcal{O}} = \mathcal{O}/I$.*

1. *$\bar{\mathcal{O}}$ es Cohen-Macaulay de dimensión d $\iff$ $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = 0$ para $i \neq n - d$.*
2. *$\bar{\mathcal{O}}$ es Gorenstein de dimensión d $\iff$ $\mathrm{Ext}^{n-d}_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) \simeq \bar{\mathcal{O}}$ y $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = 0$, para $i \neq n - d$.*

Demostración. Procedemos por inducción sobre $n = \dim \mathcal{O}$.

a) Si $\dim \mathcal{O} = 0$, entonces $\mathcal{O}$ es inyectivo. Por tanto, $\bar{\mathcal{O}}$ es de Cohen-Macaulay; y $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = 0$, para todo $i > 0$. Probemos 2.: Si $\mathrm{Hom}_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = \bar{\mathcal{O}}$, entonces

$$\mathrm{Hom}_{\bar{\mathcal{O}}}(\mathcal{O}/\mathfrak{m}, \bar{\mathcal{O}}) = \mathrm{Hom}_{\bar{\mathcal{O}}}(\mathcal{O}/\mathfrak{m}, \mathrm{Hom}_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O})) = \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = \mathcal{O}/\mathfrak{m}$$

luego, por 7.6.20, $\bar{\mathcal{O}}$ es inyectivo y por tanto Gorenstein. Recíprocamente, supongamos que $\bar{\mathcal{O}}$ es Gorenstein. Dado un $\bar{\mathcal{O}}$-módulo finito generado N, denotemos $N^* = \mathrm{Hom}_{\mathcal{O}}(N, \mathcal{O})$. $(\mathcal{O}/\mathfrak{m})^* = \mathcal{O}/\mathfrak{m}$, por ser $\mathcal{O}$ Gorenstein de dimensión 0. Es fácil demostrar, por inducción sobre la longitud de N, que N^* tiene la misma longitud que N y que $N = N^{**}$. Además, $\mathrm{Hom}_{\mathcal{O}}(N, N') = \mathrm{Hom}_{\mathcal{O}}(N'^*, N^*)$. Por tanto, $\mathrm{Hom}_{\mathcal{O}}(\bar{\mathcal{O}}^*, \mathcal{O}/\mathfrak{m}) = \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \bar{\mathcal{O}}) = \mathcal{O}/\mathfrak{m}$, luego $\bar{\mathcal{O}}^*$ es monógeno y por longitudes $\bar{\mathcal{O}}^* \simeq \bar{\mathcal{O}}$.

b) Supongamos ahora $\dim \mathcal{O} > 0$.

Si $\dim \bar{\mathcal{O}} < \dim \mathcal{O}$, existe un $t \in I$, no divisor de cero en $\mathcal{O}$. Por 7.6.23, $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = \mathrm{Ext}^{i-1}_{\mathcal{O}/t\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}/t\mathcal{O})$ y por inducción concluimos el teorema.

Supongamos $\dim \bar{\mathcal{O}} = \dim \mathcal{O} = n > 0$.

b.1) Si todo elemento no invertible de $\bar{\mathcal{O}}$ es divisor de cero, entonces existe un elemento $t \in \bar{\mathcal{O}}$ anulado por $\mathfrak{m}$, luego un morfismo inyectivo $\mathcal{O}/\mathfrak{m} \hookrightarrow \bar{\mathcal{O}}$. Ahora bien, tomando $\mathrm{Ext}^n_{\mathcal{O}}(-, \mathcal{O})$ tendremos que $\mathrm{Ext}^n_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) \neq 0$. Además, $\bar{\mathcal{O}}$ no es Cohen-Macaulay ni Gorenstein. En conclusión, no se cumple ninguna de las condiciones del teorema.

b.2) Supongamos que existe $t \in \bar{\mathcal{O}}$ no invertible y no divisor de cero. Si $\bar{\mathcal{O}}$ es Cohen-Macaulay de dimensión d, de la sucesión exacta

$$0 \to \bar{\mathcal{O}} \xrightarrow{t\cdot} \bar{\mathcal{O}} \to \bar{\mathcal{O}}/t\bar{\mathcal{O}} \to 0$$

y aplicando las hipótesis de inducción resulta $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) = 0$ para $i \neq n - d$, junto con la sucesión exacta

$$0 \to \mathrm{Ext}^{n-d}_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) \xrightarrow{t\cdot} \mathrm{Ext}^{n-d}_{\mathcal{O}}(\bar{\mathcal{O}}, \mathcal{O}) \to \mathrm{Ext}^{n-d+1}_{\mathcal{O}}(\bar{\mathcal{O}}/t\bar{\mathcal{O}}, \mathcal{O}) \to 0$$

que muestra, si $\bar{\mathcal{O}}$ es Gorenstein, que $\mathrm{Ext}^{n-d}(\bar{\mathcal{O}}, \mathcal{O}) = \bar{\mathcal{O}}$. Considérese la misma sucesión exacta para los recíprocos.

□

7.7. Criterios de platitud

7.7.1. Criterio local de platitud y consecuencias

1. Definición: Sea M un A-módulo e $I \subseteq A$ un ideal. Diremos que M es I-idealmente separado si para todo ideal $\mathfrak{a} \subseteq A$, finito generado, $\mathfrak{a} \otimes_A M$ es separado con la topología I-ádica.

Por ejemplo, si B es una A-álgebra noetheriana e $I \cdot B$ está contenido en todo maximal de B, entonces todo B-módulo finito generado es I-idealmente separado.

2. Criterio local de platitud: *Sea A un anillo noetheriano, $I \subseteq A$ un ideal y M un A-módulo I-idealmente separado. Las siguientes condiciones son equivalentes*

1. *M es un A-módulo plano.*
2. *M/I^nM es un A/I^n-módulo plano, para todo $n \geq 0$.*
3. *M/IM es un A/I-módulo plano y $(\bigoplus_{n=0}^{\infty} I^n/I^{n+1}) \underset{A}{\otimes} M \simeq \bigoplus_{n=0}^{\infty} (I^nM/I^{n+1}M)$.*
4. *M/IM es un A/I-módulo plano y $\operatorname{Tor}_1^A(A/I, M) = 0$.*

Demostración. 1. $\Rightarrow$ 2. es obvio. 2. $\Rightarrow$ 1. Tenemos que probar que para todo ideal finito generado $\mathfrak{a} \subset A$ el morfismo $\mathfrak{a} \underset{A}{\otimes} M \to M$, $a \otimes m \mapsto am$ es inyectivo. Basta probar que en el diagrama conmutativo

$$\begin{array}{ccc} \mathfrak{a} \otimes M & \longrightarrow & M \\ \downarrow & & \downarrow \\ \widehat{\mathfrak{a} \otimes M} & \longrightarrow & \widehat{M} \end{array}$$

el morfismo $\widehat{\mathfrak{a} \otimes M} \to \widehat{M}$ es inyectivo. Por el lema de Artin-Rees, la topología I-ádica en $\mathfrak{a}$ coincide con la topología definida por la filtración $\{I^k \cap \mathfrak{a}\}$. Por lo tanto, la topología definida en $\mathfrak{a} \otimes M$ por $\{I^k(\mathfrak{a} \otimes M)\}$, coincide con la topología definida por $\{(I^k \cap \mathfrak{a}) \otimes M\}$. En conclusión $\widehat{\mathfrak{a} \otimes M} = \varprojlim (\bar{\mathfrak{a}}_k \otimes_A M) = \varprojlim (\bar{\mathfrak{a}}_k \otimes_{A/I^k} M/I^kM)$, donde $\bar{\mathfrak{a}}_k = \mathfrak{a}/(I^k \cap \mathfrak{a}) \subset A/I^k$. Como el límite proyectivo de inyecciones es una inyección, el morfismo $\widehat{\mathfrak{a} \otimes M} \to \widehat{M}$ es inyectivo.

2. $\Rightarrow$ 3. $I^n/I^{n+1} \otimes_A M = I^n/I^{n+1} \otimes_{A/I^{n+1}} M/I^{n+1}M = I^n/I^{n+1} \cdot M/I^{n+1}M = I^nM/I^{n+1}M$.

3. $\Rightarrow$ 4. Consideremos el diagrama

$$\begin{array}{ccccccc} & & I^{k+1}/I^n \underset{A}{\otimes} M & \longrightarrow & I^k/I^n \underset{A}{\otimes} M & \longrightarrow & I^k/I^{k+1} \underset{A}{\otimes} M \longrightarrow 0 \\ & & \phi_{k+1} \downarrow & & \phi_k \downarrow & & \wr \downarrow \\ 0 & \longrightarrow & I^{k+1}M/I^nM & \longrightarrow & I^kM/I^nM & \longrightarrow & I^kM/I^{k+1}M \longrightarrow 0 \end{array}$$

Por inducción descendente podemos suponer que ϕ_{k+1} es isomorfismo (ϕ_n lo es), luego ϕ_k es isomorfismo. Por tanto, $I/I^n \otimes_A M \overset{\phi_1}{=} IM/I^nM$. Del diagrama

$$\begin{array}{ccc} I \otimes M & \longrightarrow & M \\ \downarrow & & \downarrow \\ \widehat{I \otimes M} & \hookrightarrow & \widehat{M} \end{array}$$

(donde la flecha inferior es inyectiva porque es límite proyectivo de las inyecciones $(I \otimes_A M)/(I^n \otimes_A M) = I/I^n \otimes_A M \overset{\phi_1}{=} IM/I^nM \hookrightarrow M/I^nM$) tenemos que $I \otimes_A M = I \cdot M$, luego $\mathrm{Tor}_1^A(A/I, M) = 0$.

4. $\Rightarrow$ 2. Si $\mathrm{Tor}_1^A(A/I, M) = 0$, entonces $\mathrm{Tor}_1^A(N, M) = 0$ para todo A/I-módulo N. En efecto, sea una sucesión exacta de A/I-módulos $0 \to K \to L \to N \to 0$ donde L es un A/I-módulo libre. Tensando por $\underset{A}{\otimes} M$ obtenemos

$$\begin{array}{ccccccccc} \mathrm{Tor}_1^A(L,M) & \longrightarrow & \mathrm{Tor}_1^A(N,M) & \longrightarrow & K \otimes_A M & \longrightarrow & L \otimes_A M & \longrightarrow & N \otimes_A M \longrightarrow 0 \\ \| & & & & \| & & \| & & \| \\ 0 & \longrightarrow & \mathrm{Tor}_1^{A/I}(N, M/IM) & \to & K \otimes_{A/I} M/IM & \to & L \otimes_{A/I} M/IM & \to & N \otimes_{A/I} M/IM \to 0 \end{array}$$

Como M/IM es un A/I-módulo plano, concluimos que $\mathrm{Tor}_1^A(N, M) = 0$. Ahora, si N es un A/I^k-módulo, demostremos que $\mathrm{Tor}_1^A(N, M) = 0$: Observemos que $I \cdot N$ y N/IN son A/I^{k-1}-módulos. De la sucesión exacta $0 \to IN \to N \to N/IN \to 0$ obtenemos, por inducción sobre k, que $\mathrm{Tor}_1^A(N, M) = 0$.

Por tanto, dada una sucesión exacta $0 \to N_1 \to N_2 \to N_3 \to 0$ de A/I^k-módulos, la fila superior del diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 \otimes_A M & \longrightarrow & N_2 \otimes_A M & \longrightarrow & N_3 \otimes_A M & \longrightarrow & 0 \\ & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\ & & N_1 \otimes_{A/I^k} M/I^kM & \to & N_2 \otimes_{A/I^k} M/I^kM & \to & N_3 \otimes_{A/I^k} M/I^kM & & \end{array}$$

es exacta, luego M/I^kM es un A/I^k-módulo plano. □

3. Corolario : *Sean A y B dos k-álgebras de tipo finito y $f : A \to B$ un morfismos de k-álgebras. Entonces, f es un morfismo plano si y solo si para todo ideal maximal $\mathfrak{m} \subset A$, $G_{\mathfrak{m}}A \otimes_A B = G_{\mathfrak{m}}B$. Geométricamente, un morfismo de variedades algebraicas $f^* : Y = \mathrm{Spec}B \to \mathrm{Spec}A = X$ es plano si y solo si*

$$C_xX \times_x f^{*-1}(x) = C_{X/f^{*-1}(x)}$$

para todo punto cerrado $x = \mathrm{Spec}A/\mathfrak{m}_x$ de X.

Demostración. El corolario es local en B, podemos suponer que B es local de ideal maximal y y A local de ideal maximal $f^*(y) = x$. Ahora ya el corolario es consecuencia directa de los puntos 1. y 3. del criterio local de platitud. □

4. Definición: Sean $\mathcal{O}$ y $\mathcal{O}'$ dos anillos locales de ideales maximales $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente. Un morfismo de anillos $f:\mathcal{O}\to\mathcal{O}'$ se dice que es dominante si $f^{-1}(\mathfrak{m}')=\mathfrak{m}$, es decir, $f(\mathfrak{m})\subseteq\mathfrak{m}'$.

5. Corolario: *Sea $\mathcal{O}\to\mathcal{O}'$ un morfismo dominante entre anillos locales noetherianos y M un $\mathcal{O}'$-módulo finito generado. Sean $\mathfrak{m}$ y $\mathfrak{m}'$ los ideales maximales de $\mathcal{O}$ y $\mathcal{O}'$, respectivamente. Denotemos por $\widetilde{\mathcal{O}}$ y $\widetilde{M}$ las compleciones $\mathfrak{m}$-ádicas de $\mathcal{O}$ y M, y por $\widehat{\mathcal{O}'}$ y $\widehat{M}$ las compleciones $\mathfrak{m}'$-ádicas de $\mathcal{O}'$ y M. Se verifica:*

1. *M es plano sobre $\mathcal{O}\Leftrightarrow\widehat{M}$ es plano sobre $\mathcal{O}\Leftrightarrow\widehat{M}$ es plano sobre $\widetilde{\mathcal{O}}$.*
2. *M es plano sobre $\mathcal{O}\Leftrightarrow\widetilde{M}$ es plano sobre $\mathcal{O}\Leftrightarrow\widetilde{M}$ es plano sobre $\widetilde{\mathcal{O}}$.*

Demostración. 1. La primera equivalencia se debe a que $\mathcal{O}'\to\widehat{\mathcal{O}'}$ es fielmente plano y $\widehat{M}=M\otimes_{\mathcal{O}'}\widehat{\mathcal{O}'}$. La segunda a que $\mathcal{O}\to\widetilde{\mathcal{O}}$ es fielmente plano y a que $-\otimes_{\mathcal{O}}\widehat{M}=-\otimes_{\mathcal{O}}\widetilde{\mathcal{O}}\otimes_{\widetilde{\mathcal{O}}}\widehat{M}$.
2. Es consecuencia del apartado 2. del criterio local de platitud. □

6. Teorema: *Sea $(\mathcal{O},\mathfrak{m})$ un anillo local regular, $(\mathcal{O}',\mathfrak{m}')$ un anillo local Cohen-Macaulay y $\varphi:\mathcal{O}\to\mathcal{O}'$ un morfismo dominante. Entonces, $\dim\mathcal{O}'=\dim\mathcal{O}+\dim(\mathcal{O}'/\mathfrak{m}\cdot\mathcal{O}')$ si y solo si $\mathcal{O}'$ es plano sobre $\mathcal{O}$.*

Demostración. Procedemos por inducción sobre $\dim\mathcal{O}$. Si $\dim\mathcal{O}=0$, entonces $\mathcal{O}$ es cuerpo y acabamos. Si $\dim\mathcal{O}>0$, sea $a\in\mathfrak{m}\setminus\mathfrak{m}^2$ y sean $\bar{\mathcal{O}}=\mathcal{O}/a\mathcal{O}$, $\bar{\mathcal{O}}'=\mathcal{O}'/a\mathcal{O}'$.

$\Rightarrow$) Como sabemos

$$\dim\bar{\mathcal{O}}'\overset{*}{\leq}\dim\bar{\mathcal{O}}+\dim(\bar{\mathcal{O}}'/\mathfrak{m}\bar{\mathcal{O}}')=\dim\mathcal{O}-1+\dim(\mathcal{O}'/\mathfrak{m}\mathcal{O}')=\dim\mathcal{O}'-1.$$

Por tanto, $\dim\bar{\mathcal{O}}'=\dim\mathcal{O}'-1$.

$*$[Sea $f_1,\dots,f_r$ un sistema mínimo de parámetros de $\bar{\mathcal{O}}'/\mathfrak{m}\bar{\mathcal{O}}'$ y $f_{r+1},\dots,f_n$ un sistema de parámetros mínimo de $\bar{\mathcal{O}}$. Entonces $f_1,\dots,f_n$ es un sistema de parámetros de $\bar{\mathcal{O}}'$]

Por lo tanto a es $\mathcal{O}'$-regular y $\bar{\mathcal{O}}'$ es Cohen-Macaulay. Por hipótesis de inducción $\bar{\mathcal{O}}'$ es un $\bar{\mathcal{O}}$-módulo plano. Así pues $\operatorname{Tor}_1^{\bar{\mathcal{O}}}(\mathcal{O}/\mathfrak{m},\bar{\mathcal{O}}')=0$. Como a es $\mathcal{O}$-regular y $\mathcal{O}'$-regular sabemos, por el lema 7.5.7, que $\operatorname{Tor}_1^{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}')=\operatorname{Tor}_1^{\bar{\mathcal{O}}}(\mathcal{O}/\mathfrak{m},\bar{\mathcal{O}}')=0$. Por el criterio local de platitud $\mathcal{O}'$ es plano sobre $\mathcal{O}$.

$\Leftarrow$) Si $\mathcal{O}'$ es plano sobre $\mathcal{O}$, a es $\mathcal{O}'$-regular, puesto que es $\mathcal{O}$-regular. Por inducción tenemos

$$\begin{aligned}\dim\mathcal{O}'&=\dim\bar{\mathcal{O}}'+1=\dim\bar{\mathcal{O}}+1+\dim(\bar{\mathcal{O}}'/\mathfrak{m}\cdot\bar{\mathcal{O}}')\\&=\dim\mathcal{O}+\dim(\mathcal{O}'/\mathfrak{m}\cdot\mathcal{O}').\end{aligned}$$

□

7. Corolario: *Sea k un cuerpo, X una k-variedad algebraica afín regular irreducible e Y una k-variedad algebraica afín Cohen-Macaulay irreducible. Sea $f: Y \to X$ un morfismo de k-variedades. Para todo punto cerrado $x \in X$ se verifica que* $\dim f^{-1}(x) = \dim Y - \dim X$ *si y solo si f es plano.*

8. Proposición: *Sean B y C dos A-álgebras noetherianas planas. Entonces, un morfismo $f \in \mathrm{Hom}_{\mathrm{Spec}\,A}(\mathrm{Spec}\,C, \mathrm{Spec}\,B)$ es plano si es plano en fibras sobre* $\mathrm{Spec}\,A$.

Demostración. Podemos suponer A, B, C locales y que los morfismos $A \to B$, $B \to C$ son dominantes. Sea I el ideal maximal de A. Por hipótesis, C/IC es una B/IB-álgebra plana. Además,

$$(I^n B/I^{n+1}B) \underset{B}{\otimes} C = \left(I^n/I^{n+1} \underset{A}{\otimes} B\right) \underset{B}{\otimes} C = I^n/I^{n+1} \underset{A}{\otimes} C = I^n C/I^{n+1}C,$$

donde la primera igualdad y la última se deben al criterio local de platitud 7.7.2; por este mismo criterio concluimos que C es una B-álgebra plana, es decir, que f es plano. □

9. Proposición: *Sea $\mathcal{O} \to \mathcal{O}'$ un morfismo dominante entre anillos locales noetherianos. Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Sean M y P dos $\mathcal{O}'$-módulos finito generados y supongamos que P es un $\mathcal{O}$-módulo plano. Un morfismo de $\mathcal{O}'$-módulos $i: M \to P$ es inyectivo de conúcleo un $\mathcal{O}$ módulo plano (luego M es un $\mathcal{O}$ módulo plano)* $\iff$ *$M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to P \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}$ es inyectivo.*

Demostración. $\Rightarrow$) Se deduce de la sucesión exacta

$$0 = \mathrm{Tor}_{\mathcal{O}}^1(\mathcal{O}/\mathfrak{m}, P/M) \to M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to P \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}$$

$\Leftarrow$) Si consideramos el diagrama conmutativo

$$\begin{array}{ccc} G_{\mathfrak{m}}M & \longrightarrow & G_{\mathfrak{m}}P \\ {\scriptstyle\text{epi}}\uparrow & & \| \\ G_{\mathfrak{m}}\mathcal{O} \otimes_{\mathcal{O}/\mathfrak{m}} M/\mathfrak{m}M & \xrightarrow{\text{iny}} & G_{\mathfrak{m}}\mathcal{O} \otimes_{\mathcal{O}/\mathfrak{m}} P/\mathfrak{m}P \end{array}$$

concluimos que el morfismo $G_{\mathfrak{m}}M \to G_{\mathfrak{m}}P$ es inyectivo. Entonces el morfismo inducido en los completados $\mathfrak{m}$-ádicos, $\hat{M} \to \hat{P}$ es inyectivo y como M y P son $\mathfrak{m}$-ádicamente separados (pues son $\mathcal{O}'$-módulos finito generados) el morfismo $M \to P$ es inyectivo. Por ser $M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \to P \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}$ inyectivo y P un $\mathcal{O}$-módulo plano, entonces $\mathrm{Tor}_1^{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, P/M) = 0$. Por el criterio local de platitud P/M es un $\mathcal{O}$-módulo plano.

□

10. Corolario: *Sea $\mathcal{O} \to \mathcal{O}'$ un morfismo dominante entre anillos locales noetherianos, y sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Sea M un $\mathcal{O}'$-módulo finito generado y $b \in \mathcal{O}'$ un elemento no invertible. Las siguientes condiciones son equivalentes:*

1. *M es un $\mathcal{O}$-módulo plano y $\bar{b}$ no es divisor de cero en $M/\mathfrak{m}M$.*
2. *M/bM es un $\mathcal{O}$-módulo plano y b no es divisor de cero en M.*

Demostración. 1. $\Rightarrow$ 2. Considérese el morfismo $M \xrightarrow{b\cdot} M, m \mapsto b \cdot m$, en la proposición anterior.

2. $\Rightarrow$ 1. Tensando la sucesión exacta $0 \to M \xrightarrow{b\cdot} M \to M/bM \to 0$ por $\otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}^n$, obtenemos la sucesión exacta

$$0 \to M/\mathfrak{m}^n M \xrightarrow{b\cdot} M/\mathfrak{m}^n M \to M/(\mathfrak{m}^n M + bM) \to 0$$

luego b no es divisor de cero en $M/\mathfrak{m}^n M$, para todo n. Por el lema de la serpiente la sucesión $0 \to \mathfrak{m}^{n-1}M/\mathfrak{m}^n M \xrightarrow{b\cdot} \mathfrak{m}^{n-1}M/\mathfrak{m}^n M \to \mathfrak{m}^{n-1}\bar{M}/\mathfrak{m}^n \bar{M} \to 0$, donde $\bar{M} = M/bM$. Si consideramos el diagrama de filas exactas

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G_{\mathfrak{m}}M & \xrightarrow{b\cdot} & G_{\mathfrak{m}}M & \longrightarrow & G_{\mathfrak{m}}(M/bM) & \longrightarrow & 0 \\
 & & \pi\uparrow & & \pi\uparrow & & \| & & \\
0 & \longrightarrow & (G_{\mathfrak{m}}\mathcal{O}) \otimes_{\mathcal{O}/\mathfrak{m}} M/\mathfrak{m}M & \xrightarrow{b\cdot} & (G_{\mathfrak{m}}\mathcal{O}) \otimes_{\mathcal{O}/\mathfrak{m}} M/\mathfrak{m}M & \longrightarrow & (G_{\mathfrak{m}}\mathcal{O}) \otimes_{\mathcal{O}/\mathfrak{m}} M/(\mathfrak{m}M + bM) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \operatorname{Ker}\pi & \xrightarrow{b\cdot} & \operatorname{Ker}\pi & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

obtenemos, por el lema de Nakayama (grado a grado), que $\operatorname{Ker}\pi = 0$. Por tanto, M es un $\mathcal{O}$-módulo plano.

□

7.7.2. Platitud genérica

11. Lema: *Sea A un anillo íntegro noetheriano y M un A-módulo finito generado. Entonces existe $0 \neq a \in A$ tal que M_a es un A_a-módulo libre.*

Demostración. $M_{A\setminus 0}$ es un $A_{A\setminus 0}$-espacio vectorial. Digamos que $\frac{m_1}{s_1}, \ldots, \frac{m_n}{s_n}$ es una base. El morfismo $\phi\colon A^n \to M, 1_i \mapsto m_i$, es un isomorfismo en el punto genérico de A, luego es isomorfismo en un entorno del punto genérico y concluimos. □

12. Lema: *Sea A un anillo íntegro noetheriano y B una A-álgebra de tipo finito. Sea M un B-módulo finito generado. Entonces existe $0 \neq a \in A$ tal que M_a es un A_a-módulo libre.*

Demostración. Escribamos $B = A[\xi_1, \dots \xi_m]$. Procedemos por inducción sobre m. Si $m = 0$, concluimos por el lema anterior.

Si $m > 0$, escribamos $B' = A[\xi_2, \dots, \xi_m]$, luego $B = B'[\xi_1]$. Sea $m_1, \dots, m_r$ un sistema generador del B-módulo M. Sea $M_0 = \langle m_1, \dots, m_r \rangle'$ el B'-submódulo de M, generado por $m_1, \dots, m_r$. Entonces $M = \sum_{i=0}^{\infty} \xi_1^i M_0$

Sea $M_n = \sum_{i=0}^{n} \xi_1^i M_0 \subseteq M$. Obviamente, $M_{n-1} \subseteq M_n$ y $N_n := M_n / M_{n-1}$ es un B'-módulo finito generado, para todo n. Veamos que todos los B'-módulos N_n son isomorfos para todo $n >> 0$: Consideremos los epimorfismos $M_0 \xrightarrow{\xi_1^n \cdot} N_n$. Se tiene que la cadena de B'-submódulos de M_0,

$$\operatorname{Ker} \xi_1 \cdot \subseteq \operatorname{Ker} \xi_1^2 \cdot \subseteq \cdots \subseteq \operatorname{Ker} \xi_1^n \cdot \subseteq \cdots$$

que por noetherianidad estabiliza a partir de un cierto n. Con lo que se concluye, $N_r = M_0 / \operatorname{Ker} \xi_1^r = M_0 / \operatorname{Ker} \xi_1^n = N_n$, para todo $r \geq n$.

Por inducción sobre el número de parámetros m, existe un $a \in A$ tal que todos los B'-módulos $(N_i)_a$ son A_a-módulos libres. Por lo tanto, M_a es un A_a-módulo libre porque localizando en a tenemos que

$$M_0 = N_0, M_1 = M_0 \oplus M_1/M_0 = N_0 \oplus N_1, \dots, M_n = \oplus_{i=0}^{n} N_i \text{ y } M = \cup_{i=0}^{\infty} M_i = \oplus_{i=0}^{\infty} N_i.$$

□

13. Criterio topológico de Nagata: *Sea A un anillo noetheriano. Un subconjunto U de* $\operatorname{Spec} A$ *es abierto si y solo si verifica: Si $\bar{x} \cap U \neq \emptyset$, entonces $\bar{x} \cap U$ es un entorno de x en $\bar{x}$ (denotamos con la barra el cierre topológico).*

Demostración. La necesidad es obvia. Veamos la suficiencia. Sean $C_1, \dots, C_r$ las componentes irreducibles de $\overline{\operatorname{Spec} A \setminus U}$ y sean $x_1, \dots, x_r$ los puntos genéricos de $C_1, \dots, C_r$. Si $\bar{x}_i \cap U \neq \emptyset$, entonces, existe un entorno abierto W de x_i en $\bar{x}_i = C_i$ tal que $x_i \in W \subset U$; por lo tanto $C_1 \cup \cdots \cup C_r = \overline{\operatorname{Spec} A \setminus U} = C_1 \cup \cdots \cup (C_i \setminus W) \cup \cdots \cup C_r$, lo que contradice la definición de los C_i. Así pues, $\bar{x}_i \cap U = \emptyset$ para todo i. Por lo tanto, $C_1 \cup \cdots \cup C_r = \operatorname{Spec} A \setminus U$ y U es abierto. □

14. Teorema de platitud genérica: *Sea A un anillo noetheriano, B una A-álgebra de tipo finito y M un B-módulo finito generado. El conjunto*

$$U := \{x \in \operatorname{Spec} B : M_x \textit{ es un } A\textit{-módulo plano}\}$$

es un abierto de $\operatorname{Spec} B$.

Demostración. Tenemos que ver que U verifica el criterio topológico de Nagata 7.7.13. Evidentemente si $\bar{x} \cap U \neq \emptyset$ entonces $x \in U$. Sea $\mathfrak{p}_x$ el ideal definido por x y escribamos $\mathfrak{p} = A \cap \mathfrak{p}_x$, $\bar{A} = A/\mathfrak{p}$.

Dado $y \in \bar{x}$, entonces $y \in \bar{x} \cap U$, es decir, M_y es un A-módulo plano si y solo si $\mathrm{Tor}_1^A(M_y, \bar{A}) = 0$ y $(M/\mathfrak{p}M)_y$ es $\bar{A}$- plano. Ahora bien, $\mathrm{Tor}_1^A(M, \bar{A})_x = \mathrm{Tor}_1^A(M_x, \bar{A}) = 0$, por lo que es cero en un entorno V de x. Además, por el teorema anterior, existe $a \in A \setminus \mathfrak{p}$ tal que $(M/\mathfrak{p}M)_a$ es un $\bar{A}_a$-módulo libre. Por tanto, $x \in V \cap (aB)_0^c \cap \bar{x} \subset U$ y hemos terminado. □

15. Definición: Diremos que un subconjunto irreducible Z de un espacio topológico es casi-cerrado si existe una abierto W tal que $\emptyset \neq W \cap \bar{Z} \subset Z$.

16. Definición: Si B es una A-álgebra de tipo finito diremos que el morfismo inducido $\mathrm{Spec}B \to \mathrm{Spec}A$ es de tipo finito.

17. Lema: *Los morfismos de tipo finito* $\mathrm{Spec}B \to \mathrm{Spec}A$ *transforman casi-cerrados en casi-cerrados.*

Demostración. Por ser B de tipo finito sobre A, podemos factorizar $\mathrm{Spec}B \to \mathrm{Spec}A$ como la composición de una inmersión cerrada $\mathrm{Spec}B \hookrightarrow \mathbb{A}^n \times \mathrm{Spec}A$ y la proyección π natural $\mathbb{A}^n \times \mathrm{Spec}A \xrightarrow{\pi} \mathrm{Spec}A$. Como el lema es obvio para las inmersiones cerradas, basta probarlo para π. Ahora bien, podemos escribir π como composición de proyecciones desde rectas afines, así pues basta comprobar el lema para la proyección $\mathbb{A}^1 \times \mathrm{Spec}A \to \mathrm{Spec}A$, que denotaremos por f. Para probar que la imagen de un casi-cerrado Z es un casi-cerrado, podemos suponer que $\overline{f(Z)} = \mathrm{Spec}A$, sin más que considerar la proyección $\mathbb{A}^1 \times \overline{f(Z)} \to \overline{f(Z)}$. Tomando reducidos podemos suponer que A es íntegro.

En conclusión, podemos suponer que $\bar{Z} = \mathrm{Spec}B$, $B = A[x]/\mathfrak{p}$ con A y B íntegros y $\overline{f(Z)} = \mathrm{Spec}A$. Sea $U_b \subset \mathrm{Spec}B$ un abierto básico incluido en Z, con $b = \sum a_i x^i$. Basta ver que $f(U_b)$ contiene un abierto. Si $\mathfrak{p} = 0$, entonces

$$\begin{aligned} f(U_b) &= \{z \in \mathrm{Spec}A : z \in f(U_b)\} = \{z \in \mathrm{Spec}A : f^{-1}(z) \cap U_b \neq \emptyset\} \\ &= \{z \in \mathrm{Spec}A : 0 \neq \bar{b} \in k(z)[x]\} = \{z \in \mathrm{Spec}A : 0 \neq \bar{a}_i \in k(z), \forall i\} = \bigcup_i U_{a_i}. \end{aligned}$$

Si $\mathfrak{p} \neq 0$, sea $a'_m x^m + \cdots + a'_0$ un elemento no nulo de $\mathfrak{p}$. Localizando A y B por a'_m podemos suponer que a'_m es invertible y el morfismo $A \to B$ es finito. Por tanto, b verifica un polinomio con coeficientes en A, $x^n + \cdots + a$, con $a \neq 0$, luego b es invertible si a lo es; es decir, $f^{-1}(U_a) \subseteq U_b$ y tendremos que $U_a \subseteq f(U_b)$.

□

18. Inducción noetheriana: *Si para demostrar cierto teorema hacemos uso de un cierto espacio topológico noetheriano $X \neq \emptyset$, y probamos que el teorema se cumple si y solo si se cumple para un cerrado $X_1 \subsetneq X$ y podemos repetir este argumento con X_1 y sucesivamente, tendremos por la noetherianidad de X, que $X_n = \emptyset$, para $n >> 0$, y solo hay que probar el teorema en este caso (que suele ser trivial). Este modo de proceder se denomina demostración por inducción noetheriana sobre X.*

19. Teorema: *Si A es un anillo noetheriano y B una A-álgebra de tipo finito plana, entonces el morfismo natural $f\colon \mathrm{Spec}B \to \mathrm{Spec}A$ es abierto.*

Demostración. Dado que todo abierto básico de $\mathrm{Spec}B$ vuelve a ser de tipo finito y plano sobre A, basta probar que $f(\mathrm{Spec}B)$ es un abierto. Más aún, basta probar que $f(\mathrm{Spec}B)$ contiene un abierto U, porque por inducción noetheriana $f(f^{-1}(U^c))$ será un abierto de $U^c := (\mathrm{Spec}A)\backslash U$ y por tanto $f(\mathrm{Spec}B)$ también. Tomando las componentes irreducibles de $\mathrm{Spec}A$ y sus antimágenes por f, podemos reducirnos al caso en que $\mathrm{Spec}A$ es irreducible. Es más, podemos suponer que A es íntegra. Por el lema anterior $f(\mathrm{Spec}B)$ es unión de un número finito de casi-cerrados, luego basta ver que es denso en $\mathrm{Spec}A$. Basta ver que $f(\mathrm{Spec}B)$ contiene el punto genérico de $\mathrm{Spec}A$. Dado $x \in \mathrm{Spec}B$ e $y = f(x) \in \mathrm{Spec}A$, el morfismo $A_y \to B_x$ es fielmente plano, luego el morfismo inducido en los espectros es epiyectivo, luego el punto genérico de A está en la imagen de f.

□

7.8. Morfismos lisos y formalmente lisos

Cuando decimos que una variedad $\mathrm{Spec}A$ es una k-variedad algebraica subrayamos el morfismo implícito $\mathrm{Spec}A \to \mathrm{Spec}k$. El desarrollo de la Geometría Algebraica exige ampliar el estudio de las variedades $\mathrm{Spec}A$ al estudio de los morfismos de tipo finito $\mathrm{Spec}A \to \mathrm{Spec}R$, con R-anillo. Esto permitirá hablar de parametrizaciones de variedades con base de parámetros $\mathrm{Spec}R$. Tendrán particular importancia las parametrizaciones planas, es decir los morfismos $R \to A$ planos. Más adelante introduciremos las parametrizaciones planas de variedades lisas, Cohen-Macaulay y Gorenstein, es decir, los morfismos lisos, Cohen-Macaulay, Gorenstein, respectivamente.

Probaremos que los morfismos lisos coinciden con los morfismos formalmente lisos, lo cual equivaldrá a dar una caracterización de los morfismos lisos en términos de sus funtores de puntos.

1. Definición: Diremos que un morfismo $\mathrm{Spec}B \to \mathrm{Spec}A$ es un morfismo liso si plano, de tipo finito y las fibras son variedades algebraicas lisas.

Si $X \to S$ es un morfismo liso entonces la inmersión diagonal $X \hookrightarrow X \times_S X$ es una inmersión regular, por por 7.7.10 (porque lo es en fibras sobre S por 7.4.9).

2. Definición: Diremos que un morfismo $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es de dimensión n si sus fibras son unión de cerrados irreducibles de dimensión n.

3. Teorema: *Sea $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es un morfismo de tipo finito plano de dimensión n. Entonces, f es liso si y solo si $\Omega_{B/A}$ es un B-módulo localmente libre de rango n.*

Demostración. Si f es liso entonces $\Omega_{B/A}$ es un B-módulo localmente libre por 7.4.5, y es de rango n porque en fibras es de rango n por 4.3.14. Recíprocamente si $\Omega_{B/A}$ es un B-módulo localmente libre de rango n, entonces así sucede en fibras sobre $S = \operatorname{Spec} A$, luego éstas son lisas por 4.3.14. □

7.8.1. Extensiones de álgebras conmutativas

Todas las álgebras consideradas son conmutativas.

4. Definición: Sea B una A-álgebra y L un B-módulo. Llamaremos A-extensión de B por L a toda sucesión exacta de A-módulos

$$0 \to L \to E \xrightarrow{\pi} B \to 0,$$

donde E es una A-álgebra, pensamos el morfismo $L \to E$ como una inclusión, π es morfismo de A-álgebras y $e \cdot l = \pi(e) \cdot l$ para cualesquiera $e \in E$, $l \in L$.

Es inmediato comprobar que L es un ideal de E de cuadrado nulo.

5. Definición: Llamaremos A-extensión trivial de B por L a la A-álgebra $E = B \oplus L$, con el producto definido por $(b,l)\cdot(b',l') = (bb', bl' + b'l)$ y la denotaremos $B * L$.

6. Definición: Sean E y E' dos A-extensiones de B por L. Un isomorfismo de A-álgebras $\phi\colon E \to E'$ diremos que es un isomorfismo de A-extensiones de B por L si el el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow \mathrm{Id} & & \downarrow \phi & & \downarrow \mathrm{Id} & & \\ 0 & \longrightarrow & L & \longrightarrow & E' & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

es conmutativo. Denotaremos $\operatorname{Isom}_{B-\mathrm{ext}}(E,E')$ al conjunto de isomorfismos de A-extensiones.

Diremos que una extensión es trivial si es isomorfa a la extensión trivial.

7. Proposición : *E es trivial si y solo si el morfismo $E \to B$ admite sección (de A-álgebras). Además,*

$$\mathrm{Isom}_{B-ext}(B*L, B*L) = \mathrm{Der}_A(B,L)$$

Demostración. La extensión trivial tiene sección $B \to B*L$, $b \mapsto (b,0)$. Recíprocamente, si $s\colon B \to E$ es una sección, induce un morfismo $B*L \to E$, $(b,l) \mapsto s(b)+l$, que es un isomorfismo de extensiones.

Dada una A-derivación D de B en L, consideremos el morfismo $B*L \to B*L$ definido por $(b,l) \mapsto (b, l+Db)$ es un isomorfismo de extensiones. Recíprocamente, si $B*L \xrightarrow{\phi} B*L$ es un isomorfismo de extensiones, entonces $\phi(b,l) = (b, l+Db)$, siendo $D\colon B \to L$ un morfismo de A-módulos, que es una derivación por ser ϕ morfismo de álgebras. □

Denotaremos $\mathrm{Exalcom}_A(B,L)$ al conjunto de A-extensiones de B por L, módulo isomorfismos de A-extensiones.

Un morfismo de B-módulos $f\colon L \to L'$ induce una aplicación

$$\begin{aligned} f_*\colon \mathrm{Exalcom}_A(B,L) &\to \mathrm{Exalcom}_A(B,L') \\ E &\mapsto (E*L')/(l, -f(l))_{l\in L} \end{aligned}$$

El conjunto $\mathrm{Exalcom}_A(B,L)$ tiene estructura de grupo mediante el producto:

$$\begin{aligned} \mathrm{Exalcom}_A(B,L) \times \mathrm{Exalcom}_A(B,L) &\longrightarrow \mathrm{Exalcom}_A(B,L) \\ (E,E') &\longmapsto E \underset{B}{\times} E'/(l,-l)_{l\in L}, \end{aligned}$$

donde $E \times_B E' = \{(e,e') \in E \times E' \colon \pi(e) = \pi'(e')\}$. El elemento neutro es la extensión trivial. El paso al opuesto es el morfismo $(-1)_*$, siendo $-1\colon L \to L$, $l \mapsto -l$. Con esta estructura, el morfismo f_* anteriormente definido es morfismo de grupos.

Un morfismo de A-álgebras $\phi\colon B \to B'$, induce un morfismo de grupos

$$\begin{aligned} \phi^*\colon \mathrm{Exalcom}_A(B',L) &\to \mathrm{Exalcom}_A(B,L) \\ E' &\mapsto E' \underset{B}{\times} B' \end{aligned}$$

Finalmente, un morfismo de anillos $\phi\colon A \to A'$ induce un morfismo de grupos

$$\begin{aligned} \phi'\colon \mathrm{Exalcom}_{A'}(B,L) &\to \mathrm{Exalcom}_A(B,L) \\ E &\mapsto E \end{aligned}$$

cuyo núcleo se denota $\mathrm{Exalcom}_{A'/A}(B,L)$ y representa las clases de A'-extensiones de B por L que son A-extensiones triviales.

8. Teorema: *Sean $A \xrightarrow{f} B \xrightarrow{\phi} B'$ morfismos de anillos y L un B'-módulo. Se tienen las sucesiones exactas*

1. $0 \to \mathrm{Der}_B(B',L) \to \mathrm{Der}_A(B',L) \to \mathrm{Der}_A(B,L) \xrightarrow{\delta} \mathrm{Exalcom}_{B/A}(B',L) \to 0.$
2. $0 \to \mathrm{Exalcom}_{B/A}(B',L) \to \mathrm{Exalcom}_B(B',L) \xrightarrow{f'} \mathrm{Exalcom}_A(B',L) \xrightarrow{\phi^*} \mathrm{Exalcom}_A(B,L).$

Es decir, se tiene la sucesión exacta

$$0 \to \mathrm{Der}_B(B',L) \to \mathrm{Der}_A(B',L) \to \mathrm{Der}_A(B,L) \to$$
$$\to \mathrm{Exalcom}_B(B',L) \xrightarrow{f'} \mathrm{Exalcom}_A(B',L) \xrightarrow{\phi^*} \mathrm{Exalcom}_A(B,L)$$

Demostración. En primer lugar, definamos $\delta\colon \mathrm{Der}_A(B,L) \to \mathrm{Exalcom}_B(B',L)$. Dada una A-derivación $D\colon B \to L$, consideramos la A-extensión trivial $B' * L$ y la dotamos de estructura de B-álgebra mediante el morfismo de anillos

$$B \longrightarrow B' * L$$
$$b \mapsto (\phi(b), Db)$$

que es morfismo de anillos por ser D derivación. Además el morfismo $B' * L \to B'$ es de B-álgebras, luego $B' * L$ es una B-extensión de B' por L. Veamos ahora la exactitud de la sucesión.

- La exactitud de $0 \to \mathrm{Der}_B(B',L) \to \mathrm{Der}_A(B',L) \to \mathrm{Der}_A(B,L)$ es inmediata.

- Exactitud de $\mathrm{Der}_A(B',L) \to \mathrm{Der}_A(B,L) \xrightarrow{\delta} \mathrm{Exalcom}_B(B',L)$. Sea D una A-derivación de B en L. Si D proviene de una derivación de B' (que seguimos denotando D), entonces la B-extensión $B' * L$ construida anteriormente admite la sección $B' \to B' * L$, $b' \mapsto (b', Db')$, luego es trivial. Recíprocamente, si la B-extensión $B' * L$ asociada a D es trivial, entonces admite sección $B' \to B' * L$, $b' \mapsto (b', D'b')$ y D' es una derivación de B' en L que restringida a B es D.

- Exactitud de $\mathrm{Der}_A(B,L) \xrightarrow{\delta} \mathrm{Exalcom}_B(B',L) \xrightarrow{f'} \mathrm{Exalcom}_A(B',L)$. Por definición de δ, la B-extensión $\delta(D)$ es A-trivial. Recíprocamente, si una B-extensión E de B' por L es A-trivial, entonces $E = B' * L$, como A-álgebra, y el morfismo de anillos $B \to B' * L$, $b \mapsto (\phi(b), Db)$ define una A-derivación D de B en L, de modo que $E = \delta(D)$.

- Exactitud de $\mathrm{Exalcom}_B(B',L) \xrightarrow{f'} \mathrm{Exalcom}_A(B',L) \xrightarrow{\phi^*} \mathrm{Exalcom}_A(B,L)$. Si E es una A-extensión de B' por L que está en el núcleo de ϕ^*, entonces $E \times_{B'} B$ es A-extensión trivial de B por L, luego admite sección $B \to E \times_{B'} B$. Componiendo este sección con la proyección natural $E \times_{B'} B \to E$, se obtiene un morfismo de anillos $B \to E$ que dota a E de estructura de B-álgebra, compatible con su estructura de A-álgebra. Por tanto, E está en la imagen de f'. Recíprocamente, si E es una B-extensión de B' por L, entonces $E \times_{B'} B$ es una A-extensión trivial de B por L, porque la proyección $E \times_{B'} B \to B$ tiene sección $b \mapsto (b, b)$ □

7.8.2. Morfismos formalmente lisos

9. Definición: Un morfismo de anillos $A \to B$ es formalmente liso si para toda A-álgebra C y todo ideal I de C de cuadrado nulo, el morfismo natural

$$\mathrm{Hom}_{A-\text{álg}}(B,C) \to \mathrm{Hom}_{A-\text{álg}}(B,C/I)$$

es epiyectivo. También se dice que B es formalmente liso sobre A.

10. Ejemplo: Es inmediato que el anillo de polinomios $A[x_1,\ldots,x_n]$ es formalmente liso sobre A.

11. Proposición: *Si $A \to B$ es un morfismo de anillos formalmente liso y $A \to A'$ es un morfismo de anillos, entonces $A' \to A' \otimes_A B$ es un morfismo de anillos formalmente liso.*

Demostración. En efecto,

$$\mathrm{Hom}_{A'-\text{álg}}(A' \otimes_A B, C) = \mathrm{Hom}_{A-\text{álg}}(B,C) \twoheadrightarrow \mathrm{Hom}_{A-\text{álg}}(B,C/I) = \mathrm{Hom}_{A'-\text{álg}}(A' \otimes_A B, C/I).$$

□

12. Teorema: *Si $f : A \to B$ es formalmente liso, entonces $\Omega_{B/A}$ es un B-módulo proyectivo.*

Demostración. Sea $M \to \overline{M} \to 0$ un epimorfismo de módulos. Hay que ver que tomando $\mathrm{Hom}_B(\Omega_{B/A}, \quad)$, se obtiene un epimorfismo. Es decir, hay que ver que el morfismo $\mathrm{Der}_A(B,M) \to \mathrm{Der}_A(B,\overline{M})$ es epiyectivo. Sea D una A-derivación de B en $\overline{M}$. Consideremos el diagrama

$$\begin{array}{ccc} B & \xrightarrow{(\mathrm{Id},D)} & B * \overline{M} \\ {\scriptstyle f}\uparrow & & \uparrow \\ A & \xrightarrow{(f,0)} & B * M \end{array}$$

Por ser f formalmente liso, (Id,D) extiende a un morfismo $\alpha : B \to B * M$. Ahora, $\alpha = (\mathrm{Id},D')$, con D' una A-derivación de B en M, que compuesta con el epimorfismo $M \to \bar{M}$ es la derivación D. □

13. Teorema: *$A \to B$ es formalmente liso $\Leftrightarrow \mathrm{Exalcom}_A(B,L) = 0$, para todo B-módulo L.*

Demostración. Supongamos que $A \to B$ es formalmente liso y veamos que toda A-extensión de B por L es trivial. Si E es una A-extensión de B por L, el morfismo $E \xrightarrow{\pi} B$ induce una aplicación $\mathrm{Hom}_{A-\text{álg}}(B,E) \to \mathrm{Hom}_{A-\text{álg}}(B,B)$, que es epiyectiva por ser $A \to B$ formalmente liso. En particular, la identidad de B tiene antimagen, luego $E \to B$ tiene sección y por tanto es trivial.

Recíprocamente, supongamos que toda A-extensión de B es trivial y veamos que $A \to B$ es formalmente liso. Sea C una A-álgebra e I un ideal de C de cuadrado nulo. Tenemos que ver que el morfismo $\mathrm{Hom}_{A-\text{álg}}(B,C) \to \mathrm{Hom}_{A-\text{álg}}(B,C/I)$ es epiyectivo. Dado un morfismo $B \to C/I$, el producto fibrado $B \underset{C/I}{\times} C$ es una A-extensión de B por I, que ha de ser trivial por hipótesis. Por tanto, existe sección $B \to B \underset{C/I}{\times} C$, que compuesta con la proyección en C nos da el morfismo $B \to C$ buscado. □

14. Lema: *Sea $I \subset B$ un ideal y L un B-módulo. Entonces, se cumple*

$$\mathrm{Hom}_B(I/I^2, L) \simeq \mathrm{Exalcom}_B(B/I, L).$$

Demostración. Sea E una B-extensión de B/I por L. La imagen de I por el morfismo estructural $B \to E$ está contenida en L, luego induce un morfismo $I/I^2 \to L$ de B-módulos . Recíprocamente, sea $f : I/I^2 \to L$ un morfismo de B-módulos. Obviamente, B/I^2 es una B-extensión de B/I por I/I^2, luego $f_*(B/I^2)$ es una B-extensión de B/I por L. Es fácil ver que estas asignaciones son inversas entre sí.

□

15. Criterio jacobiano de lisitud formal: *Sea $A \to B$ un morfismo formalmente liso e I un ideal de B. La condición necesaria y suficiente para que B/I sea formalmente liso sobre A es que la sucesión de diferenciales*

$$0 \to I/I^2 \to \Omega_{B/A} \otimes_B B/I \to \Omega_{(B/I)/A} \to 0$$

sea exacta y escindida.

Demostración. Supongamos que B/I es formalmente liso sobre A. Por ser $\Omega_{(B/I)/A}$ un B/I-módulo proyectivo (por 7.8.12), la sucesión de diferenciales es exacta si y solo si tomando homomorfismos en todo B/I-módulo L es exacta. Por el lema anterior obtenemos la sucesión

$$0 \to \mathrm{Der}_A(B/I, L) \to \mathrm{Der}_A(B, L) \to \mathrm{Exalcom}_B(B/I, L) \to 0$$

que es exacta por el teorema 7.8.8.

Recíprocamente, si la sucesión $0 \to I/I^2 \to \Omega_{B/A} \otimes_B B/I \to \Omega_{(B/I)/A} \to 0$ es exacta y escindida, entonces para todo B/I-módulo L se obtiene tomando $\mathrm{Hom}_{B/I}(-,L)$, por el lema anterior, la sucesión exacta

$$0 \to \mathrm{Der}_A(B/I,L) \to \mathrm{Der}_A(B,L) \to \mathrm{Exalcom}_B(B/I,L) \to 0$$

Como B es formalmente liso, entonces $\mathrm{Exalcom}_A(B,L) = 0$, luego de nuevo por el teorema 7.8.8, obtenemos que $\mathrm{Exalcom}_A(B/I,L) = 0$ y por tanto $A \to B/I$ es formalmente liso.

□

16. Corolario: *Sea A un anillo noetheriano y C una A-álgebra de tipo finito. C es lisa sobre A si y solo si es formalmente lisa.*

Demostración. Por ser C una A-álgebra de tipo finito $C = A[x_1,\dots,x_n]/I$. Sea $B := A[x_1,\dots,x_n]$, entonces $C = B/I$.

Si C es una A-álgebra lisa entonces $\Omega_{C/A}$ es un C-módulo localmente libre y la sucesión del criterio jacobiano de lisitud formal es exacta porque lo es en fibras sobre los puntos cerrados de $\mathrm{Spec}\, A$, luego $A \to C$ es formalmente liso.

Supongamos que C es una A-álgebra formalmente lisa. Obviamente C en fibras sobre y cumple el criterio Jacobiano de lisitud, luego en fibras es liso. Sólo nos falta probar que C es A-plano. Dado $\mathfrak{m}_x \subset C$ y $\mathfrak{p}_y = \mathfrak{m}_x \cap A$, solo tenemos que probar que $A_y \to C_x$ es plano. La lisitud formal es estable por localizaciones. Podemos suponer que A es local de ideal maximal $\mathfrak{p}_y$. Probemos que $I/\mathfrak{m}_x I = \bar{I}/\bar{\mathfrak{m}}_x \bar{I}$, donde denotamos con las barras los correspondientes ideales en $B/\mathfrak{p}_y B$. Tensando por $\otimes_C C/\mathfrak{m}_x$ en la sucesión exacta del criterio formal de lisitud, obtenemos que $I/\mathfrak{m}_x I \subset \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2$ e igualmente, como $A/\mathfrak{p}_y \to C/\mathfrak{p}_y C$ es formalmente liso, $\bar{I}/\bar{\mathfrak{m}}_x \bar{I} \subset \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2$; y ambos subespacios coinciden. Sea $f_1,\dots,f_r$ un sistema generador mínimo (localmente en x) de I, entonces $\bar{f}_1,\dots,\bar{f}_r \in \bar{I}$, es un sistema generador mínimo de $\bar{I}$. La sucesión $\bar{f}_1,\dots,\bar{f}_r$ es regular, entonces por 7.7.10, $A \to C_x$ es plano.

□

7.9. Problemas

1. Sea $f : K \to L$ un morfismo de complejos y $\mathrm{Cono}(f)$ su cono. Prueba

   a) si f es inyectivo, el morfismo natural $\mathrm{Cono}(f) \to \mathrm{Coker}\, f$ es un cuasi-isomorfismo.

   b) si f es epiyectivo, el morfismo natural $(\mathrm{Ker}\, f)[1] \to \mathrm{Cono}(f)$ es un cuasi-isomorfismo.

2. Sea K un bicomplejo y denotemos por $K^{\leq m} = \cdots \to K^{i,\cdot} \to \cdots \to K^{m-1,\cdot} \to Z^m \to 0$ (donde $Z^m = \operatorname{Ker} \mathrm{d}_1^m$). Demuestra que el conúcleo de la inclusión $K^{\leq n-1} \hookrightarrow K^{\leq n}$ es cuasi-isomorfo a $H_{\mathrm{d}_1}(K)[-n]$

3. Dar una nueva demostración del teorema 7.2.16 usando el problema anterior.

4. Prueba que si $f : K \to L$ es un cuasi-isomorfismo entre complejos superiormente acotados de A-módulos planos y M es otro complejo de A-módulos, entonces $f \otimes 1 : K \otimes M \to L \otimes M$ es un cuasi-isomorfismo.

5. **Fórmula de Kunneth algebraica:** Sea K un complejo superiormente acotado de A-módulos planos cuyos grupos de cohomología sean A-módulos planos y K' otro complejo de A-módulos. Entonces el morfismo natural

$$H(K) \otimes_A H(K') \to H(K \otimes_A K')$$

es isomorfismo.

Resolución: Sean d y d' las diferenciales de K y K' respectivamente, $Z = \operatorname{Ker} d$ y $B = \operatorname{Im} d$.

De las sucesiones exactas

$$0 \to Z^n \to K^n \xrightarrow{d} B^{n+1} \to 0$$
$$0 \to B^n \to Z^n \to H^n(K) \to 0$$

por inducción descendente obtenemos que B y Z son complejos de A-módulos planos. Podemos suponer que K es acotado, sin más que poner K como límite inductivo de acotados $K = \varinjlim K_n$, siendo K_n el subcomplejo $K_n = \bigoplus_{r \geq -n} K^r$, pues

la cohomología y el producto tensorial conmutan con límites inductivos.

Sea $K^{\leq n} \equiv \cdots \to K^{n-2} \to K^{n-1} \to Z^n \to 0$. Como K es superiormente acotado, basta ver que el teorema es cierto para $K^{\leq n}$ para todo n. Se tiene la sucesión exacta de módulos planos

$$0 \to K^{\leq n-1} \to K^{\leq n} \to C_n \to 0$$

con $C_n = 0 \to B^n \to Z^n \to 0$. Como K es acotado, $K^{\leq n-1}$ es nulo para n suficientemente pequeño, luego basta probar el teorema para C_n. El epimorfismo natural $C_n \xrightarrow{\pi} H^n(K)[-n]$ es un cuasi-isomorfismo. Tensando por K', $C_n \otimes K'$ es cuasi-isomorfo a $H^n(K)[-n] \otimes K'$ (obsérvese que $H^n(K)$ es plano y $\operatorname{Ker} \pi = 0 \to B^n \to B^n \to 0$, o aplíquese el teorema 7.2.16). Como el teorema es cierto para $H^n(K)$, hemos terminado.

6. Prueba que A es regular si y solo si $A[x]$ lo es.

7. Sea M un A-módulo inyectivo y $\bar{A} = A/J$. Prueba que $\mathrm{Hom}_A(\bar{A}, M)$ es un $\bar{A}$-módulo inyectivo. Prueba que si $\mathrm{Ext}^i_A(\bar{A}, A) = 0$, para todo $i \neq n$, entonces para todo $\bar{A}$-módulo N se verifica

$$\mathrm{Ext}^i_A(N, \mathrm{Ext}^n_A(\bar{A}, A)) = \mathrm{Ext}^{i+n}_A(N, A)$$

8. Sea N un A-módulo y $x \in A$ un elemento A-regular y N-regular. Sea M un A/xA-módulo. Prueba que $\mathrm{Ext}^i_A(N, M) = \mathrm{Ext}^i_{A/xA}(N/xN, M)$.

9. Sea A un anillo noetheriano. Prueba que A es un anillo de Cohen-Macaulay si y solo si $A[x]$ lo es.

10. Sea A un anillo noetheriano. Prueba que A es un anillo de Gorenstein si y solo si $A[x]$ lo es.

Capítulo 8

Desingularización de superficies

Juan B. Sancho

8.1. Introducción

En este capítulo vamos a dar una demostración completa de la desingularización de superficies, en característica cero, inmersas en un ambiente liso de dimensión tres. Seguiremos las líneas maestras de la desingularización de Hironaka para variedades de dimensión arbitraria.

La demostración constará de las siguientes etapas:

Transformaciones permisibles. El primer paso es probar que las transformaciones permisibles (explosiones con centro liso equisingular) no aumentan la multiplicidad.

Reducción al caso singular. Usando la desingularización de anillos de dimensión uno, se demuestra que la desingularización de superficies se reduce al caso en que la superficie es el espectro de un anillo local.

Contacto maximal. Se prueba que existe una superficie lisa W, llamada de contacto maximal, que pasa por todos los puntos m-múltiples de la superficie singular S, conservándose esta propiedad después de una sucesión arbitraria de transformaciones permisibles.

La existencia de la superficie de contacto maximal se obtiene solo localmente. De aquí proviene la necesidad de reducir la desingularización al caso local. En este punto de la existencia de la superficie de contacto maximal es donde se hace uso de la hipótesis de característica cero.

Exponente idealístico. Consiste en una pareja (I,r), formada por un ideal I definido en la superficie de contacto maximal W y un entero $r>0$. Esta pareja tiene la propiedad de que su locus singular, definido por

$$\mathrm{Sing}_W(I,r)=\{w\in W:\mathrm{mult.}_w I\geq r\}$$

coincide con el locus de los puntos m-múltiples de la superficie singular S. Además, la propiedad anterior se mantiene por transformaciones permisibles (con una conveniente definición de transformada propia de un exponente idealístico).

Desingularización de un ideal. El último paso es probar que una pareja (I,r) se desingulariza mediante un número finito de transformaciones permisibles. Por la propiedad dicha del exponente idealístico, esas mismas transformaciones dan lugar a que en la superficie singular S desaparezcan los puntos m-múltiples.

Veremos que la desingularización de (I,r) consiste, en buena parte, en desingularizar las curvas definidas en W por los generadores del ideal I.

Las ideas básicas para desingularizar las variedades algebraicas de cualquier dimensión son las mismas que las que se usan aquí para superficies. La desingularización de variedades se prueba mediante un argumento inductivo que se puede resumir con mucha imprecisión así: La desingularización de variedades de dimensión $\leq n-1$ permite desingularizar ideales (I,r) definidos en dimensión n, y esto a su vez permite desingularizar las variedades de dimensión n.

Supondremos k algebraicamente cerrado de característica cero. Los anillos considerados serán siempre noetherianos.

8.2. Multiplicidad y platitud normal en hipersuperficies

Dado $x \in \operatorname{Spec} A$, denotemos $(A_x/\mathfrak{p}_x A_x) = k(x)$ el cuerpo residual de x.

1. Lema: *Sea M un A-módulo finito generado. La función*

$$f\colon \operatorname{Spec} A \to \mathbb{N},\ f(x) = \dim_{k(x)} M \otimes_A k(x).$$

es una función semicontinua superiormente (es decir, $\{x \in \operatorname{Spec} A\colon f(x) > m\}$ es un cerrado de $\operatorname{Spec} A$ para cada $m \in \mathbb{N}$).

Demostración. Es la proposición 0.10.10. De otro modo: Si $f(x) = n$ entonces por el lema de Nakayama existen $m_1,\ldots,m_n \in M$ que generan M_x. Entonces, $m_1,\ldots,m_n$ generan M en un entorno U de x, luego $f(y) \leq n$ para todo $y \in U$. Por tanto, f es una función semicontinua superiormente. □

2. Teorema: *Sea $H = \operatorname{Spec} A$ una hipersuperficie de una k-variedad regular X. La multiplicidad de H, en los puntos cerrados de H, es una función superiormente semicontinua. Como consecuencia, la multiplicidad alcanza un máximo finito.*

Demostración. Sea $\Delta \subset (A \otimes_k A)$ el ideal de la diagonal. Consideremos los módulos de jets de orden r o de partes principales de orden r,

$$J^r_{A/k} := (A \otimes_k A)/\Delta^{r+1}$$

con la estructura de A-módulo por el segundo factor. Se verifica que $J^r_{A/k} \otimes_A k(x) = A/\mathfrak{m}_x^{r+1}$ (véase 3.6.4). Así pues, la función de Samuel de H en x es $S_{A_x}(n) = l(A/\mathfrak{m}_x^n) = \dim_{k(x)} J^{n-1}_{A/k} \otimes_A k(x)$.

Por otra parte, si X es una variedad regular de dimensión d y H es una hipersuperficie definida por los ceros de una función de multiplicidad m_x en x, entonces (ejemplo 5.6.4) la función de Samuel de H en x es

$$S_{A_x}(n+1) = \binom{n+d}{d} - \binom{n+d-m_x}{d}.$$

Por tanto, $S_{A_x}(n+1) > \binom{n+d}{d} - 1 \iff n - m_x < 0 \iff m_x > n$. Con todo, $m_x > n \iff \dim_{k(x)} J^n_{A/k} \otimes_A k(x) > \binom{n+d}{d} - 1$. Por el lema anterior, la multiplicidad es una función superiormente semicontinua. La consecuencia se sigue de la noetherianidad de A. □

Sea X una variedad algebraica e Y una subvariedad algebraica cerrada de X definida por un ideal $I \subset \mathcal{O}_X$.

3. Definición: Se dice que X es normalmente plano a lo largo de Y, si el graduado

$$G_I \mathcal{O}_X = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$$

es una $\mathcal{O}_Y$-álgebra plana, es decir, I^n/I^{n+1} es un $\mathcal{O}_Y$-módulo plano para todo n.

4. Lema: *Sea $\mathcal{O}$ un anillo local regular de dimensión n, $x \in \operatorname{Spec}\mathcal{O}$ el punto cerrado e $y \in \operatorname{Spec}\mathcal{O}$. Si $\mathcal{O}/\mathfrak{p}_y$ es un anillo local regular de dimensión r, entonces $\mathfrak{p}_y$ está generado por $n-r$ parámetros de diferenciales en x linealmente independientes y $\mathcal{O}_y$ es un anillo regular de dimensión $n-r$.*

Demostración. Denotemos por $\mathfrak{m}$ al ideal maximal de $\mathcal{O}$. Por 4.3.10, $\mathfrak{p}_y = (t_1, \ldots, t_{n-r})$, donde los t_i son linealmente independientes en $\mathfrak{m}/\mathfrak{m}^2$. De nuevo por 4.3.10, los anillos $\mathcal{O}/(t_1, \ldots, t_i)$ son regulares. Por tanto, $0 \subset (t_1) \subset \cdots \subset (t_1, \ldots, t_{n-r}) = \mathfrak{p}_y$ es una cadena de ideales primos y $\dim \mathcal{O}_y \geq n-r$. Como $\mathfrak{p}_y \mathcal{O}_y$ está generado por $n-r$ parámetros concluimos que $\mathcal{O}_y$ es un anillo regular de dimensión $n-r$. □

5. Proposición: *En las hipótesis y notaciones del lema anterior, se cumple que*

$$G_{\mathfrak{p}_y}\mathcal{O} = \mathcal{O}/\mathfrak{p}_y[t_1,\ldots,t_{n-r}]$$

Demostración. Consideremos el morfismo epiyectivo

$$\begin{aligned}\mathcal{O}/\mathfrak{p}_y[t_1,\ldots,t_{n-r}] &\xrightarrow{\phi} G_{\mathfrak{p}_y}\mathcal{O}\\ t_i &\mapsto \bar{t}_i \in \mathfrak{p}_y/\mathfrak{p}_y^2\end{aligned}$$

$\mathcal{O}_y$ es regular, luego ϕ es isomorfismo al localizar en y; como $\mathcal{O}/\mathfrak{p}_y[t_1,\ldots,t_{n-r}]$ es íntegro, se concluye que ϕ es isomorfismo.

□

6. Corolario: *Toda variedad regular es normalmente plana a lo largo de cualquier subvariedad regular.*

Nos encontramos ahora con una dificultad técnica que será definitivamente resuelta en el capítulo de esquemas. Si $A[\xi_1,\ldots,\xi_n]$ es una A-álgebra graduada, entonces $\widetilde{X} = \mathrm{Proj}\,A[\xi_1,\ldots,\xi_n]$ no es, en general, una variedad afín, es decir, no es isomorfo a $\mathrm{Spec}B$, para cierto anillo B. Los espectros proyectivos no son variedades algebraicas afines, en general. Al explotar a lo largo de una subvariedad nos salimos del marco de las variedades afines, en general. Ahora bien, sabemos que $\widetilde{X}$ se recubre por las variedades afines

$$U^h_{\xi_i} = \mathrm{Spec}\,A[\xi_1/\xi_i,\ldots,\xi_n/\xi_i]$$

Toda variedad algebraica es unión de variedades algebraicas afines. Por ello estudiaremos las propiedades de las variedades algebraicas proyectivas, localmente. Así pues, cuando escribamos $\mathcal{O}_{\widetilde{X}}$ entienda el lector que estamos considerando las funciones de $\widetilde{X}$ en cualquiera de los abiertos afines que recubren $\widetilde{X}$. Por ejemplo, diremos que $\widetilde{X}$ es regular en un punto, si al restringirnos a un abierto afín U que contenga a x, el anillo local $(\mathcal{O}_U)_x$ es regular (de hecho, este anillo local no depende del abierto afín considerado). Cuando digamos subvariedad cerrada de $\widetilde{X}$, queremos decir que en cada abierto afín es una subvariedad algebraica cerrada, etc. Trate el lector a las variedades algebraicas proyectivas como afines y cuando quiera probar algo hágalo localmente. Si el lector conoce el concepto de variedad diferenciable, en Geometría Diferencial, estará ya habituado a ello.

7. Teorema: *Si $\widetilde{X} \to X$ es la explosión de una variedad regular X con centro en una subvariedad regular Y, entonces $\widetilde{X}$ es regular.*

Demostración. Sea $\mathfrak{p}_Y \subset \mathscr{O}_X$ el ideal primo de las funciones que se anulan en Y y

$$\pi\colon \tilde{X} = \operatorname{Proj} D_{\mathfrak{p}_Y}\mathscr{O}_X \to X$$

el morfismo de explosión.

Sabemos que $\pi^{-1}(X\setminus Y) = X\setminus Y$, luego todos los puntos de $\pi^{-1}(X\setminus Y)$ son regulares. Por otra parte, $\pi^{-1}(Y) = \operatorname{Proj} G_{\mathfrak{p}_Y}\mathscr{O}_X$ que es localmente isomorfo (por el lema anterior) a

$$\operatorname{Proj}\mathscr{O}/\mathfrak{p}_Y[t_1,\dots,t_{n-r}] = \mathbb{P}^{n-r-1}\times Y$$

siendo r la dimensión de Y. Por tanto, $\mathscr{O}_{\tilde{X}}/\mathfrak{p}_Y\mathscr{O}_{\tilde{X}}$ es un anillo regular. Ahora bien, $\mathfrak{p}_Y\mathscr{O}_{\tilde{X}}$ es un ideal localmente principal. Como la explosión de un anillo íntegro es íntegro, $\tilde{X}$ es regular en los puntos de $\pi^{-1}(Y)$, pues si el cociente de un anillo local íntegro por una función es regular, entonces el anillo es regular.

□

Sea H una hipersuperficie de una variedad regular X definida localmente por los ceros de una función $f \in \mathscr{O}_X$. Sea Y una subvariedad regular contenida en H, definida en X por los ceros de un ideal $\mathfrak{p}$, que denotaremos por $\bar{\mathfrak{p}}$ cuando nos restrinjamos a H. Sea $m \in \mathbb{N}$ tal que $f \in \mathfrak{p}^m\setminus\mathfrak{p}^{m+1}$.

8. Lema: *La multiplicidad de H en el punto genérico de Y es m.*

Demostración. Por 8.2.5, $G_{\mathfrak{p}}\mathscr{O}_X = \mathscr{O}_Y[t_1,\dots,t_{n-r}]$. Sea g el punto genérico de Y y $\Sigma = \mathscr{O}_{Y,g}$ el cuerpo de fracciones de $\mathscr{O}_Y$. Entonces $G_{\mathfrak{p}}\mathscr{O}_{X,g} = \Sigma[t_1,\dots,t_{n-r}]$. Por tanto, $\mathscr{O}_{X,g}$ es un anillo local regular y $f \in \mathfrak{p}^m\mathscr{O}_{X,g}\setminus\mathfrak{p}^{m+1}\mathscr{O}_{X,g}$. Si denotamos $\operatorname{in}_{\mathfrak{p}} f$ la clase de f en $\mathfrak{p}^m/\mathfrak{p}^{m+1} \subset G_{\mathfrak{p}}\mathscr{O}_{X,g}$, entonces, por 4.2.5,

$$G_{\bar{\mathfrak{p}}}\mathscr{O}_{H,g} = \Sigma[t_1,\dots,t_{n-r}]/(\operatorname{in}_{\mathfrak{p}} f)$$

y concluimos que la multiplicidad de H en g es m. □

9. Corolario: *La multiplicidad de H en un punto cerrado de Y es mayor o igual que la multiplicidad de H en el punto genérico de Y.*

Demostración. Sea $y \in Y$ un punto cerrado. Si la multiplicidad de H en el punto genérico es m, entonces $f \in \mathfrak{p}^m \subseteq \mathfrak{m}_y^m$, luego la multiplicidad en el punto y es mayor o igual que m. □

10. Proposición: *Con las notaciones anteriores, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es $\mathscr{O}_Y$-plano $\iff$ La multiplicidad de H en todos los puntos cerrados de Y es la misma que en el punto genérico de Y.*

Demostración. Evidentemente la cuestión es local, luego podemos localizar en un punto cerrado $y \in Y$. Tenemos la sucesión exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_{\mathfrak{p}}\mathscr{O}_X & \xrightarrow{\cdot \mathrm{in}_{\mathfrak{p}} f} & G_{\mathfrak{p}}\mathscr{O}_X & \longrightarrow & G_{\bar{\mathfrak{p}}}\mathscr{O}_H & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \mathscr{O}_Y[t_i] & \xrightarrow{\cdot \mathrm{in}_{\mathfrak{p}} f} & \mathscr{O}_Y[t_i] & \longrightarrow & G_{\bar{\mathfrak{p}}}\mathscr{O}_H & \longrightarrow & 0 \end{array}$$

$\mathscr{O}_Y[t_i]$ es un $\mathscr{O}_Y$-módulo plano, pues es libre. Por 7.5.1, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano $\iff$ la sucesión anterior tensada por el cuerpo residual de y sigue siendo exacta. Al tensar se obtiene

$$\begin{array}{ccccc} \bigoplus_n (\mathfrak{p}^n/\mathfrak{m}_y\mathfrak{p}^n) & \xrightarrow{\cdot[\mathrm{in}_{\mathfrak{p}} f]\in(\mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m)} & \bigoplus_n (\mathfrak{p}^{n+m}/\mathfrak{m}_y\mathfrak{p}^{n+m}) & \longrightarrow & G_{\bar{\mathfrak{p}}}\mathscr{O}_H \otimes_{\mathscr{O}_Y} k(y) \longrightarrow 0 \\ \| & & \| & & \\ k(y)[t_i] & & k(y)[t_i] & & \end{array}$$

Por tanto, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano $\iff$ la clase de f en $\mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m$ es distinta de cero. El morfismo $\mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m \hookrightarrow \mathfrak{m}_y^m/\mathfrak{m}_y^{m+1}$ es inyectivo (recordemos que $G_{\mathfrak{p}}\mathscr{O}_X = \mathscr{O}_X/\mathfrak{p}[t_1,\ldots,t_{n-r}]$ y $G_{\mathfrak{m}_y}\mathscr{O}_X = \mathscr{O}_X/\mathfrak{m}_y[t_1,\ldots,t_n]$). Por tanto, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano $\iff$ la clase de f en $\mathfrak{m}_y^m/\mathfrak{m}_y^{m+1}$ es distinta de cero. Es decir, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano $\iff$ la multiplicidad de H en el punto cerrado coincide con la multiplicidad de H en el punto genérico de Y. □

11. Observación: Consideremos el diagrama

$$0 \to G_{\mathfrak{p}}\mathscr{O}_X \xrightarrow{\cdot \mathrm{in}_{\mathfrak{p}} f} G_{\mathfrak{p}}\mathscr{O}_X \longrightarrow G_{\bar{\mathfrak{p}}}\mathscr{O}_H \to 0$$

En la demostración del teorema hemos dicho que $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano si y solo si $[\mathrm{in}_{\mathfrak{p}} f] \in \mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m$ es distinto de cero. Con los mismos argumentos, si tomamos solamente el término de $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ de grado m, tendremos que $\bar{\mathfrak{p}}^m/\bar{\mathfrak{p}}^{m+1}$ es plano si y solo si $[\mathrm{in}_{\mathfrak{p}} f] \in \mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m$ es distinto de cero. En conclusión, tenemos que $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano si y solo si su componente de grado m, $\bar{\mathfrak{p}}^m/\bar{\mathfrak{p}}^{m+1}$, es plana.

Así pues, el conjunto de puntos donde la hipersuperficie es normalmente plana a lo largo de una subvariedad regular es un abierto denso. Además, como el conjunto de puntos donde una variedad (íntegra) es regular es un abierto denso, el conjunto de puntos donde la hipersuperficie es normalmente plana a lo largo de una subvariedad (íntegra) es un abierto denso.

La proposición anterior la podemos reescribir como sigue.

12. Teorema: *Sea X una variedad regular, H una hipersuperficie de X e Y una subvariedad regular de H. Son equivalentes* [1]

1. *H es normalmente plano a lo largo de Y.*
2. *H es equimúltiple a lo largo de los puntos cerrados de Y (y en este caso la multiplicidad de H en un punto cerrado de Y coincide con la multiplicidad de H en el punto genérico de Y).*

Demos una caracterización geométrica de la platitud normal. Sea y un punto cerrado de Y. Sean

$C_{H,y} = \mathrm{Spec} G_{\mathfrak{m}_y}\mathscr{O}_H$ el cono normal a H en y

$C_{Y,y} = \mathrm{Spec} G_{\mathfrak{m}_y}\mathscr{O}_Y$ el cono normal a Y en y

$C_{H/Y} = \mathrm{Spec} G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ el cono normal de H a lo largo de Y

$C_{H/Y,y} = \mathrm{Spec}([G_{\bar{\mathfrak{p}}}\mathscr{O}_H] \otimes_{\mathscr{O}_Y} k(y))$ el cono normal de H a lo largo de Y en el punto y

Veamos que la platitud normal equivale a que, para cada punto cerrado de Y, se tenga un isomorfismo

$$C_{H,y} \simeq C_{Y,y} \times_{k(y)} C_{H/Y,y}$$

Se tiene la sucesión de morfismos

$$[G_{\bar{\mathfrak{p}}}\mathscr{O}_H] \underset{\mathscr{O}_Y}{\otimes} k(y) \to G_{\mathfrak{m}_y}\mathscr{O}_H \to G_{\mathfrak{m}_y}\mathscr{O}_Y$$

que en espectros define los morfismos $C_{Y,y} \to C_{H,y} \to C_{H/Y,y}$. Localmente en y, y siguiendo notaciones previas, $\mathfrak{p} = (t_1, \ldots, t_{n-r})$ y $(t_1, \ldots, t_{n-r}, x_1, \ldots, x_r) = \mathfrak{m}_y \subset \mathscr{O}_X$. Tenemos

$$\begin{aligned}
&G_{\bar{\mathfrak{p}}}\mathscr{O}_H = \mathscr{O}_Y[t_1, \ldots, t_{n-r}]/(\mathrm{in}_{\mathfrak{p}} f)\\
&\left[G_{\bar{\mathfrak{p}}}\mathscr{O}_H\right] \underset{\mathscr{O}_Y}{\otimes} k(y) = k(y)[t_1, \ldots, t_{n-r}]/([\mathrm{in}_{\mathfrak{p}} f])\\
&G_{\mathfrak{m}_y}\mathscr{O}_Y = k(y)[x_1, \ldots, x_r]\\
&G_{\mathfrak{m}_y}\mathscr{O}_H = k(y)[t_1, \ldots, t_{n-r}, x_1, \ldots, x_r]/(\mathrm{in}_{\mathfrak{m}_y} f)
\end{aligned}$$

Si $[\mathrm{in}_{\mathfrak{p}_Y} f]$ es igual a $\mathrm{in}_{\mathfrak{m}_y} f$, i.e., si la multiplicidad de H en y es igual a la multiplicidad de H en el punto genérico de Y, podemos definir un isomorfismo

$$\begin{array}{ccc}
\underset{k(y)[t_1,\ldots,t_{n-r},x_1,\ldots,x_r]/(\mathrm{in}_{\mathfrak{p}} f)}{\underbrace{([G_{\bar{\mathfrak{p}}}\mathscr{O}_H] \underset{\mathscr{O}_Y}{\otimes} k(y)) \underset{k(y)}{\otimes} G_{\mathfrak{m}_y}\mathscr{O}_Y}} & \xrightarrow{\sim} & \underset{k(y)[t_1,\ldots,t_{n-r},x_1,\ldots,x_r]/(\mathrm{in}_{\mathfrak{m}_y} f)}{\underbrace{G_{\mathfrak{m}_y}\mathscr{O}_H}}
\end{array}$$

[1] Si H no es una hipersuperficie, son equivalentes

1. H es normalmente plano a lo largo de Y.
2. La función de Hilbert de H es constante a lo largo de los puntos cerrados de Y.

Por tanto, si H es normalmente plano a lo largo de Y, entonces

$$C_{H,y} \simeq C_{Y,y} \times_{k(y)} C_{H/Y,y}$$

Es fácil demostrar el recíproco: Dado el isomorfismo, puede probarse que $m_y(H) = m_{\text{vért.}}(C_{H,y}) = m_{\text{vért.}}(C_{Y,y}) \cdot m_{\text{vért.}}(C_{H/Y,y}) = m_{\text{vért.}}(C_{H/Y,y})$ y este último coincide con la multiplicidad de H en el punto genérico de Y, luego H es normalmente plano a lo largo de Y.

8.3. Contacto maximal para hipersuperficies

Sea X una variedad regular, $H = \operatorname{Spec}\mathscr{O}_X/(f)$ una hipersuperficie, e $Y = \operatorname{Spec}\mathscr{O}_X/\mathfrak{p} = \operatorname{Spec}\mathscr{O}_H/\bar{\mathfrak{p}}$ una subvariedad regular. Denotemos por $\tilde{H}$ y $\tilde{X}$ las explosiones de H y X a lo largo de Y. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \tilde{H} & \longrightarrow & \tilde{X} \\ \downarrow & & \downarrow \\ H & \longrightarrow & X \end{array}$$

Escribamos $\mathfrak{p} = (t_1, \ldots, t_{n-r})$. Entonces $\mathscr{O}_{\tilde{X}}$ viene dado afínmente por los anillos

$$\mathscr{O}_X[\frac{t_1}{t}, \ldots, \frac{t_{n-r}}{t}]$$

con $t = t_1, \ldots, t_{n-r}$.

1. Proposición: *Se cumple que $\mathscr{O}_{\tilde{H}} = \mathscr{O}_{\tilde{X}}/(f/t^m)$ donde m es la multiplicidad de H en el punto genérico de Y.*

Demostración. $G_{\mathfrak{p}}\mathscr{O}_X$ es un anillo íntegro, luego $0 \neq f \in \mathfrak{p}^m/\mathfrak{p}^{m+1}$ es no divisor de cero, y por 4.2.5, $(f) \cap \mathfrak{p}^n = f \cdot \mathfrak{p}^{n-m}$. Por tanto, la sucesión de anillos de Rees

$$0 \to D_{\mathfrak{p}}\mathscr{O}_X \xrightarrow{\cdot f} D_{\mathfrak{p}}\mathscr{O}_X \to D_{\bar{\mathfrak{p}}}\mathscr{O}_H \to 0$$

es exacta. Localizando por t, también es exacta la sucesión

$$0 \to (D_{\mathfrak{p}}\mathscr{O}_X)_t \xrightarrow{\frac{f}{t^m}} (D_{\mathfrak{p}}\mathscr{O}_X)_t \to (D_{\bar{\mathfrak{p}}}\mathscr{O}_H)_t \to 0$$

y tomando las componentes de grado cero, tenemos $\mathscr{O}_{\tilde{H}} = \mathscr{O}_{\tilde{X}}/(f/t^m)$. □

2. Definición: Diremos que una subvariedad cerrada Y de H es un centro permisible de explosión si es una subvariedad regular y normalmente plana en H.

Sea X una variedad regular, $y \in X$ un punto cerrado. Si $x_1,\dots,x_n$ es un sistema de parámetros regulares de X en y, entonces $\mathrm{Der}_k(\mathscr{O}_X,\mathscr{O}_X) = \mathscr{O}_X \frac{\partial}{\partial x_1} \oplus \dots \oplus \mathscr{O}_X \frac{\partial}{\partial x_n}$ en un entorno de y. Del mismo modo que vimos para curvas planas, si $H = (f)_0$ es una hipersuperficie de multiplicidad m en un punto p y D es un operador diferencial de orden 1 de $\mathscr{O}_X$, entonces $D(f)$ tiene multiplicidad mayor o igual que $m-1$ en p. Además, si p es un punto cerrado, existe D tal que $D(f)$ tiene multiplicidad $m-1$ en p.

3. Lema fundamental: *Sea $D\colon \mathscr{O}_X \to \mathscr{O}_X$ un operador diferencial de orden 1. Sea f de multiplicidad m en el punto genérico de Y. Entonces existe un operador diferencial $\tilde{D}\colon \mathscr{O}_{\tilde{X}} \to \mathscr{O}_{\tilde{X}}$ tal que*

$$\frac{Df}{t^{m-1}} = \tilde{D}\left(\frac{f}{t^m}\right)$$

Demostración. Es análoga al lema fundamental 5.9.10 para curvas planas. □

4. Proposición: *Sea $\pi\colon \widetilde{H} \to H$ la explosión en un centro permisible Y. Sea $\bar{y} \in \pi^{-1}(Y)$ un punto cerrado e $y = \pi(\bar{y})$. Entonces,*

$$m_{\bar{y}}(\widetilde{H}) \leq m_y(H)$$

Demostración. Localmente $H = (f)_0$. Vamos a proceder por inducción sobre $m = m_y(H)$. Si $m = 1$, H es regular y por 8.2.7 $\widetilde{H}$ es regular, luego de multiplicidad 1. Supongamos $m > 1$. Consideremos una derivación D de modo que $m_y(Df) = m-1$. Sea H' la subvariedad de X definida por los ceros de Df.

Veamos que Y (localmente) es normalmente plana en H': Sea $g \in Y$ el punto genérico. Sabemos que $m_g(H') \geq m-1$ (porque $m_g(H) = m$) y $m_y(H') = m-1$, luego $m_g(H') = m-1$. En un entorno de y, Y es equimúltiple o normalmente plana.

Explotemos a lo largo de Y. $\widetilde{H'}$ viene definida por los ceros de Df/t^{m-1}, que tiene multiplicidad menor o igual que $m-1$ en $\bar{y}$, por hipótesis de inducción. Por el lema fundamental, existe $\tilde{D}$ tal que $\tilde{D}(\frac{f}{t^m}) = \frac{Df}{t^{m-1}}$. Por tanto, $\frac{f}{t^m}$ tiene a lo más multiplicidad m en $\bar{y}$, que es lo que queríamos demostrar. □

5. Notación: Denotaremos $\mathrm{Sing}_m(H)$ el conjunto de puntos de H de multiplicidad m.

6. Teorema: *Sea X una variedad regular de dimensión 3 y $S \subset X$ una superficie. Sea m la máxima de las multiplicidades de los puntos cerrados de S. Existe una sucesión finita $\bar{S} \to \therefore \to S$ de explosiones en centros permisibles de modo que $\pi(\mathrm{Sing}_m(\bar{S}))$ es un número finito de puntos cerrados.*

Demostración. Si hay un número finito de puntos singulares de multiplicidad m acabamos. El problema lo tenemos cuando aparecen curvas de puntos singulares de multiplicidad m. Explotando en puntos cerrados podemos desingularizar esas curvas. Las fibras excepcionales se epiyectan por los morfismos de explosión en puntos cerrados, por tanto no afectan a la demostración del teorema.

Una vez desingularizadas, las curvas incluidas en el locus singular de multiplicidad m son centros permisibles. Explotemos a lo largo de esas curvas regulares. Al localizar en el punto genérico de las curvas, S es de dimensión 1, luego después de un número finito de explosiones la multiplicidad baja. Es decir, después de un número finito de explosiones a lo largo de las curvas regulares, la multiplicidad en los puntos genéricos baja. Por tanto solo queda un número finito de puntos con multiplicidad m (si no consideramos las fibras excepcionales antes mencionadas).

□

7. Teorema de existencia de hipersuperficies de contacto maximal: *Sea x un punto cerrado de multiplicidad m de una hipersuperficie $H \subset X$. Existe un entorno U de x (en X) y una hipersuperficie regular $W \subset U$ tal que todos los puntos singulares de multiplicidad m de H en U están en W, i.e.,* $\mathrm{Sing}_m(H \cap U) \subseteq W$*, y la inclusión se mantiene después de cualquier sucesión de explosiones en centros permisibles incluidos en el locus singular de multiplicidad m.*

Demostración. Como en el caso de curvas planas, la idea de la demostración es que tomando una derivación D que baje la multiplicidad en 1, el locus de multiplicidad m de la hipersuperficie $(f)_0$ coincide con el locus de multiplicidad $m-1$ de $(Df)_0$, y sigue coincidiendo por sucesivas explosiones, luego la existencia de la hipersuperficie de contacto maximal se concluye por inducción sobre la multiplicidad. Procedamos ahora con precisión.

Por inducción sobre m. Si $m = 1$, entonces H es regular y $W = H$.

Supongamos que $m > 1$. Sea $U \subset X$ un entorno de x donde H viene definido por los ceros de una función f. Como en la proposición anterior, sea D tal que $m_x(Df) = m-1$ y $H' = (Df)_0$. Reduciendo U si es necesario, podemos suponer por semicontinuidad que $m-1$ es la máxima multiplicidad de H'. Entonces $\mathrm{Sing}_m(H \cap U) \subseteq \mathrm{Sing}_{m-1}(H')$. Podemos suponer que $X = U$.

Si explotamos en un centro permisible se sigue teniendo la inclusión

$$\mathrm{Sing}_m(\widetilde{H}) \subseteq \mathrm{Sing}_{m-1}(\widetilde{H'})$$

En efecto: Por 8.3.1, $\widetilde{H}$ viene definida por los ceros de f/t^m. Si $\widetilde{H}$ tiene multiplicidad m en un punto cerrado y de la fibra excepcional, entonces $\bar{D}(f/t^m)$ tiene multiplicidad mayor o igual que $m-1$ en y. Por la proposición anterior, $\widetilde{H'} = (Df/t^{m-1})_0 = (\bar{D}(f/t^m))_0$

tiene multiplicidad menor o igual que $m-1$ en y. En conclusión, $\widetilde{H'}$ tiene multiplicidad $m-1$ en y y hemos terminado.

Repitiendo el argumento, la inclusión sigue manteniéndose por sucesivas explosiones en centros permisibles.

Sea ahora W una hipersuperficie regular de contacto maximal para H', que existe por hipótesis de inducción. Ahora bien, $\mathrm{Sing}_m(H) \subseteq \mathrm{Sing}_{m-1}(H') \subseteq W$, y las inclusiones se mantienen por sucesivas explosiones. Por tanto, W es la hipersuperficie buscada.

□

8. Observación: Este resultado puede refinarse: existe una subvariedad de contacto maximal y cuya dimensión es la del tangente estricto (que más adelante definiremos).

Usando los mismos argumentos que para un único punto, es fácil construir una hipersuperficie de contacto maximal en un entorno de esos puntos. Falta solo algún detalle técnico. Por ejemplo, hemos utilizado que la localización en un punto del módulo de derivaciones de la variedad regular es libre. Pues bien, es igualmente cierto que localmente en un número finito de puntos es libre, como vemos a continuación.

9. Proposición: *Sea M un A-módulo finito generado localmente libre de rango constante n, y sean $x_1,\dots,x_r \in \mathrm{Spec}A$ un número finito de puntos cerrados. Denotemos por S el sistema multiplicativo de las funciones que no se anulan en ningún x_i. Entonces A_S es un anillo semilocal de espectro maximal $\{x_1,\dots,x_n\}$ y M_S es un A_S-módulo libre.*

Demostración. Probemos solo que M_S es un A_S-módulo libre. Sea $I = \mathfrak{m}_{x_1} \cap \cdots \cap \mathfrak{m}_{x_r}$. Consideremos el epimorfismo

$$M \to M/I = M/\mathfrak{m}_{x_1}M \times \cdots \times M/\mathfrak{m}_{x_r}M$$

Sean $m_1,\dots,m_n$ elementos de M cuyas imágenes en cada factor $M/\mathfrak{m}_{x_i}M$ sea una base (y por tanto sus imágenes en M_{x_i} son base). Sea $L = A^n$ y $L \to M$ el morfismo que manda la base a $m_1,\dots,m_n$. Localizando en S, el morfismo $L_S \to M_S$ es un isomorfismo porque lo es al localizar en cada x_i, pues transforma bases en bases. □

Conclusión: Si $\pi(\mathrm{Sing}_m(\bar{S})) = p_1,\dots,p_r \in S$ son los puntos cerrados del teorema 8.3.6, en un entorno de $p_1,\dots,p_n$ podremos construir una hipersuperficie de contacto maximal. Las sucesivas explosiones de esta hipersuperficie nos define una hipersuperficie de contacto maximal en un entorno de $\mathrm{Sing}_m(\bar{S})$.

La desingularización de S es una cuestión local. Si nos restringimos a un entorno, aún cuando explotemos por curvas que son regulares en este entorno pero no fuera de él, mediante transformaciones cuadráticas (fuera del entorno) podremos suponer que estas curvas son regulares en toda la superficie.

8.4. Exponente idealístico

Una vez que hemos demostrado la existencia de superficies de contacto maximal de una superficie, le asociaremos a la superficie de contacto maximal el exponente idealístico, de modo que el locus singular de éste, coincida con el locus singular de la superficie. Así para demostrar que la superficie desingulariza después de un número finito de explosiones lo haremos demostrando que el locus singular del exponente idealístico es vacío después de un número finito de explosiones.

1. Definición: Sea W una variedad regular. Un exponente idealístico sobre W es una pareja (I,r), siendo I un ideal de $\mathcal{O}_W$ y $r>0$.

2. Definición: Llamaremos locus singular del exponente idealístico, y lo denotaremos $\mathrm{Sing}(I,r)$, a

$$\mathrm{Sing}_W(I,r) := \{x \in W : I_x \subseteq \mathfrak{m}_x^r\}$$

3. Definición: Diremos que una explosión $\widetilde{W} \to W$ es permisible si el centro de explosión es liso (regular) y está contenido en el locus singular de I.

Denotemos por Y el centro de explosión y $\mathfrak{p}_Y$ el ideal de Y en W. Dado un punto cerrado $y \in Y$, en un entorno de y tenemos que $\mathfrak{m}_y = (t_1,\dots,t_n)$ y $\mathfrak{p}_Y = (t_1,\dots,t_{n-r})$. Entonces los anillos afines de $\widetilde{W}$ son $\mathcal{O}_W[\frac{t_1}{t},\dots,\frac{t_{n-r}}{t}]$ ($t=t_i$, para $1\le i\le n-r$). Diremos que $(\widetilde{I},r)$, definido localmente por $\widetilde{I} = \frac{I\cdot\mathcal{O}_{\widetilde{W}}}{t^r}$, es el transformado propio de (I,r).[2]

Sea X una variedad regular de dimensión 3 y $S\subset X$ una superficie. Sea m la máxima de las multiplicidades de los puntos de S. Dado un punto cerrado $s\in S$, consideremos un entorno lo suficientemente pequeño de s en el que esté definido el contacto maximal. En X podemos decir que la superficie S son los ceros de una función f (todo localmente). Podemos suponer que $\mathfrak{m}_{X,s} = (x,y,z)$ y que la superficie W de contacto maximal son los ceros de z. Como $\Omega_{X/k} =< dx,dy,dz >$ (localmente), existe una derivación D $(=\frac{\partial}{\partial z})$ tal que $Dz=1$. Nos bastará con que $Dz = 1 \mod z$.

Queremos encontrar un exponente idealístico (I,r) tal que $\mathrm{Sing}_m(S) = \mathrm{Sing}_W(I,r)$. Vamos a ver que basta tomar como I el ideal formado por f y sus sucesivas derivadas respecto a D, todas ellas elevadas a un exponente conveniente para que sean equimúltiples y la igualdad $\mathrm{Sing}_m(S) = \mathrm{Sing}_W(I,r)$ se conserve al explotar permisiblemente.

4. Proposición: *$p\in \mathrm{Sing}_m(S)$ si y solo si $p\in W$ y $m_p((D^i f)_{|W}) \ge m-i$, para todo i.*

Demostración. Consideremos el desarrollo de Taylor $f = \sum_i g_i(x,y)z^i$, en el completado en p. El punto p es una singularidad de multiplicidad m de S si y solo si $m_p(g_i(x,y)) \ge$

[2] Si se conoce la teoría de divisores y haces de línea, estamos diciendo que $\widetilde{I} = I\cdot\mathcal{O}_{\widetilde{W}} \otimes_{\mathcal{O}_{\widetilde{W}}} \mathcal{L}_{rE}$, donde E es la fibra excepcional del morfismo de explosión.

$m-i$ para todo i. Veamos que $m_p(g_i(x,y)) \geq m-i$ para todo $i \iff m_p((D^i f)_{|W}) \geq m-i$ para todo i. El directo es obvio. Veamos el recíproco. Observemos que $m_p(g_0(x,y)) = m_p((D^0 f)_{|W}) \geq m$. Por hipótesis de inducción supongamos que $m_p(g_i(x,y)) \geq m-i$ para todo $i < r$. $D^r(f)_{|W} = [r!(Dz)^r \cdot g_r + D^r(g_0 + \cdots + g_{r-1}z^{r-1})]_{|W}$. Por tanto, si $m_p(D^r(f)_{|W}) \geq m-r$ se ha de cumplir que $m_p(g_r) \geq m-r$ y hemos concluido.

□

5. Corolario: *Sigamos con las notaciones anteriores y definamos*

$$I = (f^{\frac{r}{m}}, (Df)^{\frac{r}{m-1}}, \ldots, (D^{m-1}f)^r)_{|W}$$

con $r = m!$. *Entonces,*

$$\mathrm{Sing}_m(S) = \mathrm{Sing}_W(I,r)$$

Veamos que al explotar permisiblemente la situación se conserva. Explotemos en un centro permisible de S de multiplicidad m. Este centro permisible también es centro permisible para el exponente idealístico (I,r). Siguiendo las notaciones de la proposición 8.3.1 tendremos que

1. La explosión de S, $\widetilde{S}$, viene definida por los ceros de la función $\tilde{f} = \frac{f}{t^m}$.
2. La explosión de W, $\widetilde{W}$, viene definida por los ceros de la función $\tilde{z} = \frac{z}{t}$.
3. La transformada propia de I en $\widetilde{W}$, $\widetilde{I}$, es $\widetilde{I} = (\ldots, \frac{(D^i f)^{\frac{r}{m-i}}}{t^r}, \ldots)$.

Sustituyendo t por un cierto $t' = t + hz$, podemos suponer que $Dt \in (z^n)$, con $n >> 0$ dado. En efecto, supongamos que $Dt \in (z^m)$; entonces $Dt = g \cdot z^m$. Si tomamos $t' = t - \frac{g}{m+1}z^{m+1}$, entonces $Dt' \in (z^{m+1})$. Recurrentemente concluiremos.

Ahora ya, consideremos $\tilde{D} := tD$. Tenemos que $\tilde{D}\tilde{z} = tD(\frac{z}{t}) = Dz - \frac{z}{t}Dt = 1 \mod \tilde{z}$.

Por otro lado, para $i < n$, $\tilde{D}^i(\frac{a}{t^m}) = \tilde{D}^{i-1}(\frac{Da}{t^{m-1}} + z^{\cdot n}) = \tilde{D}^{i-1}(\frac{Da}{t^{m-1}}) \mod z = \cdots = \frac{D^i a}{t^{m-i}} \mod z$. Por tanto, $(\tilde{D}^i \tilde{f})^{\frac{r}{m-i}} = (\frac{D^i f}{t^{m-i}})^{\frac{r}{m-i}} \mod z$. Luego, $\widetilde{I} = (\tilde{f}^{\frac{r}{m}}, (\tilde{D}\tilde{f})^{\frac{r}{m-1}}, \ldots, (\tilde{D}^{m-1}\tilde{f})^{\frac{r}{1}})_{|\widetilde{W}}$ y

$$\mathrm{Sing}_m(\widetilde{S}) = \mathrm{Sing}_{\widetilde{W}}(\widetilde{I},r)$$

Conclusión: el problema de desingularizar superficies se reduce a probar que por medio de transformaciones permisibles desaparece el locus singular del exponente idealístico.

6. Proposición: *Sea I un ideal sobre una superficie regular W. Existe un número finito de transformaciones cuadráticas $W_i \to W_{i-1} \to \cdots \to W_0 = W$ de modo que $I \cdot \mathcal{O}_{W_i}$ es un ideal localmente principal.*

Demostración. La cuestión es local en W. Sea $I=(f_1,\dots,f_s)$. Es fácil reducir la demostración de la proposición al caso $I=(f,g)$. Sean

$$(f)_0 = C_1 \cup C_2 \cdots \cup C_r$$
$$(g)_0 = C'_1 \cup C'_2 \cdots \cup C'_s$$

con C_i, C'_j curvas irreducibles. Si $\mathfrak{p}_{C_i} = \mathfrak{p}_{C'_j}$ para algún índice y son localmente principales, entonces $I = \mathfrak{p}_{C_i} \cdot I'$, para cierto ideal I', y basta demostrar el teorema para I'. Mediante transformaciones cuadráticas podemos suponer que las curvas $\{C_i, C'_j\}_{i,j}$, son regulares, se cortan transversalmente y que por un punto a lo más pasan solo dos curvas (obsérvese que por transformaciones cuadráticas aparecen los ciclos excepcionales).

Dado un punto p, si f se anula en p y g no, entonces $I_p = (f)_p$ y terminamos. Supongamos pues, que tanto f como g se anulan en p. Recordemos que los anillos locales regulares son dominios de factorización única. Consideremos parámetros locales en p, de modo que

$$\begin{cases} f = x^a \cdot \text{inv.} \\ g = y^b \cdot \text{inv.} \end{cases}$$

Si explotamos en el punto p, tenemos que $I \cdot k[x, y/x] = (x^a, (y/x)^b x^b)$. De nuevo, aparece un factor común, y quitándolo se concluye por inducción sobre $a+b$.

□

7. Teorema : *Dado un exponente idealístico (I,r) sobre una superficie lisa W, existe una sucesión finita de explosiones permisibles (para el exponente idealístico) $W_i \to W_{i-1} \to \cdots \to W_0 = W$, de modo que la i-ésima transformada propia de (I,r) tiene locus singular vacío.*

Demostración. Después de un número finito de transformaciones cuadráticas podemos suponer que el exponente idealístico es principal. Por tanto, $I=(g)$ localmente. Entonces $(I)_0 = C_1 \cup \cdots \cup C_k$, unión de curvas irreducibles. Explotando podemos suponer que las curvas C_i son regulares, transversales y por un punto pasan a lo más dos curvas. Veamos que explotando a lo largo de estas curvas o por transformaciones cuadráticas demostramos el teorema.

Sea $p \in \text{Sing}_w(I,r)$ un punto cerrado. Podemos tomar parámetros en un entorno de p de modo que $g = x^a y^b \cdot$inv.

1. Se puede conseguir que $a, b < r$: En efecto, supongamos $a \geq r$. Entonces la curva $(x)_0$ está contenida en $\text{Sing}_W(I,r)$. Por tanto, $(x)_0$ es un centro permisible para

explotar. Si explotamos en $(x)_0$ la superficie de contacto maximal explotada es isomorfa a la que teníamos, pues estamos explotando por un ideal principal. Sin embargo, el exponente idealístico cambia, pues es $\tilde{g} = \frac{x^a y^b}{x^r} = x^{a-r} y^b$. Recurrentemente concluiremos.

2. Sea pues $g = x^a y^b$ con $a, b < r$. Explotemos en el punto p. Tomando x como parámetro de explosión: $\tilde{g} = \frac{g}{x^r} = x^{a+b-r}(\frac{y}{x})^b$, con lo que la situación ha mejorado, pues $a+b-r < a$. Recurrentemente obtendremos que $a = b = 0$ y el locus singular es vacío.

□

Con todo, hemos demostrado el siguiente teorema.

8. Teorema : *Sea S un superficie en un ambiente regular de dimensión 3, sobre un cuerpo algebraicamente cerrado de característica cero. Después de un número finito de explosiones en centros regulares de S, podemos desingularizar a S.*

9. Ejemplo : Paraguas de Whitney, $S = (y^2 - x^2 z)_0$.

Las singularidades son los puntos donde se anula $d(y^2 - x^2 z) = 2y dy - 2xz dx - x^2 dz$. Es decir, la recta $x = y = 0$. Se verifica que $\frac{\partial^2 f}{\partial^2 y} = 2$, luego no hay puntos de multiplicidad 3.

Una superficie de contacto maximal es $W = (\frac{\partial f}{\partial y})_0 = (y)_0$.

Exponente idealístico: Tomemos $D = \frac{\partial}{\partial y}$, pues $Dy = 1$. Entonces el exponente idealístico es (I, r), con $I = ((y^2 - x^2 z)^{\frac{2}{2}}, (2y)^2)_{|W} = (x^2 z)$ y $r = 2$. El locus singular del exponente idealístico son los puntos donde $x^2 z$ tiene multiplicidad 2, que son los puntos $x = 0$ (de W).

Explotemos en la recta $x = 0$. La transformada propia del exponente idealístico es $I_1 = (\frac{x^2 z}{x^2}) = (z)$. Ahora el locus singular de $(I_1, 2)$ es vacío. Por tanto, explotando por el ideal (x, y) desingularizamos la superficie. La superficie desingularizada viene dada por los ceros de $(\frac{y}{x})^2 - z$ (en el otro abierto afín son los ceros de $1 - (\frac{x}{y})^2 z y$).

8.5. Tangente estricto

Sea $H = \mathrm{Spec} \mathcal{O}_X/(f)$ una hipersuperficie de una variedad regular. Consideremos el cono tangente en un punto x, $C_{H,x} = \mathrm{Spec} G_{\mathfrak{m}_x} \mathcal{O}_H = \mathrm{Spec}\, k[x_1, \ldots, x_n]/(\mathrm{in}_{\mathfrak{m}_x} f)$, que es una hipersuperficie de $\mathbb{A}^n = C_{X,x}$.

Denotamos m = multiplicidad de $C_{H,x}$ en el vértice, que coincide con la multiplicidad de H en x. Se verifica que m es la máxima de las multiplicidades del cono: en

efecto, dos puntos y, y' de la misma generatriz tienen la misma multiplicidad (se pasa de un punto a otro por una homotecia), luego por semicontinuidad $m \geq m_y = m_{y'}$.

1. Definición: Llamaremos "tangente estricto" de H en el punto x, y lo denotaremos $\mathscr{T}_x H$, a

$$\mathscr{T}_x H = \mathrm{Sing}_m(C_{H,x}) = \{\text{Puntos del cono con la misma multiplicidad que el vértice}\}$$

Si $y \in \mathrm{Sing}_m(C_{H,x})$, todos los puntos de la generatriz que pasa por y tienen multiplicidad m, luego la generatriz es equimúltiple. Por tanto, la generatriz es normalmente plana y $C_{H,x}$ es el producto del cono normal a la generatriz en el vértice por el cono normal a $C_{H,x}$ a lo largo de la generatriz en el vértice, es decir,

$$C_{H,x} = \mathbb{A}^1 \times C'$$

Ahora bien, como la multiplicidad es multiplicativa, $\mathrm{Sing}_m(C_{H,x}) = \mathbb{A}^1 \times \mathrm{Sing}_m(C')$. Procediendo de igual modo con C' tendremos por recurrencia

$$\mathrm{Sing}_m(C_{H,x}) = \mathbb{A}^1 \times \mathrm{Sing}_m(C') = \cdots = \mathbb{A}^r \times \{\text{vért.}\} = \mathbb{A}^r$$

Hemos demostrado por tanto que el tangente estricto es una subvariedad lineal y que $C_{H,x} = \mathbb{A}^r \times \tilde{C}$, donde el único punto de multiplicidad m de $\tilde{C}$ es el vértice.

Tenemos $C_{H,x} = \mathbb{A}^r \times \tilde{C} \hookrightarrow C_{X,x} = \mathbb{A}^n = \mathbb{A}^r \times \mathbb{A}^{n-r}$. Si trasladamos por un vector del tangente estricto el cono queda estable y recíprocamente si al trasladar por un vector el cono queda estable ese vector (que es el trasladado del vértice) es un punto del tangente estricto, i.e.,

$$\mathscr{T}_x H = \{v \in C_{X,x} : C_{H,x} + v = C_{H,x}\}$$

2. Definición: Denotaremos $\tau := \dim \mathscr{T}_x H$, que es un invariante asociado a la singularidad.

3. Lema: *Sea $\mathscr{O}$ un anillo noetheriano local de ideal maximal $\mathfrak{m}$ y $\bar{\mathscr{O}} = \mathscr{O}/(t)$, con $t \in \mathfrak{m}$. Supongamos que $\dim \bar{\mathscr{O}} = \dim \mathscr{O} - 1$ (por ejemplo si t no es divisor de cero). Entonces la multiplicidad de $\mathscr{O}$ en el punto cerrado es menor o igual que la de $\bar{\mathscr{O}}$.*

Demostración. De la sucesión exacta

$$\mathscr{O}/\mathfrak{m}^n \xrightarrow{t\cdot} \mathscr{O}/\mathfrak{m}^{n+1} \to \bar{\mathscr{O}}/\bar{\mathfrak{m}}^{n+1} \to 0$$

se deduce que $S_{\bar{\mathscr{O}}}(n+1) \geq S_{\mathscr{O}}(n+1) - S_{\mathscr{O}}(n) = \Delta S_{\mathscr{O}}(n)$. Aplicando Δ^{d-1} (con $d = \dim \mathscr{O}$) se concluye. □

4. Proposición: *Sea $\pi\colon \widetilde{H} \to H$ el morfismo de explosión de H en un punto cerrado $x \in H$ y sea $\tilde{x} \in \pi^{-1}(x)$. Si $m_{\tilde{x}}(\widetilde{H}) = m_x(H)$, entonces $\tilde{x}$ pertenece a la proyectivización de $\mathscr{T}_x H$.*

Demostración. Sabemos que $\pi^{-1}(x) = T_x H$, que es la proyectivización del cono normal. Denotemos $E = T_x H$. Localmente $C_{H,x} = \mathbb{A}^1 \times E$. Por tanto, si $[y] = \tilde{x}$, se tiene $m_{\tilde{x}}(E) = m_y(C_{H,x})$. Entonces

$$m_{\tilde{x}}(\widetilde{H}) \leq m_{\tilde{x}}(E) = m_y(C_{H,x}) \leq m_x(C_{H,x}) = m_x(H)$$

donde la primera desigualdad es por el lema anterior y la segunda por semicontinuidad de la multiplicidad. Si $m_{\tilde{x}}(\widetilde{H}) = m_x(H)$, entonces $m_y(C_{H,x}) = m_x(C_{H,x})$ e y pertenece al tangente estricto.

□

5. Ejemplo:

1. $\tau = 0$. Sea $0 = z^2 - x^2 - y^2 +$ monomios de grado mayor. El cono tangente es $z^2 - x^2 - y^2 = 0$, luego el tangente estricto es el origen y si explotamos no puede aparecer ningún punto con multiplicidad 2.

2. $\tau = 1$. Sea $0 = zx +$ monomios de grado mayor. El cono tangente es $zx = 0$, luego el tangente estricto es la recta $z = y = 0$ y si explotamos en el origen a lo sumo aparece un punto de multiplicidad 2, que se corresponde con la recta del tangente estricto.

3. $\tau = 2$. Sea $0 = z^2 +$ monomios de grado mayor. El cono tangente es $z = 0$, luego el tangente estricto es el plano $z = 0$.

Capítulo 9

Bases de Gröbner

El objetivo de este capítulo es dar un cálculo efectivo de diversos objetos definidos en Geometría Algebraica: el cierre de la imagen de un morfismo de variedades algebraicas (o teoría de la eliminación), el cierre proyectivo de una variedad afín, el espacio tangente a una variedad en un punto, deformación plana de una variedad proyectiva a una variedad proyectiva monomial, cálculo del polinomio de Hilbert de una variedad proyectiva, resoluciones de un módulo por libres, extens, tores, etc.

9.1. Órdenes monomiales

1. Notaciones: Denotaremos $R = k[x_1,\dots,x_r]$ y será L un R-módulo libre de base $\{e_1,\dots,e_s\}$. Dado un monomio $x^\alpha \in R$, diremos que $m = x^\alpha \cdot e_j \in L$ es un monomio de L. Dado otro monomio $n = x^\beta \cdot e_k \in L$, diremos que m es divisible por n si $k = j$ y x^α es divisible por x^β, y escribiremos $m/n = x^{\alpha-\beta}$. Un término de L es un monomio multiplicado por un escalar $\lambda \in k$.

2. Definición: Un orden monomial en L es un orden total $>$ en el conjunto de los monomios de L, que cumple que "si $m_1 > m_2$ son dos monomios de L y $x^\alpha \neq 1$ es un monomio de R, entonces $x^\alpha \cdot m_1 > x^\alpha \cdot m_2 > m_2$".

Por abuso de notación, diremos que un término es mayor que otro si así sucede con los monomios asociados.

Demos algunos ejemplos de órdenes monomiales en R.

3. Definición: Diremos que $>_{lex}$ es el orden lexicográfico en R si $x^\alpha >_{lex} x^\beta$ si y solo si $\alpha_i > \beta_i$ para el primer índice i que $\alpha_i \neq \beta_i$.

Diremos que $>_{hlex}$ es el orden lexicográfico homogéneo en R si $x^\alpha >_{hlex} x^\beta$ si y solo si $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ y $\alpha_i > \beta_i$ para el primer índice i que $\alpha_i \neq \beta_i$.

Diremos que $>_{ilex}$ es el orden lexicográfico inverso en R si $x^\alpha >_{ilex} x^\beta$ si y solo si $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ y $\alpha_i < \beta_i$ para el último índice i que $\alpha_i \neq \beta_i$.

Por ejemplo, $x_1x_3^2 >_{hlex} x_2x_3^2$ y $x_1x_3^2 >_{ilex} x_2x_3^2$; $x_1x_2x_3 >_{hlex} x_2^3$ y $x_1x_2x_3 <_{ilex} x_2^3$.

Si L es un R-módulo libre de base $\{e_1,\dots,e_s\}$ y tenemos un orden monomial $>$ en R, podemos definir un orden monomial en L del modo que sigue: $x^\alpha e_i > x^\beta e_j$ si $i < j$ ó $i = j$ y $x^\alpha > x^\beta$.

4. Lema: *Todo orden monomial en L es artiniano (es decir, todo subconjunto de monomios tiene un mínimo).*

Demostración. Sea X un conjunto de monomios de L. El R-submódulo de L generado por X está generado por un número finito de ellos $\{x_1,\dots,x_s\}$, pues L es noetheriano. Dado un monomio $x \in X$, se cumple que $x = \sum_{i=1}^s p_i \cdot x_i$, para ciertos $p_i \in R$. Por tanto, para algún i y algún término t_i de p_i, $x = t_i \cdot x_i$ (salvo un escalar). Es decir, cada monomio de X es múltiplo de algún x_i. Por tanto, el menor de $\{x_1,\dots,x_s\}$ es el mínimo de X. □

Si I es un conjunto ordenado artiniano, toda cadena de desigualdades en I, $i_1 \geq i_2 \geq \cdots \geq i_n \geq \cdots$ estabiliza. Dicho de otro modo, no existen cadenas infinitas de desigualdades estrictas $i_1 > i_2 > \cdots > i_n > \cdots$.

5. Definición: Dado $f \in L$ escribamos $f = \sum_i t_i$ como suma de términos no nulos (del modo obvio). Llamaremos término mayor de f al mayor de todos los términos t_i y lo denotaremos $max_> f$ (o simplemente $max(f)$).

Dado un submódulo $M \subseteq L$, denotaremos $max_> M := \langle max_> f, f \in M\rangle_R \subset L$ (o lo denotaremos simplemente $max(M)$).

6. Ejercicio: Sea $f \in R = k[x_1,\dots,x_r]$ homogénea.

1. Si $max_{>_{hlex}} f \in k[x_s,\dots,x_r]$ para algún s, entonces $f \in k[x_s,\dots,x_r]$.
2. Si $max_{>_{ilex}} f \in (x_s,\dots,x_r)$ para algún s, entonces $f \in (x_s,\dots,x_r)$.

Dado $f \in L$ y $p \in R$, sea n el término de p tal que $n \cdot max(f)$ sea máximo, entonces $max(pf) = n \cdot max(f)$: sea m un término de f y n' otro término de p tenemos que $n' \cdot m \leq n' \cdot max(f) \leq n \cdot max(f)$. En particular, $max(x^\alpha \cdot f) = x^\alpha \cdot max(f)$. Por tanto, $max(M) = \langle max(f), f \in M\rangle_k$.

7. Definición: Sea E un k-espacio vectorial e I un conjunto totalmente ordenado artiniano. Sea para cada $i \in I$, un subespacio vectorial $E_i \subseteq E$, de modo que $E_i \subseteq E_{i'}$, si $i < i'$. Diremos que la cadena de subespacios vectoriales de E, $\{E_i\}_{i\in I}$, es filtrante si $\cup_{i\in I} E_i = E$. Denotaremos $G_iE := E_i/\cup_{j<i} E_j$ y $GE := \oplus_{i\in I} G_iE$ (si $0 \in I$ es el mínimo de I, definimos $G_0E := E_0$).

8. Lema: *Si para cada $i \in I$, $\{e_{ij}\}_j$ son vectores de E_i cuyas clases forman una base de G_iE entonces los vectores $\{e_{ij}\}_{i,j}$ forman una base de E.*

Demostración. Dado $0 \neq e \in E$, sea i mínimo tal que $e \in E_i$. Entonces, $\bar{e} = \sum_j \lambda_{ij}\bar{e}_{ij}$ en G_iE y sea $e' = e - \sum_j \lambda_{ij}e_{ij}$. Si $e' \neq 0$, sea $i' < i$ mínimo tal que $e' \in E_{i'}$. Entonces, $\bar{e}' = \sum_{j'} \lambda'_{i'j'}\bar{e}_{i'j'}$ en $G_{i'}E$ y sea $e'' = e' - \sum_{j'} \lambda_{i'j'}e_{i'j'}$. Por ser I artiniano este proceso termina en un número finito de pasos, con lo que podremos escribir e como combinación lineal de los e_{rs}.

Los vectores $\{e_{ij}\}_{i,j}$ son linealmente independientes: Sea $e = \sum_{ij} \lambda_{ij}e_{ij}$, con algún $\lambda_{i'j'} \neq 0$. Sea i'' maximal cumpliendo que existe j'' tal que $\lambda_{i''j''} \neq 0$. Entonces, $\bar{e} = \sum_j \lambda_{i''j}\bar{e}_{i''j}$ en $G_{i''}E$, y $\bar{e}$ es no nulo porque $\{\bar{e}_{i''j}\}_j$ es la base considerada en $G_{i''}E$. Por tanto, e es no nulo.

□

9. Proposición: *Sean $\{E_i\}_{i\in I}$ y $\{E'_i\}_{i\in I}$ dos cadenas filtrantes de dos espacios vectoriales E, E' y sea $T: E \to E'$ una aplicación lineal tal que $T(E_i) \subseteq E'_i$ para todo $i \in I$. Entonces, T es inyectivo (resp. epiyectivo, isomorfismo) si el morfismo natural inducido $GT: GE \to GE'$ es inyectivo (resp. epiyectivo, isomorfismo).*

Demostración. Si GT es inyectivo entonces T es inyectivo: Dado $0 \neq e \in E$ sea i mínimo tal que $e \in E_i$. Entonces $0 \neq \bar{e} \in G_iE$, luego $0 \neq GT(\bar{e}) = \overline{T(e)}$ y $T(e) \neq 0$.

Si GT es epiyectivo entonces T es epiyectivo: Si T no es epiyectivo, sea i mínimo para el que existe $e' \in E'_i$ de modo que $e' \notin \operatorname{Im} T$. Evidentemente, $0 \neq \bar{e}' \in G_iE'$. Sea $\bar{e} \in G_iE$, tal que $GT(\bar{e}) = \bar{e}'$. Entonces, $\overline{e' - T(e)} = 0 \in G_iE'$, luego existe $j < i$ tal que $e' - T(e) \in E'_j$. Por tanto, por la elección de i, existe $v \in E$ tal que $e' - T(e) = T(v)$. En conclusión, $e' = T(e + v) \in \operatorname{Im} T$ y hemos llegado a contradicción. □

Sea E espacio vectorial con una cadena filtrante $\{E_i\}_{i\in I}$ de subespacios vectoriales. Dado un subespacio vectorial $E' \subseteq E$ tenemos la cadena filtrante de subespacios vectoriales de E', $\{E' \cap E_i\}_{i\in I}$. En el espacio vectorial cociente $\bar{E} = E/E'$ tenemos la cadena filtrante de subespacios vectoriales $\{\bar{E}_i\}_{i\in I}$. Se cumple que la sucesión natural

$$0 \to GE' \to GE \to G\bar{E} \to 0$$

es exacta.

10. Sea I el conjunto de los monomios de L. Consideremos en L la cadena filtrante de subespacios vectoriales

$$\{L_{\leq m} := [k\text{-subesp. vect. de } L \text{ generado por los monomios menores o iguales que } m]\}_{m\in I}.$$

Obviamente, para cada monomio $m \in I$, $G_m L = k \cdot m$ y $GL = L$. Sea $M \subseteq L$ un submódulo y consideremos en M y L/M las cadenas filtrantes inducidas. Dado $f \in M$, tendremos que $f = max(f)+$ términos de grado menor, luego $f \in M_{\leq max(f)} := M \cap L_{\leq max(f)}$ y $\bar{f} = max(f) \in G_{max(f)}M \subseteq G_{max(f)}L = k \cdot max(f)$. Es decir,

$$max(M) = GM \subset GL = L.$$

11. Teorema de Macaulay: *El conjunto de los monomios de L que no pertenecen a $max(M)$ forman una base de L/M.*

Demostración. De la sucesión exacta

$$0 \to max(M) = GM \to GL = L \to G(L/M) \to 0$$

obtenemos que los monomios de L que no pertenecen a $max(M)$ forman una base de $G(L/M)$. Por el lema anterior los monomios de L que no pertenecen a $max(M)$ forman una base de L/M.

□

12. Proposición: *Sean $N \subseteq M \subseteq L$ submódulos. Si $max(N) = max(M)$ entonces $N = M$.*

Demostración. Si $GN = max(N) = max(M) = GM$, entonces $N = M$, por la proposición 9.1.9.

□

9.2. Bases de Gröbner

Supondremos siempre que $R = k[x_1, \ldots, x_r]$ y que $L = \oplus_{i=1}^{s} R \cdot e_i$ es un R-módulo libre con un orden monomial.

1. Definición: Sea $M \subseteq L$ un submódulo. Diremos que un sistema de generadores de M, $\{g_1, \ldots, g_t\}$ es una base de Gröbner de M si $\{max(g_1), \ldots, max(g_t)\}$ es un sistema generador de $max(M)$.

2. Proposición: *Sean $f, f_1, \ldots, f_t \in L$. Entonces, existe una expresión*

$$f = \sum_i p_i \cdot f_i + f', \quad \text{con } p_i \in R, \text{ y } f' \in L$$

de modo que ninguno de los monomios de f' están en $\langle max(f_1), \ldots, max(f_t)\rangle$ y $max(f) \geq max(p_i f_i)$, para todo i. Diremos que f' es un resto de f respecto de $f_1, \ldots, f_t$ y que la expresión $f = \sum_i p_i \cdot f_i + f'$ es una expresión estándar de f respecto de los f_i.

Demostración. Sea m el término mayor de f divisible por algún $max(f_i)$. Sea $f_1' = f-(m/max(f_i))\cdot f_i$, entonces

$$f = (m/max(f_i))\cdot f_i + f_1'$$

$max(f) \geq m = max((m/max(f_i))\cdot f_i)$ y el término mayor de f_1' divisible por algún $max(f_i)$ es menor estricto que m. Por inducción descendente (recuérdese el lema 9.1.4), f_1' cumple la proposición, luego f también.

□

3. Observación: La expresión $f = \sum_i p_i \cdot f_i + f'$ no es única. Si bien se puede seguir un proceso para que siempre obtengamos la misma expresión: En la demostración de la proposición anterior, considérese f_i, con i mínimo tal que $max(f_i)$ divida a m.

4. Criterio de Buchberger: *Sea $M = \langle f_1,\dots,f_t\rangle \subseteq L$ un submódulo. Si $max(f_i)$ y $max(f_j)$ contienen el mismo vector de la base de L, sea $m_{ij} := m.c.d.(max(f_i), max(f_j))$ y $f_{ij} := (max(f_j)/m_{ij})\cdot f_i - (max(f_i)/m_{ij})\cdot f_j$, para $1 \leq i < j \leq t$; si $max(f_i)$ y $max(f_j)$ no contienen el mismo vector de la base de L digamos que $f_{ij} := 0$. Sea*

$$f_{ij} = \sum_k p_k f_k + f_{ij}'$$

una expresión estándar de f_{ij} respecto de $f_1,\dots,f_t$. Entonces, $f_1,\dots,f_t$ forman una base de Gröbner de M si y solo si $f_{ij}' = 0$, para todo $i < j$.

Demostración. Si $f_1,\dots,f_t$ forman una base de Gröbner de M, entonces como $f_{ij}' = f_{ij} - \sum_i p_i f_i \in M$, entonces $max(f_{ij}') \in max(M) = \langle max(f_1),\dots,max(f_t)\rangle$ lo que es contradictorio por definición de expresión estándar, salvo que $max(f_{ij}') = 0$, luego $f_{ij}' = 0$.

Supongamos ahora que los $f_{ij}' = 0$.

Sea R^t el R-módulo libre de base $\{\xi_1,\dots,\xi_t\}$ y consideremos el epimorfismo de R-módulos $\pi: R^t \to M$, $\pi(\xi_i) = f_i$.

Consideremos en R^t el orden monomial $>$ definido por:

$$x^\alpha\cdot\xi_i > x^\beta\cdot\xi_j \text{ si } \begin{cases} max(x^\alpha\cdot f_i) > max(x^\beta\cdot f_j) \\ \text{ó} \\ max(x^\alpha\cdot f_i) = max(x^\beta\cdot f_j) \text{(salvo un escalar) e } i<j \end{cases}$$

Sea J el conjunto de los monomios de R^t.

Consideremos en M la filtración $\{M_{\leq x^\alpha\cdot\xi_i} := \pi((R^t)_{\leq x^\alpha\cdot\xi_i})\}_{x^\alpha\cdot\xi_i\in J}$. Se cumple que

$$G_{x^\alpha\cdot\xi_i}M = \begin{cases} 0, & \text{si existe } x^\beta\xi_j < x^\alpha\cdot\xi_i : x^\beta\cdot max(f_j) = x^\alpha\cdot max(f_i). \\ k\cdot\overline{x^\alpha\cdot f_i} \neq 0, & \text{en otro caso.} \end{cases}$$

En efecto, supongamos que existe $x^\beta \xi_j < x^\alpha \cdot \xi_i$ de modo que $x^\beta \cdot max(f_j) = x^\alpha \cdot max(f_i)$ (tomemos el j mínimo posible, luego $x^\beta \cdot \xi_j$ es el máximo monomio menor que $x^\alpha \cdot \xi_i$). El monomio x^α es divisible por $(max(f_j)/m_{ij})$, digamos de cociente x^γ, y tenemos $x^\alpha \cdot max(f_i) = x^\gamma \cdot (max(f_j)/m_{ij}) \cdot max(f_i) = x^\beta \cdot max(f_j)$. Luego, $x^\alpha \cdot f_i - x^\beta \cdot f_j = x^\gamma \cdot ((max(f_j)/m_{ij}) \cdot f_i - (max(f_i)/m_{ij}) \cdot f_j) = x^\gamma \cdot f_{ij} = x^\gamma \cdot \sum_k p_k f_k$ que pertenece a $M_{\leq x^\beta \cdot \xi_j}$ porque para todo término $x^{\gamma'}$ de p_k no nulo, se cumple que $x^\gamma \cdot x^{\gamma'} \cdot \text{máx}(f_k) \leq x^\gamma \cdot \text{máx}(p_k f_k) \leq x^\gamma \cdot \text{máx}(f_{ij}) < \text{máx}(x^\beta f_j) = x^\beta \,\text{máx}(f_j)$. Por tanto, $x^\alpha \cdot f_i \in M_{\leq x^\beta \cdot \xi_j}$, $M_{\leq x^\alpha \cdot \xi_i} = M_{\leq x^\beta \cdot \xi_j}$ y $G_{x^\alpha \cdot \xi_i} M = 0$. En caso contrario, tenemos un morfismo natural $G_{x^\alpha \cdot \xi_i} M \to G_{x^\alpha \cdot \text{máx}(f_i)} M$, obviamente $G_{x^\alpha \cdot \xi_i} M = k \cdot \overline{x^\alpha \cdot f_i}$ y como el morfismo $G_{x^\alpha \cdot \xi_i} M \to G_{x^\alpha \cdot max(f_i)} M$ aplica $\overline{x^\alpha \cdot f_i}$ en $x^\alpha \cdot max(f_i)$, que es no nulo, concluimos que $\overline{x^\alpha \cdot f_i}$ es no nulo.

Dado $f \in M$, sea $x^\alpha \cdot \xi_i$ el mínimo tal que $f \in M_{\leq x^\alpha \cdot \xi_i}$. Entonces, $0 \neq \bar{f} \in G_{x^\alpha \cdot \xi_i} M$ y $\bar{f} = \lambda \cdot \overline{x^\alpha \cdot f_i}$, para cierto escalar λ no nulo, y su imagen en $G_{x^\alpha \cdot max(f_i)} M$ es $\lambda \cdot x^\alpha \cdot max(f_i)$. En conclusión, $max(M) = \langle max(f_1), \ldots, max(f_t) \rangle$.

□

5. Observación: El criterio de Buchberger nos da un algoritmo para calcular una base de Gröbner. Dado un submódulo $M = \langle f_1, \ldots, f_t \rangle \subset L$ si $f_1, \ldots, f_t$ no forman una base de Gröbner entonces algún $f'_{ij} \neq 0$ (seguimos notaciones del criterio). Sustituyamos $f_1, \ldots, f_t$ por $f_1, \ldots, f_t, f'_{ij}$ y repitamos el proceso. Este proceso acaba en un número finito de pasos pues las inclusiones $\langle max(f_1), \ldots, max(f_t) \rangle \underset{\neq}{\subset} \langle max(f_1), \ldots, max(f_t), max(f'_{ij}) \rangle$ son estrictas.

6. Teorema de Schreyer: *Sea $M = \langle g_1, \ldots, g_t \rangle \subseteq L$ un submódulo generado por una base de Gröbner. Si $max(g_i)$ y $max(g_j)$ contienen el mismo vector de la base de L sea $m_{ij} = m.c.d.(max(g_i), max(g_j))$, $g_{ij} = (max(g_j)/m_{ij}) \cdot g_i - (max(g_i)/m_{ij}) \cdot g_j$, y sea*

$$g_{ij} = \sum_k p_k g_k + g'_{ij}$$

una expresión estándar de g_{ij} respecto de $g_1, \ldots, g_t$. Por el criterio de Buchberger, $g'_{ij} = 0$, para todo i, j.

Sea R^t un módulo libre de base $\xi_1, \ldots, \xi_t$, $\pi \colon R^t \to M$ el epimorfismo de módulos definido por $\pi(\xi_i) = g_i$ y $\phi \colon \Lambda^2 R^t \to R^t$ el morfismo definido por

$$\phi(\xi_i \wedge \xi_j) = \begin{cases} 0, \text{ si } max(g_i) \text{ no contiene el mismo vector de la base de } L \text{ que } max(g_j). \\ (max(g_j)/m_{ij}) \cdot \xi_i - (max(g_i)/m_{ij}) \cdot \xi_j - \sum_k p_k \xi_k, \text{ si } max(g_i) \text{ contiene el} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{mismo vector de la base que } max(g_j). \end{cases}$$

Entonces, la sucesión

$$\Lambda^2 R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$$

es exacta.

Además, si en R^t definimos el orden monomial $>$: $x^\alpha \cdot \xi_i > x^\beta \cdot \xi_j$ si $max(x^\alpha \cdot g_i) > max(x^\beta \cdot g_j)$ o $max(x^\alpha \cdot g_i) = max(x^\beta \cdot g_j)$ (salvo un escalar) y $i < j$, entonces $\phi(\xi_i \wedge \xi_j)$ es una base de Gröbner de $\operatorname{Ker}\pi$.

Demostración. La sucesión $\Lambda^2 R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$ es exacta por la proposición 9.1.9, porque tomando "graduados" es exacta:

Sea J el conjunto de todos los monomios de R^t. Consideremos en M la filtración

$$\{M_{\leq x^\alpha \cdot \xi_i} := \pi((R^t)_{\leq x^\alpha \cdot \xi_i})\}_{x^\alpha \cdot \xi_i \in J}.$$

Como vimos en la demostración del criterio de Buchberger, se cumple que

$$G_{x^\alpha \cdot \xi_i} M = \begin{cases} 0, & \text{si existe } x^\beta \xi_j < x^\alpha \cdot \xi_i \text{ tal que } x^\beta \cdot max(g_j) = x^\alpha \cdot max(g_i). \\ k \cdot \overline{x^\alpha \cdot g_i} \neq 0, & \text{en otro caso.} \end{cases}$$

Definamos

$$(\Lambda^2 R^t)_{x^\alpha \cdot \xi_i} := \bigoplus_{\substack{j>i \\ x^\gamma \cdot max(g_j)/m_{ij} = x^\alpha}} k \cdot x^\gamma \cdot \xi_i \wedge \xi_j$$

Existe x^γ (único) tal que $x^\gamma \cdot max(g_j)/m_{ij} = x^\alpha$ si y solo si $max(g_j)$ divide a $x^\alpha \cdot m_{ij}$, que equivale a que divida a $x^\alpha \cdot max(g_i)$, que equivale a que existe x^β tal que $x^\beta \cdot max(g_j) = x^\alpha \cdot max(g_i)$. Por tanto, $(\Lambda^2 R^t)_{x^\alpha \cdot \xi_i} = 0$ si y solo si no existe $j > i$ tal que $x^\beta \cdot max(g_j) = x^\alpha \cdot max(g_i)$. Consideremos en $\Lambda^2 R^t$ la filtración $\{(\Lambda^2 R^t)_{\leq x^\alpha \cdot \xi_i} := \oplus_{x^\beta \cdot \xi_j \leq x^\alpha \cdot \xi_i} (\Lambda^2 R^t)_{x^\beta \cdot \xi_j}\}$. Por tanto, $G_{x^\alpha \cdot \xi_i} \Lambda^2 R^t = (\Lambda^2 R^t)_{x^\alpha \cdot \xi_i}$. Observemos que $\phi((\Lambda^2 R^t)_{\leq x^\alpha \cdot \xi_i}) \subseteq (R^t)_{\leq x^\alpha \cdot \xi_i}$. Las sucesiones

$$G_{x^\alpha \cdot \xi_i} \Lambda^2 R^t \xrightarrow{G\phi} G_{x^\alpha \cdot \xi_i} R^t \xrightarrow{G\pi} G_{x^\alpha \cdot \xi_i} M \to 0$$

son exactas. Luego, $G\Lambda^2 R^t \to G \operatorname{Ker}\pi$ es epiyectivo. Por la proposición 9.1.9, $\Lambda^2 R^t \to \operatorname{Ker}\pi$ es epiyectivo y concluimos que

$$\Lambda^2 R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$$

es exacta. Por último, como $G\Lambda^2 R^t = \Lambda^2 R^t = \langle \xi_i \wedge \xi_j \rangle$, entonces

$$max(\operatorname{Ker}\pi) = G \operatorname{Ker}\pi = G\phi(\Lambda^2 R^t) = \langle G\phi(\xi_i \wedge \xi_j) \rangle = \langle max(\phi(\xi_i \wedge \xi_j)) \rangle,$$

y $\phi(\xi_i \wedge \xi_j)$ es una base de Gröbner de $\operatorname{Ker}\pi$.

□

7. Observación: Si $M = \langle f_1, \ldots, f_t \rangle \subset L$ no está generado por una base de Gröbner, mediante el algoritmo de Buchberger completemos a una base de Gröbner $M = \langle f_1, \ldots, f_{t'} \rangle$. Consideremos la sucesión exacta $\Lambda^2 R^{t'} \xrightarrow{\phi'} R^{t'} \xrightarrow{\pi'} M \to 0$ del teorema de Schreyer. Escribamos $f_i = \sum_{j=1}^{t} p_{ij} f_j$, para todo $1 \leq i \leq t'$ (podemos decir que $p_{ij} = \delta_{ij}$, para todo $i \leq t$ y todo j). Sea $\varphi\colon R^{t'} \to R^t$ el epimorfismo definido por $\varphi(\xi_i) = \sum_j p_{ij}\xi_j$ y $\pi\colon R^t \to M$, $\pi(\xi_i) = f_i$. Entonces, el diagrama

$$\begin{array}{ccccccc} \Lambda^2 R^{t'} & \xrightarrow{\phi'} & R^{t'} & \xrightarrow{\pi'} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & \nearrow{\scriptstyle \pi} & & & \\ & & R^t & & & & \end{array}$$

es conmutativo y la sucesión

$$\Lambda^2 R^{t'} \xrightarrow{\varphi\circ\phi'} R^t \xrightarrow{\pi} M \to 0$$

es exacta.

En conclusión, dado un morfismo entre módulos libres $R^t \to L$ sabemos calcular el núcleo. Sabemos resolver los sistemas de ecuaciones R-lineales homogéneos.

9.3. Aplicaciones

En las distintas aplicaciones se supondrá que el lector ya conoce diversos conceptos como: extens y tores de módulos (ver sección 7.3), variedad afín, espectro proyectivo (ver sección 3.7), explosión a lo largo de un cerrado (ver sección 5.5), espacio tangente en un punto (ver subsección 4.2.1), etc.

9.3.1. Teoría de la eliminación

Dado un sistema de ecuaciones $p_1(x_1, \ldots, x_r) = 0, \ldots, p_t(x_1, \ldots, x_r) = 0$ queremos eliminar las variables $x_1, \ldots, x_s$. Es decir, queremos calcular qué relaciones algebraicas cumplen

$$\bar{x}_{s+1}, \ldots, \bar{x}_r \in k[x_1, \ldots, x_r]/(p_1, \ldots, p_t)$$

Queremos calcular el núcleo del morfismo $k[x_{s+1}, \ldots, x_r] \to k[x_1, \ldots, x_r]/(p_1, \ldots, p_t)$, que es $k[x_{s+1}, \ldots, x_r] \cap (p_1, \ldots, p_t)$. Geométricamente, queremos calcular el cierre de la imagen del morfismo

$$\operatorname{Spec} k[x_1, \ldots, x_r]/(p_1, \ldots, p_t) \to \mathbb{A}^{r-s} = \operatorname{Spec} k[x_{s+1}, \ldots, x_r], (\alpha_1, \ldots, \alpha_r) \mapsto (\alpha_{s+1}, \ldots, \alpha_r)$$

En general, dados $\bar{q}_1,\dots,\bar{q}_s \in k[x_1,\dots,x_r]/(p_1,\dots,p_t)$ queremos calcular las relaciones algebraicas que cumplen. Observemos que

$$k[x_1,\dots,x_r,y_1,\dots,y_s]/(p_1(x),\dots,p_t(x),y_1-q_1(x),\dots,y_s-q_s(x)) = k[x_1,\dots,x_r]/(p_1,\dots,p_t)$$

y vía esta identificación, $\bar{y}_i = \bar{q}_i$. Luego las relaciones que cumplen los $\bar{q}_i$ son las relaciones que cumplen las $\bar{y}_i$. El caso general coincide con el caso anterior.

Geométricamente, sabremos calcular el cierre de la imagen de un morfismo entre variedades afines

$$\begin{array}{lcl} X = \operatorname{Spec} k[x_1,\dots,x_r]/(p_1,\dots,p_t) & \to & Y = \operatorname{Spec} k[y_1,\dots,y_s]/(p'_1,\dots,p'_{t'}) \\ (\alpha_1,\dots,\alpha_r) & \mapsto & (q_1(\alpha_1,\dots,\alpha_r),\dots,q_s(\alpha_1,\dots,\alpha_r)) \end{array}$$

1. Lema : *Sea $f \in R = k[x_1,\dots,x_r]$. Si $max_{>_{lex}} f \in k[x_s,\dots,x_r]$ para algún s, entonces $f \in k[x_s,\dots,x_r]$.*

2. Proposición : *Consideremos el orden lexicográfico en $k[x_1,\dots,x_r]$ y un ideal $I \subseteq k[x_1,\dots,x_r]$ de base de Gröbner $g_1,\dots,g_t$. Si $g_1,\dots,g_{t'}$ son aquellos g_i en los que no aparecen las variables $x_1,\dots,x_s$, entonces*

$$k[x_{s+1},\dots,x_r] \cap I = (g_1,\dots,g_{t'}), \qquad (\textit{ideal de } k[x_{s+1},\dots,x_r])$$

Demostración. Obviamente, $(g_1,\dots,g_{t'}) \subseteq k[x_{s+1},\dots,x_r] \cap I$.

Dado $f \in k[x_{s+1},\dots,x_r] \cap I$, se tiene que $max(f)$ es un múltiplo de un $max(g_i)$ y en él no aparecen las variables $x_1,\dots,x_s$, luego $max(f) \in \langle max(g_1),\dots,max(g_{t'})\rangle_{k[x_{s+1},\dots,x_r]}$. Por tanto, la inclusión $(g_1,\dots,g_{t'}) \subseteq k[x_{s+1},\dots,x_r] \cap I$ en graduados es epiyectiva, luego es una igualdad. □

Sea $A = k[x_1,\dots,x_r]/(p_1,\dots,p_r)$ e $I = (\xi_1,\dots,\xi_s)$ un ideal de A. Se define el dilatado de A por I, que denotamos $D_I A$, como sigue

$$D_I A := A \oplus I \oplus \cdots \oplus I^n \oplus \cdots = A[\xi_1 \cdot t,\dots,\xi_s \cdot t] \subseteq A[t]$$

Luego, $D_I A = k[\bar{x}_1,\dots,\bar{x}_r,\xi_1 \cdot t,\dots,\xi_s \cdot t] \subset A[t] = k[x_1,\dots,x_r,t]/(p_1,\dots,p_r)$, que sabemos calcular porque sabemos calcular las relaciones que cumplen $\bar{x}_1,\dots,\bar{x}_r,\xi_1 \cdot t,\dots,\xi_s \cdot t$.

Se dice que $\operatorname{Proj} D_I A$ es la explosión de $\operatorname{Spec} A$ a lo largo de $(I)_0$. Se cumple que

$$\operatorname{Proj} D_I A = \cup_i \operatorname{Spec} A[\xi_1/\xi_i,\dots,\xi_s/\xi_i].$$

Sabemos calcular $A[\xi_1/\xi_i,\dots,\xi_s/\xi_i] = k[\bar{x}_1,\dots,\bar{x}_r,\xi_1/\xi_i,\dots,\xi_s/\xi_i] \subseteq A_{\xi_i} = A[y]/(\xi_i \cdot y - 1)$, luego sabemos calcular la explosión de una variedad a lo largo de un cerrado.

9.3.2. Cálculo de la función de Hilbert

Sea $I \subseteq k[x_1,\dots,x_r] = R$ un ideal homogéneo y consideremos el anillo graduado $S = k[x_1,\dots,x_r]/I$. Queremos calcular la función de Hilbert de S:

$$H_S(n) := \dim_k [S]_n = \begin{array}{l}\text{La dimensión del subespacio vectorial de } S \\ \text{generado por las clases de los monomios de grado } n\end{array}$$

3. Proposición: *Consideremos en $k[x_1,\dots,x_r]$ el orden lexicográfico homogéneo. Entonces la función de Hilbert de $S = k[x_1,\dots,x_r]/I$ es igual a la función de Hilbert de $GS = k[x_1,\dots,x_r]/max(I)$.*

Demostración. Denotemos $[S]_{\leq n} = \oplus_{m\leq n}[S]_m$ el subespacio vectorial de S formado por las clases de los polinomios de grado menor o igual que n. Sea I el conjunto de los monomios de $k[x_1,\dots,x_r]$. La filtración $\{S_{\leq x^\alpha} := \overline{k[x_1,\dots,x_r]_{\leq x^\alpha}}\}_{x^\alpha \in I}$ refina a la filtración $\{[S]_{\leq n}\}_{n\in\mathbb{N}}$ (si x^α es el mayor monomio de grado n, entonces $S_{\leq x^\alpha} = [S]_{\leq n}$).

Por tanto,

$$\dim_k [S]_n = \dim_k([S]_{\leq n}/[S]_{\leq n-1}) = \sum_{|x^\alpha|=n} \dim_k G_{x^\alpha} S = \dim_k [GS]_n$$

□

4. Ejemplo: Sea K una extensión de cuerpos de $\mathbb{Q}$ de tipo finito. Dado un polinomio $p(x) \in K[x]$, sabemos descomponerlo en producto de polinomios irreducibles: Supongamos como hipótesis que K es el cuerpo de fracciones de un anillo íntegro $A = \mathbb{Q}[x_1,\dots,x_n]/I$. Reordenando, podemos suponer que $x_1,\dots,x_i$ es un subconjunto másximo de variables de modo que $\mathbb{Q}[x_1,\dots,x_i] \to A$, $x_i \mapsto \bar{x}_i$ es inyectivo. Por tanto, $\mathbb{Q}(x_1,\dots,x_i) \hookrightarrow K$ es un morfismo finito. sabemos descomponer todo polinomio con coeficientes en $\mathbb{Q}(x_1,\dots,x_i)$ en producto de irreducibles, por 0.3.35. Por tanto, argumentando como en 2.3.13, sabemos descomponer todo polinomio con coeficientes en K en producto de irreducibles.

Sea ahora $I = (m_1,\dots,m_t) \subseteq k[x_1,\dots,x_r]$ un ideal generado por monomios. Calculemos, por inducción sobre t, la función de Hilbert de R/I. Sean

$$I' := (m_2,\dots,m_t) \text{ e } I'' := (m_2/m.c.d.(m_2,m_1),\dots,m_t/m.c.d.(m_t,m_1))$$

Es fácil comprobar que la sucesión

$$0 \to R/I'' \xrightarrow{m_1\cdot} R/I' \to R/I \to 0$$

es exacta. Por inducción conocemos la función de Hilbert de R/I' y R/I'', luego la de R/I, pues por la sucesión exacta anterior

$$H_{R/I}(n) = H_{R/I'}(n) - H_{R/I''}(n-d),$$

siendo $d = \mathrm{gr}(m_1)$.

9.3.3. Cierre proyectivo de una variedad afín

Dado $f \in k[x_1,\ldots,x_r]$, diremos que el polinomio homogéneo

$$F = x_0^{\mathrm{gr}\, f} \cdot f(x_1/x_0,\ldots,x_r/x_0) \in k[x_0,\ldots,x_r]$$

es la homogeneización de f por x_0. Evidentemente, $F(1,x_1,\ldots,x_r) = f(x_1,\ldots,x_r)$.

Si $H \in k[x_0,\ldots,x_r]$ es un polinomio homogéneo y $H(1,x_1,\ldots,x_r) = 0$, entonces $H = (x_0-1)\cdot H'$, para cierto polinomio H' y como H es homogéneo es fácil ver que $H = 0$. Por tanto, si F es la homogeneización de $f \in k[x_1,\ldots,x_r]$ por x_0 y F' es un polinomio homogéneo tal que $F'(1,x_1,\ldots,x_r) = f$ (luego $\mathrm{gr}\, F' \geq \mathrm{gr}\, f = \mathrm{gr}\, F$), entonces $F' - x_0^{\mathrm{gr}\, F' - \mathrm{gr}\, F} \cdot F = 0$, es decir, $F' = x_0^{\mathrm{gr}\, F' - \mathrm{gr}\, F} \cdot F$.

Dado un ideal $I \subseteq k[x_1,\ldots,x_r]$ diremos que $J := (F)_{f\in I} \subseteq k[x_0,\ldots,x_r]$, donde F es la homogeneización de f por x_0, es la homogeneización de I por x_0. Dada $X = \mathrm{Spec}\, k[x_1,\ldots,x_r]/I$ se dice que $\mathrm{Proj}\, k[x_0,\ldots,x_r]/J$ es el cierre proyectivo de X.

5. Proposición: *Consideremos en $k[x_1,\ldots,x_r]$ el orden $>_{hlex}$. Sea $I \subseteq k[x_1,\ldots,x_r]$ un ideal y $g_1,\ldots,g_t$ una base de Gröbner de I. Entonces, la homogeneización de I por x_0 es el ideal homogéneo generado por las homogeneizaciones $G_1,\ldots,G_t$ de $g_1,\ldots,g_t$ por x_0.*

Demostración. Sea $x_{r+1} := x_0$ y consideremos el orden lexicográfico homogéneo en $k[x_1,\ldots,x_{r+1}]$. Dado $f \in k[x_1,\ldots,x_r]$ y su homogeneización F por x_{r+1}, es claro que $max(f) = max(F)$. Sea $J = (F)_{f\in I} \subseteq k[x_1,\ldots,x_{r+1}]$. Por tanto,

$$max(J) = (max(I)) = (max(g_1),\ldots,max(g_t)) = (max(G_1),\ldots,max(G_t))$$

Luego la inclusión $(G_1,\ldots,G_t) \subseteq J$ es epiyectiva. □

9.3.4. Deformación plana de una variedad proyectiva a una variedad proyectiva monomial

Consideremos en $k[x_1,\ldots,x_r]$ el orden lexicográfico homogéneo. Sea $I \subseteq k[x_1,\ldots,x_r]$ un ideal homogéneo y $(f_1,\ldots,f_s)$ una base de Gröbner de I. Sea

$$I_0 = max(I) = (max(f_1),\ldots,max(f_s))$$

el ideal "monomial asociado". Sea $C = \operatorname{Proj} k[x_1,\dots,x_{r+1}]/I$ y $C_0 = \operatorname{Proj} k[x_1,\dots,x_{r+1}]/I_0$. El polinomio de Hilbert de C, que es el polinomio de Hilbert de $k[x_1,\dots,x_r]/I$, coincide con el polinomio de Hilbert de C_0, pues es el polinomio de Hilbert de $k[x_1,\dots,x_r]/I_0$.

Sea m_i' el máximo grado con el que aparece la variable x_i en todos los monomios no nulos de todas las f_j, $(1 \le j \le s)$. Sea m' el máximo de todos los m_i'. Definamos $m_i := (r-i+1)\cdot m'^{r-i}$, para $1 \le i \le r$. Es fácil comprobar que

$$f_j(t^{m_1}x_1,\dots,t^{m_r}x_r) = t^{n_j}\cdot max(f_j) + \text{polinomio en } t \text{ de grado menor que } n_j$$

para cierto n_j. Por tanto, $f_j^t := t^{n_j}\cdot f_j(t^{-m_1}x_1,\dots,t^{-m_r}x_r) = max(f_j) + \dot{t} \in k[t][x_1,\dots,x_r]$. Observemos que si hacemos cociente por t, $max(f_j) = \bar{f}_j^t$ y si hacemos cociente por $t-1$, entonces $f_j = \bar{f}_j^t$.

Sea $I_t := (f_j^t)_j \subset k[t][x_1,\dots,x_r]$ y $C_t := \operatorname{Proj} k[t][x_1,\dots,x_r]/I_t$ y consideremos el morfismo natural $\pi\colon C_t \to \operatorname{Spec} k[t] = \mathbb{A}^1$. Observemos que $\pi^{-1}(0) = C_0$ y que $\pi^{-1}(1) = C$. Veamos que $\pi^{-1}(\mathbb{A}^1\setminus\{0\}) = C\times(\mathbb{A}^1\setminus\{0\})$: En efecto, entre los anillos de funciones, el morfismo

$$\begin{array}{rcl} k[t,1/t][x_1,\dots,x_r]/I_t & \to & k[t,1/t]\otimes_k k[x_1,\dots,x_r]/I = k[t,1/t][x_1,\dots,x_r]/(I) \\ x_i & \mapsto & t^{m_i}\cdot x_i \end{array}$$

es un isomorfismo.

Por lo tanto, la fibra por π de todo punto cerrado de $\mathbb{A}^1$ es una variedad proyectiva de polinomio de Hilbert igual al de C. Luego el morfismo π es plano (ver [28]). En conclusión, hemos obtenido el siguiente teorema.

6. Teorema: *El morfismo $\pi\colon C_t \to \mathbb{A}^1$ es una deformación plana de C a C_0.*

9.3.5. Cálculo del espacio tangente en un punto

Dada $f \in k[x_1,\dots,x_r]$, escribamos $f = f_n + f_{n+1} + \cdots + f_m$ como suma de polinomios homogéneos f_i de grado i y cumpliendo $f_n \neq 0$; denotaremos $f_b := f_n$. Sea $I \subseteq k[x_1,\dots,x_r]$ un ideal y denotemos $I_b = (f_b)_{f\in I}$. Dada $X = \operatorname{Spec} k[x_1,\dots,x_r]/I$, se denomina espacio tangente a X en el origen a $T_0X := \operatorname{Spec} k[x_1,\dots,x_r]/I_b$. Calculemos I_b.

7. Proposición: *Sea $I = (f_1,\dots,f_t) \subseteq k[x_1,\dots,x_r]$ un ideal y sea $J = (F_1,\dots,F_t)$ el ideal generado por las homogeneizaciones, F_i, de los f_i por x_0. Consideremos en $k[x_0,x_1,\dots,x_r]$ el orden lexicográfico homogéneo, sea $G_1,\dots,G_{t'}$ una base de Gröbner del ideal J y $g_i := G_i(1,x_1,\dots,x_r)$ la deshomogeneización de G_i por x_0. Entonces,*

$$I_b = ((g_1)_b,\dots,(g_{t'})_b)$$

Demostración. Si en $k[x_0,\dots,x_r]$ hacemos cociente por x_0-1 tendremos que $J=I$.

Consideremos en $k[x_0,\dots,x_r]$ la filtración $\{k[x_0,\dots,x_r]_{\leq(m,n)} := \{$polinomios de grado menor o igual que m, de grado en x_0 menor o igual que $n\}\}_{(m,n)}$ (suponemos $m\geq n$ y el orden lexicográfico en las parejas de números naturales (m,n)). Sea $f\in k[x_1,\dots,x_r]$ un polinomio de grado m, $n=m-\operatorname{gr} f_b$ y F la homogeneización f de por x_0. Entonces, $F=x_0^n f_b(x_1,\dots,x_r)+$ polinomio homogéneo de grado en x_0 menor que n, $F\in k[x_0,\dots,x_r]_{\leq(m,n)}$ y

$$\bar{F}=x_0^n\cdot f_b\in G_{(m,n)}k[x_0,\dots,x_r]=x_0^n\cdot k[x_1,\dots,x_r]_{m-n}$$

Por tanto, si en J consideramos la filtración inducida $\{k[x_0,\dots,x_r]_{\leq(m,n)}\cap J\}$, tenemos que $GJ=(x_0^{n_f}\cdot f_b)_{f\in I}\subset Gk[x_0,\dots,x_r]=k[x_0,\dots,x_r]$ (para ciertos $n_f\in\mathbb{N}$). Si en GJ hacemos $x_0=1$ obtendremos I_b.

Por otra parte, $J=(G_1,\dots,G_{t'})$. Si probamos que $GJ=(\bar{G}_1=x_0^{n_1}\cdot(g_1)_b,\dots,\bar{G}_{t'}=x_0^{n_{t'}}\cdot(g_{t'})_b)$ habremos demostrado la proposición. Tenemos que probar que la inclusión $(\bar{G}_1,\dots,\bar{G}_{t'})\subseteq GJ$ es epiyectiva.

La filtración definida por el orden lexicográfico homogéneo en $k[x_0,\dots,x_r]$ refina la filtración recién definida: $k[x_0,\dots,x_r]_{\leq(m,n)}=k[x_0,\dots,x_r]_{\leq x_0^n\cdot x_1^{m-n}}$. Por tanto, graduar primero por la filtración recién definida y después por la filtración del orden lexicográfico homogéneo (que denotaremos $G_{\leq}$) es igual a graduar por el orden lexicográfico homogéneo. Tenemos que $(max(G_1),\dots,max(G_{t'}))\subseteq G_{\leq}(\bar{G}_1,\dots,\bar{G}_{t'})\subseteq G_{\leq}GJ=G_{\leq}J=(max(G_1),\dots,max(G_{t'}))$. Por tanto, la inclusión $(\bar{G}_1,\dots,\bar{G}_{t'})\subseteq GJ$ al graduar es epiyectiva, luego es epiyectiva.

□

9.3.6. Expresión de un elemento como combinación lineal de los generadores

Sea $M=\langle f_1,\dots,f_t\rangle\subseteq L$ un R-submódulo. Sabemos calcular por el algoritmo de Buchberger una base de Gröbner $g_1,\dots,g_{t'}$ (en términos de los f_i). Dado $f\in L$, por la proposición 9.2.2, sabemos (de modo algorítmico) decidir si $f\in M$ y en este caso escribir $f=\sum_i p_i g_i$. y por tanto sabemos escribir $f=\sum_i p'_i f_i$.

Las clases de los monomios que no a pertenecen $max(M)=\langle max(g_1),\dots,max(g_{t'})\rangle$ forman una base de L/M. Dado $\bar{f}\in L/M$, por la proposición 9.2.2, obtenemos de modo algorítmico, $\bar{f}=\bar{f}'$ de modo que f' es suma de monomios que no pertenecen a $max(M)$. Es decir, sabemos escribir todo $\bar{f}\in L/M$ como combinación k-lineal de los elementos de la base de L/M.

9.3.7. Cálculo del núcleo y de antimágenes de un morfismo entre módulos finito generados

Entenderemos que dar un R-módulo N es dar un sistema de generadores del módulo y dar las relaciones que verifican éstos, es decir, sabemos escribir $N = L/\langle l_i \rangle$ como un módulo libre finito generado (con una base conocida) cociente por un submódulo finito generado (con un sistema generador expresado en términos de la base). Dicho de otro modo entenderemos que dar N es dar una representación del módulo por libres $L_2 \to L_1 \to N \to 0$.

8. Podríamos considerar en vez de R cualquier álgebra de tipo finito. En efecto, si N es un $R' = R/I$-módulo y $L_2 \to L_1 \to N \to 0$ es una presentación de N por R-módulos libres, entonces $L_2 \otimes_R R' \to L_1 \otimes_R R' \to N \to 0$ es una presentación de N por R'-módulos libres (pues tensar es exacto por la derecha). Recíprocamente, sea $R'^m \xrightarrow{\phi'} R'^n \xrightarrow{\pi'} N \to 0$ una presentación de N por R'-módulos libres. Sean $\phi\colon R^m \to R^n$ y $\pi\colon R^n \to N$ morfismos de R-módulos tales que al tensar por $\otimes_R R'$ obtenemos ϕ' y π'. Sea $i\colon R^s \to R$ un morfismo de imagen I. Entonces

$$R^m \oplus (R^s)^n \xrightarrow{\phi + (i \times \overset{n}{\dots} \times i)} R^n \xrightarrow{\pi} N \to 0$$

es una presentación de N por R-módulos libres.

9. Dado un módulo $N = L/\langle l_i \rangle$ y $N' = \langle \overline{l'_j} \rangle \subseteq N$, entonces tenemos dado $N/N' = L/\langle l_i, l'_j \rangle$.

10. Si N es un submódulo de un R-módulo libre finito generado L, para dar N basta dar un sistema generador de N en L, por la observación al teorema de Schreyer 9.2.7. En general, sabemos calcular las relaciones que cumple unos cuantos elementos de un módulo: Sea $L'_2 \xrightarrow{\phi'} L'_1 \xrightarrow{\pi'} N' \to 0$ una presentación por libres de N' y un submódulo $N = \langle n_1, \dots, n_r \rangle \subseteq N'$. Sean $l'_i \in L'_1$ tales que $\pi'(l_i) = n_i$. Sea $M := \pi'^{-1}(N) = \phi'(L'_2) + \langle l'_i \rangle$, entonces $M/\phi'(L'_2) = N$. Como M es un submódulo del libre L'_1 sabemos dar una presentación por libres de M, luego también de N.

11. Consideremos un morfismo de R-módulos $f\colon N \to N'$. Es decir, dado $N = \langle n_i \rangle$ (conocemos las relaciones que cumplen los n_i) y $N' = \langle n'_j \rangle$ (conocemos las relaciones que cumplen los n'_j), tenemos $f(n_i) = \sum_j p_{ij} n'_j$, para ciertos $p_{ij} \in R$.

Dado $f\colon N \to N'$ sabemos calcular (es decir, dar) $\operatorname{Coker} f$. Sabemos calcular $\operatorname{Im} f$, pues es un submódulo de N'.

Dado un morfismo de R-módulos $f\colon N \to N'$ y un submódulo $M \subseteq N'$, sabemos calcular $f^{-1}(M)$ (en particular sabemos calcular $\operatorname{Ker} f$):

Dado un morfismo $F: L_1 \to L_1'$ entre módulos libres finito generados y un submódulo $M \subseteq L_1'$, sabemos calcular $F^{-1}(M)$, como submódulo de L_1. En efecto, sea $\phi': L_2' \to M$ un epimorfismo de un libre L_2' en M. Consideremos el morfismo $H: L_1 \oplus L_2' \to L_1'$, $H(l_1, l_2') := F(l_1) - \phi'(l_2')$. Por el teorema de Schreyer, sabemos calcular $\mathrm{Ker} H$ y si $\pi_1: L_1 \oplus L_2' \to L_1$ es la proyección en el primer factor tenemos que $\pi_1(\mathrm{Ker} H) = F^{-1}(M)$.

Consideremos, ahora, un morfismo $F: L_1 \to L_1'$ que haga conmutativo el diagrama de filas exactas

$$\begin{array}{ccccccc} L_2 & \xrightarrow{\phi} & L_1 & \xrightarrow{\pi} & N & \longrightarrow & 0 \\ & & \downarrow F & & \downarrow f & & \\ L_2' & \xrightarrow{\phi'} & L_1' & \xrightarrow{\pi'} & N' & \longrightarrow & 0 \end{array}$$

Sabemos calcular ${\pi'}^{-1}(M)$. Entonces, $f^{-1}(M) = \pi(\pi^{-1}(f^{-1}(M))) = \pi(F^{-1}({\pi'}^{-1}(M))$ y hemos concluido.

Obviamente, si $f: N \to N'$ es un morfismo de $R' = R/I$-módulos, en particular es un morfismo de R-módulos y dado $M \subseteq N'$ sabemos calcular $f^{-1}(M)$.

Una consecuencia inmediata es que sabemos calcular una resolución de longitud n por R'-módulos libres de todo R'-módulo.

12. Proposición: *Sean $I, I' \subseteq R'$ dos ideales, entonces sabemos calcular $I \cap I'$. Geométricamente, dadas dos subvariedades afines sabemos calcular su unión.*

Demostración. Denotemos $i: I \hookrightarrow R'$ a la inclusión. Entonces, $i^{-1}(I') = I \cap I'$. □

13. Proposición: *Dado un R'-módulo finito generado N y $a \in R'$, sabemos calcular el núcleo del morfismo $N \to N_a$.*

Demostración. El núcleo K del morfismo $N \to N_a$, es igual a $\cup_{n\in\mathbb{N}} \mathrm{Ker} a^n \cdot$ ($a^n \cdot : N \to N$, $n \mapsto a^n n$). Dado i sabemos calcular $\ker a^i \cdot$. Las inclusiones $0 \subseteq \mathrm{Ker} a \cdot \subset \cdots \subset \mathrm{Ker} a^n \cdot \subset \cdots$ estabilizan a partir de un n, justo a partir del primer n tal que $\mathrm{Ker} a^n \cdot = \mathrm{Ker} a^{n+1} \cdot$. Podemos calcular este n y tenemos que $K = \mathrm{Ker} a^n \cdot$.

□

9.3.8. Cálculo de la descomposición primaria de un ideal

14. Lema : *Supongamos por sencillez que k es un cuerpo de característica cero y A una k-álgebra finita. Sabemos calcular el radical de A. Si sabemos descomponer todo polinomio $p(x) \in k[x]$ como producto de polinomios irreducibles entonces sabemos descomponer A en producto directo de k-álgebras finitas locales y sabemos calcular la descomposición primaria del ideal* (0)*.*

Demostración. El radical de $k[x]/(p(x))$ es $(\overline{\frac{p}{m.c.d.(p,p')}})$.

Si sabemos calcular el radical de una k-álgebra finita B, sabemos calcular el radical de B/I, porque $\operatorname{rad}(B/I) = \overline{\operatorname{rad} B}$, pues

$$(B/I)/\overline{\operatorname{rad} B} = B/(\operatorname{rad} B + I) = (B/\operatorname{rad} B)/\bar{I}$$

es reducido (todo cociente de la k-álgebra finita reducida $B/\operatorname{rad} B$ es reducido).

Si sabemos calcular el radical de B y C, sabemos calcular el radical de $B \otimes_k C$: $\operatorname{rad}(B \otimes_k C) = \operatorname{rad} B \otimes C + B \otimes \operatorname{rad} C$, porque

$$(B \otimes C)/(\operatorname{rad} B \otimes C + B \otimes \operatorname{rad} C) = (B/\operatorname{rad} B) \otimes (C/\operatorname{rad} C)$$

es reducido.

Toda k-álgebra finita es cociente de una k-álgebra $k[x_1,\dots,x_n]/(p_1(x_1),\dots,p_n(x_n))$. Por tanto, sabemos calcular el radical de toda k-álgebra finita.

Sea A una k-álgebra finita separable (de dimensión n). Todos los elementos de A son primitivos salvo los que pertenecen a un número (menor que $\binom{n}{2}$)) finito de hiperplanos: si $\bar{k}$ es el cierre algebraico de k, $\operatorname{Hom}_{k-alg}(A,\bar{k}) = \{\phi_1,\dots,\phi_n\}$, entonces si $a \notin \operatorname{Ker}(\phi_i - \phi_j)$ para todo $i \neq j$, entonces a es primitivo. Si $a \in A$ es primitivo, entonces tenemos isomorfismos explícitos $A = k[a] = k[x]/(p(x))$, donde $p(x)$ es el polinomio característico del endomorfismo $a\cdot\colon A \to A$, $b \mapsto ab$. Como sabemos descomponer $p(x)$ en producto de polinomios irreducibles sabemos descomponer A en producto directo de cuerpos.

Por último, sea A una k-álgebra finita. Tenemos $A/\operatorname{rad} A = K_1 \times \cdots \times K_r$. Tenemos que $A = \prod_i A_i$, con $A/\operatorname{rad} A_i = K_i$ y tenemos que calcular los k-álgebras finitas locales A_i. Sea $\pi\colon A \to A/\operatorname{rad} A$ el morfismo de paso al cociente. Sea $c_i \in A$ tal que $\pi(c_i) = (0,\dots,0,\underset{i}{1},1\dots,0)$ (tendremos que $c_i = (c_{ij}) \in \prod_i A_i$, con $c_{ij} \in A_j$ nilpotente si $j \neq i$ y c_{ii} invertible). Sea $n_i > 0$ tal que $\operatorname{Ker} c_i^{n_i}\cdot = \operatorname{Ker} c_i^{n_i+1}\cdot$. Tendremos que $A_i = c_i^{n_i} \cdot A$ y la descomposición primaria del cero es $\cap_i(A_1 \times \cdots \times \underset{i}{0} \times \cdots \times A_n)$.

□

15. Lema : *Sea $I \subseteq k[x_1,\dots,x_n]$ un ideal y $S = k[x_i,\dots,x_n]\backslash\{0\}$ con $i > 1$. Sabemos calcular $I_S \cap k[x_1,\dots,x_n]$.*

Con mayor precisión, consideremos en el anillo $k[x_1,\dots,x_n]$ el orden lexicográfico y sea $\{g_1,\dots,g_s\}$ una base de Gröbner de I. Escribamos $g_i = \sum_{\alpha_i=\cdots=\alpha_n=0} a_\alpha x^\alpha$, con $a_\alpha \in k[x_i,\dots,x_n]$, sea α tal que $\operatorname{máx}(g_i) = \operatorname{máx}(a_\alpha)x^\alpha$ y definamos $a_i = a_\alpha$ y $a = \prod_{i=1}^s a_i$. Entonces, $I_S \cap k[x_1,\dots,x_n] = I_a \cap k[x_1,\dots,x_n]$.

Demostración. Escribamos $A = k[x_i,\dots,x_n]$ y $k[x_1,\dots,x_n] = A[x_1,\dots,x_{i-1}]$. Consideremos la siguiente filtración en $A[x_1,\dots,x_{i-1}]$ de susbespacios vectoriales de índices

$\alpha = (\alpha_1, \cdots, \alpha_{i-1})$, $E_\alpha := \oplus_{\alpha' \leq \alpha} A \cdot x^{\alpha'}$. Denotemos con G' la graduación por esta filtración. Obviamente, $G'_\alpha A[x_1, \ldots, x_{i-1}] = A \cdot x^\alpha$, luego $G'A[x_1, \ldots, x_{i-1}] = A[x_1, \ldots, x_{i-1}]$. Un refinamiento de esta filtración es la filtración dada por el orden lexicográfico de $k[x_1, \ldots, x_n]$: tenemos $E_{\alpha'} \subset E_{(\alpha,\beta)} \subset E_\alpha$ si $\alpha' < \alpha$, y $E_\alpha = \cup_{\beta=(\beta_i,\ldots,\beta_n)} E_{(\alpha,\beta)}$. Por tanto, $G_{(\alpha,\beta)} G'_\alpha k[x_1, \ldots, x_n] = G_{(\alpha,\beta)} k[x_1, \ldots, x_n]$.

Consideremos en I la filtración $I_\alpha := E_\alpha \cap I$. Sea $\tilde{g}_i := \frac{max(g_i)}{\text{máx}(a_i)} \in k[x_1, \ldots, x_{i-1}]$. Veamos que $G'I = (a_1\tilde{g}_1, \ldots, a_s\tilde{g}_s)$: Obviamente $(a_1\tilde{g}_1, \ldots, a_s\tilde{g}_s) \subseteq G'I$. Ahora bien, $GG'I = GI = (\text{máx}(g_1), \ldots, \text{máx}(g_s))$ y por otra parte

$$(\text{máx}(g_1), \ldots, \text{máx}(g_s)) = (\text{máx}(a_1)\tilde{g}_1, \ldots, \text{máx}(a_s)\tilde{g}_s) \subset G(a_1\tilde{g}_1, \ldots, a_s\tilde{g}_s).$$

Por tanto la inclusión $(a_1\tilde{g}_1, \ldots, a_s\tilde{g}_s) \subseteq G'I$ es epiyectiva, es decir, una igualdad.

Por tanto, el conúcleo de la inclusión $G'I_a = (G'I)_a = (\tilde{g}_1, \ldots, \tilde{g}_s) \subset A_a[x_1, \ldots, x_{i-1}]$ es un A_a-módulo libre. Luego, el morfismo $a' \cdot : A_a[x_1, \ldots, x_{i-1}]/I_a \to A_a[x_1, \ldots, x_{i-1}]/I_a$, $\bar{b} \mapsto \overline{a'b}$ es inyectivo para todo $a' \in A$ no nulo, porque en los graduados es inyectivo. Luego, el morfismo $(k[x_1, \ldots, x_n]/I)_a \to (k[x_1, \ldots, x_n]/I)_S$ es inyectivo y

$$\begin{aligned} I_S \cap k[x_1, \ldots, x_n] &= \text{Ker}[k[x_1, \ldots, x_n] \to (k[x_1, \ldots, x_n]/I)_S] \\ &= \text{Ker}[k[x_1, \ldots, x_n] \to (k[x_1, \ldots, x_n]/I)_a] = I_a \cap k[x_1, \ldots, x_n]. \end{aligned}$$

□

La descomposición de un polinomio en producto de polinomios irreducibles es computacionalmente elaborado, pero imprescindible para el cálculo de descomposiciones primarias. Si queremos calcular el radical de un ideal $(p(x)) \subseteq k[x]$, no necesitamos calcular las raíces de $p(x)$, si no que solo tendremos que calcular $m.c.d.(p(x), p'(x))$.

16. Proposición : *Sabemos calcular el radical de todo ideal $I \subset K[x_1, \ldots, x_n]$ con* $\text{car}\, K = 0$.

Demostración. Procedemos por inducción sobre n. Supongamos $n = 1$. Sabemos calcular el máximo común divisor de dos polinomios luego sabemos escribir $I = (p)$. Entonces, $\text{rad}(I) = (\frac{p}{m.c.d.(p,p')})$. Supongamos $n > 1$.

Si $I \cap K[x_i] = (p_i(x_i)) \neq 0$ para todo i, entonces $K[x_1, \ldots, x_n]/I$ es un cociente de $K[x_1, \ldots, x_n]/(p_1(x_1), \ldots, p_n(x_n))$, luego sabemos calcular su radical, luego $\text{rad}\, I$.

Podemos suponer que $I \cap K[x_i] = 0$, para cierto i. Sea $S = K[x_i] \backslash \{0\}$. Por inducción sobre n sabemos calcular $\text{rad}\, I_S$ y sabemos calcular $(\text{rad}\, I_S) \cap K[x_1, \ldots, x_n] =: J$. Si $I = \cap_i \mathfrak{q}_i$ es una descomposición primaria minimal (de primos asociados $\mathfrak{p}_i := \text{rad}(\mathfrak{q}_i)$), entonces $J = \cap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{p}_i$. Reordenando si es necesario, sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ primos minimales de la de la descomposición, disjuntos con S, luego $J = \cap_{i=1}^m \mathfrak{p}_i$. Sea $I' = (I : J^r)$, para

$r >> 0$. Observemos que $I' = \cap_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r \not\subseteq \mathfrak{p}_j} \mathfrak{q}_j$. $I \subsetneq I'$ (si $I' = A$, entonces $\operatorname{rad} I = J$). Por inducción noetheriana sabemos calcular $\operatorname{rad} I'$ y concluimos porque $\operatorname{rad} I = J \cap \operatorname{rad} I'$.

□

17. Teorema: *Sea $I \subset K[x_1,\ldots,x_n]$ un ideal, con $K = \mathbb{Q}(y_1,\ldots,y_m)$. Sabemos calcular una descomposición primaria de I.*

Demostración. Procedemos por inducción sobre n. Supongamos $n = 1$. Podemos suponer $I \neq 0$. Sabemos calcular el máximo común divisor de dos polinomios luego sabemos escribir $I = (p)$. Sabemos factorizar todo polinomio en $K[x_1]$ en producto de irreducibles por 0.3.35, luego sabemos calcular la descomposición primaria de I. Supongamos $n > 1$.

Si $I \cap K[x_i] = (p_i(x_i)) \neq 0$ para todo i, la K-álgebra $K[x_1,\ldots,x_n]/I$ es un cociente de $K[x_1,\ldots,x_n]/(p_1(x_1),\ldots,p_n(x_n))$, luego es una K-álgebra finita, luego sabemos calcular la descomposición primaria del ideal (0) y concluimos.

Podemos suponer que $I \cap K[x_i] = 0$, para cierto i. Sea $S = K[x_i]\backslash\{0\}$. Observemos que $I_S \neq K[x_1,\ldots,x_n]_S$. Sabemos calcular $s \in S$ tal que

$$I_S \cap K[x_1,\ldots,x_n] = I_s \cap K[x_1,\ldots,x_n] =: I'.$$

Por inducción sobre n, sabemos calcular una descomposición primaria de I_S, luego sabemos calcular una descomposición primaria de I'. Si $I = I'$, hemos terminado. Si $I \subsetneq I'$, sea m, tal que $I' = (I : s^m)$. Entonces, $I = I' \cap (I + (s))$. Como $I \subsetneq I + (s)$, por inducción noetheriana sabemos calcular una descomposición primaria de $I + (s)$, luego sabemos calcular una descomposición primaria de I.

□

9.3.9. Cálculo de extens y tores.

Sabemos calcular $\operatorname{Hom}_{R'}(N,N')$: Tomemos $\operatorname{Hom}_{R'}(-,N')$ en la presentación por libres

$$L_2 \xrightarrow{\phi} L_1 \xrightarrow{\pi} N \to 0$$

Obtenemos la sucesión exacta

$$0 \to \operatorname{Hom}_{R'}(N,N') \xrightarrow{\pi^*} \operatorname{Hom}_{R'}(L_1,N') = \oplus^{n_1} N' \xrightarrow{\phi^*} \operatorname{Hom}_{R'}(L_2,N') = \oplus^{n_2} N'$$

(donde n_1 y n_2 son los rangos de los módulos libres L_1 y L_2 respectivamente). Luego, $\operatorname{Hom}_{R'}(N,N') = \operatorname{Ker}\phi^*$, que sabemos calcular. Con mayor generalidad, sabemos

calcular $Ext^n_{R'}(N,N')$, pues sabemos calcular los grupos de homología del complejo $\mathrm{Hom}_{R'}(L^\bullet,N')$, donde $L^\bullet \to N$ es una resolución por libres de N.

Calculemos, ahora, $N \otimes_{R'} N'$: Escribamos $N = L/M$ y $N' = L'/M'$, entonces $N \otimes N' = L \otimes L'/(L \otimes M' + M \otimes L')$. Con mayor generalidad, sabemos calcular $Tor^{R'}_n(N,N')$, pues sabemos calcular los grupos de homología del complejo $L^\bullet \otimes N'$, donde $L^\bullet \to N$ es una resolución por libres de N.

Parte III

Geometría Algebraica Global

Capítulo 10

Haces. Cohomología de haces

Toda la teoría de variedades algebraicas desarrollada hasta aquí padece de una grave deficiencia. No tenemos una noción clara de cuáles son, localmente o no, las funciones algebraicas sobre una variedad algebraica no afín. Así pues, dado un abierto de una variedad algebraica, no sabemos quién es su anillo de funciones algebraicas. Tampoco sabemos cuál es el anillo de funciones algebraicas del espacio proyectivo. Cualquiera que sea la noción de función algebraica que tengamos, ésta debe cumplir que viene determinada localmente, como sucede con las funciones diferenciables en las variedades diferenciales. Es pues necesario introducir el concepto de haz.

10.1. Haces

El concepto de prehaz formaliza la esencia del proceso de restricción de funciones, el de haz la esencia del proceso de reconstrucción de funciones a partir de funciones locales. Procesos que son la substancia y fundamento de la experiencia física.

1. Definición: Sea X un espacio topológico. Un prehaz de conjuntos (resp. grupos, anillos, etc.) sobre X, es una ley que asigna a cada abierto $U \subseteq X$ un conjunto (resp. grupos, anillos, etc.) $P(U)$ de modo que cumple que

1. Si V es un abierto contenido en otro abierto U, se tiene un morfismo de restricción: $\phi_{U,V} : P(U) \to P(V)$. Para cada $s \in P(U)$, denotaremos $s_{|V} = \phi_{U,V}(s)$ y diremos que es la restricción de s a V.

2. Para cada abierto U, $\phi_{U,U} = \mathrm{Id}$.

3. Si $W \subseteq V \subseteq U$ son abiertos, entonces $\phi_{U,W} = \phi_{V,W} \circ \phi_{U,V}$, es decir, $(s_{|V})_{|W} = s_{|W}$.

Dicho de otro modo: Sea $\mathscr{T}_X$ la categoría cuyos objetos son los abiertos de X y cuyos morfismos se definen por

$$\mathrm{Hom}_{\mathscr{T}_X}(U,V) = \begin{cases} \text{La inclusión, si } U \subseteq V \\ \emptyset, \text{ en otro caso} \end{cases}$$

Un prehaz de conjuntos sobre X es un funtor contravariante de $\mathscr{T}_X$ en $\mathscr{C}_{Conj}$.

2. Definición: Los elementos de $P(U)$ se denominan secciones de P en U, y también se denotan por $P(U) = \Gamma(U,P)$.

Análogamente se definen los prehaces de grupos, de grupos abelianos, de anillos, etc, sin más que sustituir la categoría de conjuntos por la categoría de grupos, de grupos abelianos, de anillos, respectivamente. Si A es un prehaz de anillos, llamaremos prehaz de A-módulos a todo prehaz P de grupos abelianos que cumpla:

1. Para cada abierto U, tenemos una aplicación $A(U) \times P(U) \to P(U)$, $(a,s) \mapsto a \cdot s$ que junto con la suma + del grupo abeliano $P(U)$, dota a $P(U)$ de estructura de $A(U)$-módulo.

2. Si $V \subseteq U$, entonces $(a \cdot s)_{|V} = a_{|V} \cdot s_{|V}$, para cualesquiera $a \in A(U)$ y $s \in P(U)$.

3. Ejemplos: 1. Sea G un conjunto (resp. un grupo abeliano, etc). Sea $P(U) = G$ para todo abierto $U \subseteq X$. Si tomamos como morfismos de restricción la identidad, entonces P es un prehaz de conjuntos (resp. de grupos abelianos, etc) en X, que se denomina prehaz constante G y se suele denotar por G.

2. Sea $\mathscr{C}^0(U)$ el anillo de funciones reales y continuas sobre $U \subseteq X$. Si tomamos como morfismos de restricción la restricción ordinaria de funciones, entonces $\mathscr{C}^0$ es un prehaz, que se denomina prehaz de funciones continuas sobre X.

   Análogamente, si X es una variedad diferenciable, se definen los prehaces de funciones diferenciales, de campos diferenciales, formas diferenciales, tensores, etc.

3. Sea $X = \mathbb{R}^2 \setminus \{0\}$, $P(U) = [\text{1-formas exactas en } U]$ y los morfismos de restricción los evidentes. Se dice que P es el prehaz de 1-formas exactas en X.

4. Sea A un anillo y $X = \mathrm{Spec}\, A$. Asociando a cada abierto $U \subseteq X$ el anillo $A_U := \{\frac{a}{s}$, con $a \in A$ y $s \in A$ que no se anula en ningún punto de $U\}$ y tomando como morfismos de restricción los de localización, se obtiene un prehaz de anillos, que se denomina prehaz de localizaciones de A.

5. Si M es un A-módulo, asociando a cada abierto $U \subset \operatorname{Spec} A$ el A_U-módulo $M_U := M \otimes_A A_U$ se obtiene un prehaz, que se denomina prehaz de localizaciones de M.

6. Sea $\pi\colon Y \to X$ una aplicación continua. Para cada abierto U de X, sea $P(U)$ las secciones continuas de π sobre U, es decir, $P(U) = \operatorname{Hom}_X(U, Y)$. Los morfismos de restricción son los definidos por la restricción de aplicaciones. P es un prehaz sobre X, que se denomina prehaz de secciones de π. Este ejemplo es el que motiva los nombres de "secciones" y "morfismos de restricción" que hemos dado para un prehaz cualquiera.

4. Definición: Sea P un prehaz sobre X y $x \in X$. Llamaremos fibra de P en x a

$$P_x := \varinjlim_{x \in U} P(U)$$

Los elementos de P_x se denominan gérmenes de secciones de P en x. Por definición, un germen de sección de P en x es dar una pareja (U, s) formada por un abierto U que contiene a x y una sección s de P en U, donde se identifican dos parejas (U, s) y (U', s') si existe un abierto $W \subset U \cap U'$ que contiene a x tal que $s_{|W} = s'_{|W}$. En pocas palabras, un germen de sección de P en x es dar una sección de P en un entorno abierto arbitrariamente pequeño de x.

Dada una sección s en un abierto U, para cada $x \in U$ denotaremos s_x a la imagen de s en P_x por el morfismo natural $P(U) \to P_x$ y diremos que s_x es el germen de s en x.

5. Proposición: *Sea $X = \operatorname{Spec} A$ y M un A-módulo. Sea P el prehaz de localización de M definido en 10.1.3, 5. Para todo $x \in \operatorname{Spec} A$ se cumple que $P_x = M_x$.*

Demostración. Por definición, $P_x = \varinjlim_{x \in U} M_U$. Como tenemos morfismos naturales de localización $M_U \to M_x$, tenemos un morfismo natural $P_x \to M_x$. Dejamos al lector que compruebe que es un isomorfismo. □

6. Ejercicio: La fibra del prehaz de funciones reales continuas de $\mathbb{R}^n$ en un punto $x \in \mathbb{R}^n$ coincide con $C^0(\mathbb{R}^n)_x$ (donde $\mathfrak{m}_x$ es el ideal maximal de las funciones que se anulan en x).

7. Definición: Un morfismo de prehaces $f\colon P \to P'$ sobre X es un morfismo de funtores, es decir, es dar un morfismo $f_U\colon P(U) \to P'(U)$ (para cada abierto U) que conmuta con los morfismos de restricción. Denotaremos por $\operatorname{Hom}(P, P')$ al conjunto de morfismos de prehaces de P en P'.

Si $f: P \to P'$ es un morfismo de prehaces, induce un morfismo en la fibra de cada punto $f_x: P_x \to P'_x$, de modo que para toda sección s en un abierto U que contiene a x se cumple que $f_x(s_x) = (f_U(s))_x$.

8. Definición: Sea X un espacio topológico. Diremos que un prehaz F sobre X es haz si para todo abierto U y todo recubrimiento abierto $\{U_\alpha\}$ de U la sucesión

$$F(U) \xrightarrow{\delta} \prod_\alpha F(U_\alpha) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F(U_\alpha \cap U_\beta)$$

es exacta, donde $\delta(s) = (s_{|U_\alpha})_\alpha$, $p_1(s_\alpha) = (s_{\alpha|U_\alpha \cap U_\beta})_{\alpha,\beta}$ y $p_2(s_\alpha) = (s_{\beta|U_\alpha \cap U_\beta})_{\alpha,\beta}$. Esto quiere decir que δ es inyectiva y que su imagen son las secciones de $\prod_\alpha F(U_\alpha)$ donde coinciden p_1 y p_2. En otras palabras:

1. Si dos secciones de F sobre U coinciden al restringir a todo U_α, entonces coinciden.

2. Si tenemos una sección s_α en cada abierto U_α que coinciden en las intersecciones ($s_{\alpha|U_\alpha \cap U_\beta} = s_{\beta|U_\alpha \cap U_\beta}$), entonces existe una sección s en U cuya restricción a U_α es s_α para todo α.

Adoptaremos el convenio de que si F es un haz, entonces $F(\emptyset)$ es un conjunto de un elemento.

Los morfismos de haces son por definición los morfismos como prehaces.

9. Ejemplos:

1. Los prehaces del caso 2. del ejemplo 10.1.3 son haces. El del caso 1. es haz cuando el espacio topológico X verifique que la intersección de abiertos no vacíos es no vacía. El prehaz de secciones continuas de una aplicación continua $\pi: Y \to X$ también es un haz, es más, veremos que todo haz es de esta forma.

2. Sea $X = \mathbb{R}^2 \setminus \{0\}$. El prehaz de 1-formas exactas no es haz, pues $d(\arctan y/x)$ es localmente exacta, pero no globalmente, porque su integral a lo largo de la circunferencia unidad es diferente de cero.

10. Proposición: *Dos secciones de un haz en un abierto coinciden si y solo si tienen el mismo germen en todo punto.*

Demostración. La necesidad es obvia. La suficiencia se deduce de que si dos secciones tienen el mismo germen en un punto, entonces coinciden en un entorno del punto. Por la condición 1. de haz se concluye. □

11. Definición: Sea P un prehaz sobre un espacio topológico X. Llamaremos espacio étale de P a $\widetilde{P} = \coprod_{x\in X} P_x$.

Se tiene una proyección natural $\pi\colon \widetilde{P} \to X$, que proyecta P_x en x. Cada sección s de P en un abierto U define una sección $\widetilde{s}$ de π en U, $\widetilde{s}\colon U \to \widetilde{P}$, definida por $\widetilde{s}(x) = s_x$. Dotamos a $\widetilde{P}$ de la siguiente topología: tomamos como base de abiertos los conjuntos $\widetilde{s}(U)$, donde U recorre los abiertos de X y s recorre las secciones de P en U. Es la topología más fina que hace continuas las secciones $\widetilde{s}$.

No es difícil probar que con esta topología $\pi\colon \widetilde{P} \to X$ es continua y es un homeomorfismo local (todo punto de $\widetilde{P}$ tiene un entorno homeomorfo a su imagen por π).

12. Definición: Llamaremos haz asociado al prehaz P, que denotaremos $P^{\#}$, al haz de secciones continuas de la aplicación continua $\pi\colon \widetilde{P} \to X$, es decir,

$$P^{\#} := \mathrm{Hom}_X(-, \widetilde{P})$$

Para cada abierto U se tiene un morfismo $P(U) \to P^{\#}(U)$, $s \mapsto \widetilde{s}$, que define un morfismo de prehaces $P \to P^{\#}$.

Un morfismo de prehaces $P_1 \to P_2$ induce de modo natural una aplicación continua $\widetilde{P}_1 \to \widetilde{P}_2$ que a su vez induce un morfismo de prehaces $P_1^{\#} \to P_2^{\#}$, y se tiene un diagrama conmutativo

$$\begin{array}{ccc} P_1 & \longrightarrow & P_2 \\ \downarrow & & \downarrow \\ P_1^{\#} & \longrightarrow & P_2^{\#} \end{array}$$

13. Proposición: *1. El morfismo $P \to P^{\#}$ es isomorfismo en cada fibra.*

2. P es haz si y solo si $P \to P^{\#}$ es isomorfismo.

3. Para todo haz F se cumple que $\mathrm{Hom}(P,F) = \mathrm{Hom}(P^{\#},F)$.

Demostración. 1. Veamos solo que si θ es una sección de $P^{\#}$ en U y $x \in U$, entonces existe un abierto $V \subset U$ que contiene a x y una sección s de P en V tal que $\theta_{|V} = \widetilde{s}$. Como $\theta(x) \in P_x$ es un germen de sección de P en x, existe $s \in P(V)$ (con $x \in V$) tal que $\theta(x) = s_x$, y puede suponerse $V \subset U$. Como θ y $\widetilde{s}$ coinciden en x, coinciden en un entorno (por ser π un homeomorfismo local) y se concluye.

2. Si $P \to P^{\#}$ es isomorfismo, entonces P es haz porque $P^{\#}$ es haz. Recíprocamente, supongamos que P es haz. Para cada abierto U, el morfismo $P(U) \to P^{\#}(U)$ es inyectivo, pues si $\widetilde{s}_1 = \widetilde{s}_2$, entonces tienen la misma germen en todo punto, luego s_1 y s_2 tienen la misma germen en todo punto (por 1.), luego coinciden por ser P haz. Además es epiyectivo: si θ es una sección de $P^{\#}$ en U, por el apartado anterior existe un

recubrimiento U_α de U y secciones $s_\alpha \in P(U_\alpha)$ tales que $\theta_{|U_\alpha} = \widetilde{s_\alpha}$. Por la inyectividad anterior, se tiene que s_α y s_β coinciden en las intersecciones. Como P es haz, existe una sección $s \in P(U)$ tal que $s_{|U_\alpha} = s_\alpha$ y entonces $\widetilde{s} = \theta$.

3. No es más que considerar el diagrama conmutativo

$$\begin{array}{ccc} P & \longrightarrow & F \\ \downarrow & & \| \\ P^\# & \longrightarrow & F^\# \end{array}$$

□

Todo haz es el haz de secciones continuas de su espacio étale. Por tanto hay una correspondencia biunívoca entre los haces sobre X y los espacios topológicos sobre X localmente isomorfos a X.

14. Observación: Sea $\mathscr{B}$ una base de abiertos de X y sea P un prehaz en X definido solo sobre los abiertos de $\mathscr{B}$. Si para todo $U \in \mathscr{B}$ y y todo recubrimiento $\{U_i \in \mathscr{B}\}_{i\in I}$ de U, existen recubrimientos $\{U_{ijk} \in \mathscr{B}\}$ de $U_i \cap U_j$ de modo que la sucesión

$$P(U) \to \prod_{i\in I} P(U_i) \rightrightarrows \prod_{i,j\in I} P(U_{ijk})$$

es exacta, entonces existe un haz F en X tal que $P \simeq F_{|\mathscr{B}}$. Además, si existe un prehaz G tal que $F_{|\mathscr{B}} \simeq G_{|\mathscr{B}}$, entonces existe un único isomorfismo $F \simeq G^\#$ que restringido a $\mathscr{B}$ da isomorfismos $F_{|\mathscr{B}} \simeq G_{|\mathscr{B}} = G^\#_{|\mathscr{B}}$.

Probémoslo. Sea $P_x := \varinjlim_{x\in U\in\mathscr{B}} P(U)$ y denotemos $s_x := \bar{s} \in P_x$. Sea $\tilde{P} := \coprod_{x\in X} P_x$. Para cada abierto $U \in \mathscr{B}$ y $s \in P(U)$ sea $\tilde{s}(U) = \{s_x, \forall x \in U\}$. Dotamos $\tilde{P}$ de la topología donde una base de abiertos son los conjuntos $\tilde{s}(U)$. Definimos $F := \mathrm{Hom}_X(-, \tilde{P})$. Obviamente, $F_x = P_x$, para todo $x \in X$. El morfismo natural $i\colon P \to F_{|\mathscr{B}}$ es un isomorfismo: Dadas $s, s' \in P(U)$ si son iguales en gérmenes para todo $x \in U$, entonces existe un recubrimiento $\{U_i \in \mathscr{B}\}$ de U en los que las restricciones de s y s' son iguales, como el morfismo $P(U) \to \prod_i P(U_i)$ es inyectivo entonces $s = s'$. Por tanto, el morfismo $P \to F_{|\mathscr{B}}$ es inyectivo. Dada $t \in F(U)$ existe un recubrimiento $\{U_i \in \mathscr{B}\}$ de U y secciones $s_i \in P(U_i)$, de modo que $i(s_i) = t_{|U_i}$. Ahora bien, $s_{i|U_i\cap U_j} = s_{j|U_i\cap U_j}$ porque coinciden en gérmenes, ya que $t_{|U_i}$ y $t_{|U_j}$ coinciden en gérmenes para todo $x \in U_i \cap U_j$. Luego, existe $s \in P(U)$ tal que $s_{|U_i} = s_i$, para todo i. Además, $i(s) = t$ porque son iguales en gérmenes .Por último, observemos que $\tilde{F} \simeq \tilde{G}$, luego $F \simeq G^\#$ y $F_{|\mathscr{B}} \simeq G_{|\mathscr{B}} = G^\#_{|\mathscr{B}}$.

Igualmente, si los abiertos de $\mathscr{B}$ son compactos y para todo $U \in \mathscr{B}$ y todo recubrimiento finito $\{U_1, \ldots, U_n \in \mathscr{B}\}$ de U, existen recubrimientos $\{U_{ijk} \in \mathscr{B}\}$ de $U_i \cap U_j$ de

modo que la sucesión la sucesión

$$P(U) \to \prod_{i=1}^{n} P(U_i) \rightrightarrows \prod_{i,j=1}^{n} P(U_{ijk})$$

es exacta, entonces existe un haz F tal que $P \simeq F_{|\mathscr{B}}$. Además, si existe un prehaz G tal que $F_{|\mathscr{B}} \simeq G_{|\mathscr{B}}$, entonces existe un único isomorfismo $F \simeq G^{\#}$ que restringido a $\mathscr{B}$ da isomorfismos $F_{|\mathscr{B}} \simeq G_{|\mathscr{B}} = G^{\#}_{|\mathscr{B}}$.

15. Proposición: *1. Un morfismo $f : F \to F'$ de haces es un isomorfismo si y solo si $f_x : F_x \to F'_x$ son isomorfismos, para todo $x \in X$.*

2. Un morfismo $f : F \to F'$ de haces de grupos es el morfismo cero si y solo si $f_x = 0$ para todo $x \in X$. En particular, un haz de grupos es cero si y solo si lo es en fibras.

Demostración. 1. Veamos solo la suficiencia. Supongamos pues, que $f_x : F_x \to F'_x$ son isomorfismos para todo $x \in X$. Dados $s, s' \in F(U)$ si $f_U(s) = f_U(s')$, entonces $f_x(s_x) = f_U(s)_x = f_U(s')_x = f_x(s'_x)$. Luego $s_x = s'_x$ para todo x y $s = s'$.

Así pues, los morfismos $f_U : F(U) \to F'(U)$ son inyectivos. Dada una sección $s' \in F'(U)$, por ser los f_x epiyectivos, existirá un recubrimiento $\{U_\alpha\}$ de U y secciones $s_\alpha \in F(U_\alpha)$ de modo que $f_{U_\alpha}(s_\alpha) = s'_{|U_\alpha}$. Además las s_α coinciden sobre las intersecciones por la inyectividad de los morfismos f_{U_α}, luego definen una sección $s \in F(U)$, tal que $s_{|U\alpha} = s_\alpha$. Luego $f_U(s) = s'$, pues localmente sobre los U_α coinciden. Con todo hemos concluido que los f_U son isomorfismos.

2. Es consecuencia de que una sección de un haz en un abierto es nula si y solo si tiene germen nulo en todo punto. □

16. Definición: Sea $f : F \to F'$ un morfismo de haces de grupos. Llamaremos $\operatorname{Ker} f$ al haz definido por $(\operatorname{Ker} f)(U) = \operatorname{Ker} f_U$ (compruébese que es haz). Llamaremos $\operatorname{Im} f$ al haz asociado al prehaz (que no es haz en general) $U \rightsquigarrow \operatorname{Im} f_U$ y $\operatorname{Coker} f$ al haz asociado al prehaz $U \rightsquigarrow \operatorname{Coker} f_U$.

17. Proposición: *Si $f : F \to F'$ es un morfismo de haces de grupos, entonces*

1. $(\operatorname{Ker} f)_x = \operatorname{Ker} f_x$, *para todo* $x \in X$.

2. $(\operatorname{Im} f)_x = \operatorname{Im} f_x$, *para todo* $x \in X$.

Demostración. Por la exactitud del límite inductivo, y teniendo en cuenta que la fibra de un prehaz coincide con la de su haz asociado,

1. $(\operatorname{Ker} f)_x = \varinjlim_{x\in U} \operatorname{Ker} f_U = \operatorname{Ker} f_x$.
2. $(\operatorname{Im} f)_x = \varinjlim_{x\in U} \operatorname{Im} f_U = \operatorname{Im} f_x$.

□

18. Definición: Diremos que una sucesión de morfismos de haces de grupos

$$\cdots \to F_n \xrightarrow{f_n} F_{n+1} \xrightarrow{f_{n+1}} F_{n+2} \to \cdots$$

es exacta, si $\operatorname{Ker} f_{n+1} = \operatorname{Im} f_n$.

19. Corolario: *Una sucesión de morfismos de haces de grupos*

$$\cdots \to F_n \xrightarrow{f_n} F_{n+1} \xrightarrow{f_{n+1}} F_{n+2} \to \cdots$$

es exacta si solo si

$$\cdots \to F_{nx} \xrightarrow{f_{nx}} F_{n+1x} \xrightarrow{f_{n+1x}} F_{n+2x} \to \cdots$$

es una sucesión exacta de grupos para todo $x \in X$.

Demostración. La necesidad es consecuencia de la proposición anterior. En cuanto a la suficiencia, si la sucesión es exacta en fibras, entonces $f_{n+1} \circ f_n = 0$ porque lo es en cada punto. Por tanto, tenemos un morfismo $\operatorname{Im} f_n \to \operatorname{Ker} f_{n+1}$, que es isomorfismo por serlo en fibras. □

20. Ejercicio: Demuestra que $0 \to F' \to F \to F''$ es una sucesión exacta de haces de grupos si y solo si para todo abierto U la sucesión $0 \to F'(U) \to F(U) \to F''(U)$ es exacta.

21. Ejercicio: Sea $X = \mathbb{R}^2 \setminus \{0\}$, C^∞_X el haz de funciones diferenciables sobre X y Ω' el haz de 1-formas cerradas de X. Prueba que el morfismo $d : C^\infty_X \to \Omega'$, $g \mapsto dg$, es un epimorfismo de haces, pero $d : C^\infty(X) \to \Omega'(X)$ no es epiyectiva.

10.1.1. Límites inductivos y proyectivos de haces

22. Definición: Sea I un conjunto de índices y sea $\{F_i\}_{i\in I}$ una familia de haces de grupos abelianos. Llamaremos suma directa de los F_i, y lo denotaremos $\oplus F_i$, al haz asociado al prehaz $U \rightsquigarrow \bigoplus_{i\in I} F_i(U)$. Llamaremos producto directo de los F_i y lo denotaremos $\prod_{i\in I} F_i$ al haz $(\prod_{i\in I} F_i)(U) := \prod_{i\in I} F_i(U)$ (compruébese que es haz).

Se cumple que $(\oplus_i F_i)_x = \oplus_i F_{ix}$. Se tiene un morfismo natural $(\prod_{i\in I} F_i)_x \to \prod_{i\in I} F_{ix}$, que no es isomorfismo en general.

23. Ejercicio: Prueba que

$$\mathrm{Hom}(\oplus_i F_i, G) = \prod_i \mathrm{Hom}(F_i, G) \text{ y } \mathrm{Hom}(G, \prod_i F_i) = \prod_i \mathrm{Hom}(G, F_i).$$

24. Definición: Sea I un conjunto filtrante creciente y sea $\{F_i, \phi_{ij}\}_{i\leq j\in I}$ un sistema de haces y morfismos de haces. Llamaremos límite inductivo de F_i, y lo denotaremos $\varinjlim F_i$, al haz asociado al prehaz $U \rightsquigarrow \varinjlim F_i(U)$. Sea ahora I un conjunto filtrante decreciente. Llamaremos límite proyectivo de F_i y lo denotaremos $\varprojlim F_i$ al haz $(\varprojlim F_i)(U) := \varprojlim F_i(U)$ (compruébese que es haz).

Se cumple que $(\varinjlim F_i)_x = \varinjlim F_{ix}$. Existe un morfismo natural $(\varprojlim F_i)_x \to \varprojlim F_{ix}$, que no es isomorfismo en general.

25. Ejercicio: Prueba las igualdades funtoriales

$$\mathrm{Hom}(\varinjlim F_i, G) = \varprojlim \mathrm{Hom}(F_i, G) \text{ y } \mathrm{Hom}(G, \varprojlim F_i) = \varprojlim \mathrm{Hom}(G, F_i).$$

26. Teorema: *Sea X un espacio topológico con una base de abiertos compactos y tal que la intersección de dos abiertos compactos cualesquiera es compacto. Sea $\{F_i\}$ un sistema inductivo de haces en X. Entonces, para todo abierto compacto U se cumple que*

$$\varinjlim_i F_i(U) = (\varinjlim F_i)(U).$$

Demostración. Para todo recubrimiento finito $\{U_1, \ldots, U_n\}$ de U por abiertos compactos. La sucesión

$$F_i(U) \to \prod_{s=1}^n F_i(U_s) \rightrightarrows \prod_{s,t}^n F_i(U_s \cap U_t)$$

es exacta. Tomando límites inductivos

$$\varinjlim_i (F_i(U)) \to \prod_{s=1}^n \varinjlim_i (F_i(U_s)) \rightrightarrows \prod_{s,t}^n \varinjlim_i (F_i(U_s \cap U_t))$$

es exacta. Luego, las secciones en U del prehaz límite inductivo de los F_i coinciden con las del haz límite inductivo $(\varinjlim F_i)(U)$, por la observación 10.1.14.

□

10.1.2. Haces de $\mathscr{O}$-módulos

Recordemos la definición de prehaz de módulos.

27. Definición: Sea $\mathscr{O}$ un prehaz de anillos sobre un espacio topológico X. Diremos que un prehaz $\mathscr{M}$ es un prehaz de $\mathscr{O}$-módulos si, para cada abierto U de X, $\mathscr{M}(U)$ es un $\mathscr{O}(U)$-módulo de modo compatible con los morfismos de restricción, es decir, $(f \cdot m)_{|V} = f_{|V} \cdot m_{|V}$ para cualesquiera $f \in \mathscr{O}(U)$, $m \in \mathscr{M}(U)$ y $V \subset U$. Esto equivale a decir que se tienen morfismos de prehaces

$$\mathscr{M} \times \mathscr{M} \xrightarrow{+} \mathscr{M}, \qquad \mathscr{O} \times \mathscr{M} \xrightarrow{\cdot} \mathscr{M}$$

satisfaciendo los axiomas de módulo. Es obvio que si $\mathscr{M}$ es un prehaz de $\mathscr{O}$-módulos y $\tilde{\mathscr{M}}$ y $\tilde{\mathscr{O}}$ son los hacificados de $\mathscr{M}$ y $\mathscr{O}$ respectivamente, entonces $\tilde{\mathscr{M}}$ es un $\tilde{\mathscr{O}}$-módulo. Un morfismo de $\mathscr{O}$-módulos $\mathscr{M} \to \mathscr{M}'$ es un morfismo de prehaces tal que es un morfismo de $\mathscr{O}(U)$-módulos en cada abierto U.

28. Ejemplos:

1. Los haces de grupos abelianos son los (haces de) $\mathbb{Z}$-módulos, siendo $\mathbb{Z}$ el haz constante $\mathbb{Z}$.
2. Sea X una variedad diferenciable y C^∞_X el haz de funciones diferenciables sobre X. $Der_X(\mathscr{C}^\infty_X, \mathscr{C}^\infty_X)$ es el haz definido por: $U \rightsquigarrow \mathrm{Der}_{\mathbb{R}}(C^\infty_X(U), C^\infty_X(U))$. Tiene una estructura natural de $\mathscr{C}^\infty_X$-módulo y se denomina $\mathscr{C}^\infty_X$-módulo de campos tangentes. Análogamente se definen los C^∞_X-módulos de r-formas diferenciales, tensores, etc.

29. Definición: Dados dos haces F y G sobre un espacio topológico X, llamaremos haz de homomorfismos de F en G, y lo denotaremos $\underline{\mathrm{Hom}}_X(F,G)$, al haz:

$$\underline{\mathrm{Hom}}_X(F,G)(U) := \mathrm{Hom}_U(F_{|U}, G_{|U}).$$

Análogamente, si $\mathscr{M}$ y $\mathscr{M}'$ son $\mathscr{O}$-módulos, se define el haz homomorfismos de $\mathscr{O}$-módulos de $\mathscr{M}$ en $\mathscr{M}'$, y lo denotaremos $\underline{\mathrm{Hom}}_{\mathscr{O}}(\mathscr{M}, \mathscr{M}')$, como el $\mathscr{O}$-módulo

$$\underline{\mathrm{Hom}}_{\mathscr{O}}(\mathscr{M}, \mathscr{M}')(U) := \mathrm{Hom}_{\mathscr{O}_{|U}}(\mathscr{M}_{|U}, \mathscr{M}'_{|U}).$$

30. Definición: Sean $\mathscr{M}$ y $\mathscr{M}'$ dos $\mathscr{O}$-módulos. Llamaremos producto tensorial de $\mathscr{M}$ y $\mathscr{M}'$, y lo denotaremos $\mathscr{M} \otimes_{\mathscr{O}} \mathscr{M}'$, al haz asociado al prehaz (denominado prehaz producto tensorial)

$$U \rightsquigarrow \mathscr{M}(U) \underset{\mathscr{O}(U)}{\otimes} \mathscr{M}'(U).$$

Es claro que $\mathscr{M} \otimes_{\mathscr{O}} \mathscr{M}'$ es de nuevo un $\mathscr{O}$-módulo.

31. Ejercicio: Sean $\mathcal{M},\mathcal{M}',\mathcal{M}''$ haces de $\mathcal{O}$-módulos. Prueba que

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{M}\otimes_{\mathcal{O}}\mathcal{M}',\mathcal{M}'')=\mathrm{Hom}_{\mathcal{O}}(\mathcal{M},\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M}',\mathcal{M}'')).$$

Si $\{\mathcal{M}_i,\phi_{ij}\}$ es un sistema de $\mathcal{O}$-módulos y morfismos de $\mathcal{O}$-módulos, entonces el haz límite inductivo, $\varinjlim\mathcal{M}_i$, es también un $\mathcal{O}$-módulo. Análogamente, el haz límite proyectivo, $\varprojlim\mathcal{M}_i$, es también un $\mathcal{O}$-módulo.

La suma directa y el producto directo de $\mathcal{O}$-módulos tiene también una estructura natural de $\mathcal{O}$-módulo.

10.2. Imagen directa e inversa de haces

Sea $f: X\to Y$ una aplicación continua de espacios topológicos.

1. Definición: Dado un prehaz P sobre X llamaremos imagen directa de P por f, y lo denotaremos f_*P, al prehaz sobre Y: $(f_*P)(U)=P(f^{-1}(U))$.

Es fácil comprobar que si F es un haz sobre X, entonces f_*F es un haz sobre Y. Cada morfismo de haces sobre X, $h: F\to F'$, induce un morfismo de haces sobre Y, $f_*(h): f_*F\to f_*F'$. Por tanto, la imagen directa es un funtor covariante de la categoría de haces sobre X en la categoría de haces sobre Y. Además es inmediato probar que es exacto por la izquierda y que conmuta con límites proyectivos. Si $X\xrightarrow{f}Y\xrightarrow{g}Z$ son aplicaciones continuas y F es un haz en X, es inmediato que $(g\circ f)_*F=g_*(f_*F)$.

2. Definición: Sea F un haz sobre Y de espacio étale $\tilde{F}$, y sea $f: X\to Y$ una aplicación continua. Denotaremos $f^{-1}F$ al haz sobre X de espacio étale $\tilde{F}\times_Y X$.

Obviamente, $(f^{-1}F)_x=\tilde{F}\times_Y x=F_{f(x)}$. Por tanto, el functor f^{-1} es exacto. Es inmediato comprobar que si se tienen aplicaciones continuas $X\xrightarrow{f}Y\xrightarrow{g}Z$, entonces $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

Dado un abierto $V\subseteq Y$ denotaremos por $V^{\cdot}=\mathrm{Hom}_Y(-,V)$ al haz sobre Y definido por

$$V^{\cdot}(V'):=\begin{cases}\emptyset, \text{ si } V'\not\subseteq V\\ i, \text{ donde } i \text{ es el morfismo de inclusión } V'\subseteq V\end{cases}$$

Observemos que el espacio étale asociado a $V^{\cdot}$ es V.

Se cumple que $\mathrm{Hom}(V^{\cdot},F)=F(V)$. Tenemos un morfismo natural $\coprod_{s\in F(V)}V^{\cdot}\to F$ y un epimorfismo natural $R=\coprod_{V\subseteq X,s\in F(V)}V^{\cdot}\to F$. Igualmente, podemos construir un epimorfismo $R'\to R\times_F R$ y si consideramos las composiciones $R'\to R\times_F R\overset{\pi_1}{\underset{\pi_2}{\rightrightarrows}}R$, tenemos una sucesión exacta

$$R'\rightrightarrows R\to F$$

Dada una sección $V \to \tilde{F}$ tenemos una sección $f^{-1}(V) \to f^{-1}(V) \times_Y \tilde{F} \subseteq X \times_Y \tilde{F}$. Tenemos, pues, un morfismo natural $\phi\colon F \to f_*(f^{-1}F)$.

3. Fórmula de adjunción (de Kan): *Sea $f : X \to Y$ una aplicación continua, G un haz en X y F un haz en Y. Se cumple que el morfismo*

$$\begin{aligned} \mathrm{Hom}_X(f^{-1}F, G) &\to \mathrm{Hom}_Y(F, f_*G) \\ h &\mapsto f_*(h) \circ \phi \end{aligned}$$

es isomorfismo.

Demostración. Si $F = V^{\cdot}$, entonces $f^{-1}V^{\cdot} = (f^{-1}(V))^{\cdot}$ y

$$\mathrm{Hom}_X(f^{-1}V^{\cdot}, G) = \mathrm{Hom}_X((f^{-1}V)^{\cdot}, G) = G(f^{-1}(V)) = \mathrm{Hom}_Y(V^{\cdot}, f_*G).$$

Sea $R' \rightrightarrows R \to F$ una sucesión exacta, con $R = \coprod_i V_i^{\cdot}$ y $R' = \coprod_j V_j{}^{\cdot}$. Entonces la sucesión $f^{-1}R' \rightrightarrows f^{-1}R \to f^{-1}F$ es exacta, y $f^{-1}R = \coprod_i f^{-1}(V_i)^{\cdot}$ y $R' = \coprod_j f^{-1}(V_j)^{\cdot}$. De la sucesión de filas exactas

$$\begin{array}{ccccc} \mathrm{Hom}_X(f^{-1}F, G) & \longrightarrow & \mathrm{Hom}_X(f^{-1}R, G) & \rightrightarrows & \mathrm{Hom}_X(f^{-1}R', G) \\ \downarrow & & \| & & \| \\ \mathrm{Hom}_Y(F, f_*G) & \longrightarrow & \mathrm{Hom}_Y(R, f_*G) & \rightrightarrows & \mathrm{Hom}_Y(R', f_*G) \end{array}$$

se concluye que $\mathrm{Hom}_X(f^{-1}F, G) = \mathrm{Hom}_Y(F, f_*G)$.

□

Observemos que $f^{-1}F = \mathrm{Hom}_X(-, X \times_Y \widetilde{F}) = \mathrm{Hom}_Y(-, \widetilde{F})$.

4. Proposición: *Se cumple que $f^{-1}F$ es el haz asociado al prehaz en X, F', definido por $F'(V) := \varinjlim_{U \supseteq f(V)} F(U)$.*

Demostración. Para cada abierto $U \subseteq X$ que contiene a $f(V)$, tenemos un morfismo natural

$$F(U) \to f^{-1}F(f^{-1}(U)) \to f^{-1}F(V).$$

Por tanto, tenemos un morfismo natural $F' \to f^{-1}F$. Entonces, $f^{-1}F$ coincide con el haz asociado a F' porque en gérmenes coinciden, como puede comprobar el lector. □

5. Ejercicio: Define un morfismo natural $\varphi\colon f^{-1}f_*G \to G$, de modo que vía la fórmula de adjunción $\mathrm{Hom}_Y(f^{-1}f_*G, G) = \mathrm{Hom}_X(f_*G, f_*G)$ se corresponde con el morfismo $\mathrm{Id}\colon f_*G \to f_*G$.

6. Definición: Sea F un haz en X y sea $i\colon S \hookrightarrow X$ un subespacio. Llamaremos restricción de F a S, y lo denotaremos $F_{|S}$, a la imagen inversa $i^{-1}F$.

Si $U \hookrightarrow X$ es un abierto, entonces $F_{|U}$ es el haz definido por $F_{|U}(V) = F(V)$ para cada abierto $V \subset U$, y los morfismos de restricción son los de F.

10.3. Introducción a la cohomología

Comencemos con una justificación muy sucinta, sin detalle ni rigor, de la definición de los grupos de cohomología de un haz.

En la construcción de un poliedro y en su clasificación topológica, es fundamental qué caras pegamos entre sí, a lo largo de ciertas aristas, y qué aristas pegamos entre sí, en ciertos vértices. No es extraño que los grupos de homología, del módulo diferencial de las cadenas del poliedro, sean invariantes topológicos esenciales del poliedro.

Si una superficie X compacta de $\mathbb{R}^3$ la triangulamos, tendremos que es homeomorfa al correspondiente poliedro. Así en la clasificación topológica de la superficie será fundamental la homología del poliedro considerado. Si en vez de tomar los triángulos de la triangulación de la superficie consideramos entornos abiertos "muy aproximados" a cada triángulo, tendremos un recubrimiento $\{U_i\}$ de la superficie, de modo que los abiertos $U_i \cap U_j$ serán entornos muy aproximados a las aristas y los abiertos $U_i \cap U_j \cap U_k$ serán entornos muy aproximados a los vértices. Dado un abierto $U \overset{i}{\hookrightarrow} X$, denotemos $\mathbb{Q}_U$ el haz sobre X definido por $\mathbb{Q}_U(V) = \mathbb{Q}(U \cap V)$, siendo $\mathbb{Q}$ el haz constante $\mathbb{Q}$. Si $U \subset U'$, tenemos un morfismo natural de haces $\mathbb{Q}_U \to \mathbb{Q}_{U'}$ y se tiene una sucesión exacta de haces

$$0 \to \mathbb{Q} \to \prod_i \mathbb{Q}_{U_i} \overset{d_0}{\to} \prod_{i,j} \mathbb{Q}_{U_i \cap U_j} \overset{d_1}{\to} \prod_{i,j,k} \mathbb{Q}_{U_i \cap U_j \cap U_k} \to \dots$$

donde las diferenciales son las sumas alternadas de los morfismos obvios. Es decir, hemos obtenido una resolución $C^\cdot$ del haz constante $\mathbb{Q}$. El complejo $\Gamma(X, C^\cdot)$ es esencialmente el complejo de cadenas del poliedro asociado a la superficie.

Con más generalidad, sea X un espacio topológico, $\{U_i\}$ un recubrimiento por abiertos de X y F un haz en X. Denotemos F_U el haz definido por $F_U(V) = F(U \cap V)$. Se tiene una sucesión exacta de haces

$$0 \to F \to \prod_i F_{U_i} \overset{d_0}{\to} \prod_{i,j} F_{U_i \cap U_j} \overset{d_1}{\to} \prod_{i,j,k} F_{U_i \cap U_j \cap U_k} \overset{d_2}{\to} \dots$$

luego tenemos una resolución $C^\cdot(F)$ del haz F. Los grupos de cohomología del complejo $\Gamma(X, C^\cdot(F))$ se denominan grupos de cohomología de Cech de X con valores en F asociados al recubrimiento $\{U_i\}$.

Sea $R = \coprod_i U_i$ y $\pi\colon R \to X$ el morfismo natural. Se cumple que $C^0(F) = \pi_*\pi^{-1}F$, $C^1(F) = C^0(C^0(F))$ y así sucesivamente. Tomando secciones globales y cohomología en el complejo

$$C^0(F) \to C^0(C^0(F)) \to C^0(C^0(C^0(F))) \to \cdots$$

obtenemos los grupos de cohomología Cech de X con valores en F asociados al recubrimiento $\{U_i\}$.

Si queremos independizarnos del recubrimiento $\{U_i\}$ tendremos que tomar sucesivos refinamientos del recubrimiento $\{U_i\}$, y considerar el límite inductivo de los sucesivos grupos de cohomología Cech obtenidos. Si queremos hacer esto de una sola vez de modo drástico, consideraremos el recubrimiento de X formado por el conjunto discreto de todos sus puntos: Dado un espacio topológico X consideremos la aplicación $\pi\colon \bar{X} \to X$, siendo $\bar{X}$ el conjunto X con la topología la discreta, y π la aplicación identidad. Dado un haz F en X denotemos $R^0F = \pi_*\pi^{-1}F$. Se tiene una sucesión exacta de haces

$$0 \to F \to R^0(F) \to R^0(R^0(F)) \to \dots$$

Tomando secciones globales y cohomología obtendremos los llamados grupos de cohomología de X con valores en F, que se denotaran $H^i(X,F)$. Cuando estos son nulos para $i > 0$ se dice que F es acíclico.

El teorema de De Rham nos dirá que, para el cálculo de los grupos de cohomología de X, podemos sustituir la resolución $R^\cdot(F)$ por cualquier resolución de F por haces acíclicos. Del hecho de que los haces inyectivos son flascos y de que éstos son acíclicos, obtendremos que los grupos de cohomología de un haz F se pueden obtener mediante cualquier resolución de F por haces inyectivos. En términos matemáticos, los grupos de cohomología $H^i(X,F)$ son los funtores derivados del funtor $\Gamma(X,F)$.

10.4. Cohomología de haces

Sea F un haz de grupos abelianos sobre un espacio topológico X. Sea X_{dis} el conjunto X dotado de la topología discreta y sea $\mathrm{Id}\colon X_{\text{dis}} \to X$ la identidad, que es continua. Si denotamos $C^0F = \mathrm{Id}_*\,\mathrm{Id}^{-1}F$, se tiene un morfismo natural $F \to C^0F$. Veamos explícitamente cómo es en cada abierto.

Como X_{dis} tiene la topología discreta, se tiene que $\Gamma(U,C^0F) = \prod_{x\in U} F_x$, para cada abierto U de X, y el morfismo $\Gamma(U,F) \to \Gamma(U,C^0F)$ transforma una sección s en el producto de sus gérmeness $(s_x)_{x\in U}$, que es claramente inyectivo. Definimos F_1 por la sucesión exacta

$$0 \to F \to C^0F \to F_1 \to 0$$

Repetimos el proceso con F_1 y obtenemos

$$0 \to F_1 \to C^0F_1 \to F_2 \to 0$$

y así sucesivamente

$$0 \to F_i \to C^0F_i \to F_{i+1} \to 0$$

Si denotamos $C^iF = C^0F_i$, y consideramos las composiciones $C^0F_i \to F_{i+1} \to C^0F_{i+1}$ obtenemos la sucesión exacta larga

$$0 \to F \to C^0F \to C^1F \to C^2F \to \cdots$$

que se denomina resolución de Godement de F. La resolución propiamente dicha es el complejo de haces $C^{\cdot}F = \bigoplus_{n\geq 0} C^nF$.

1. Proposición : *$F \rightsquigarrow C^{\cdot}F$ es un funtor covariante, aditivo y exacto de la categoría de haces de grupos abelianos sobre X en la categoría de complejos de haces de grupos abelianos sobre X. Para cada abierto U, $F \rightsquigarrow \Gamma(U, C^{\cdot}F)$ es un funtor covariante, aditivo y exacto con valores en la categoría de complejos de grupos abelianos.*

Demostración. Functorialidad: Dado un morfismo de haces $F' \to F$, induce un morfismo en cada fibra $F'_x \to F_x$. Tomando producto directo de las fibras se tiene un morfismo $\Gamma(U, C^0F') \to \Gamma(U, C^0F)$ en cada abierto U, luego un morfismo de haces $C^0F' \to C^0F$ que extiende al morfismo $F' \to F$, luego induce un morfismo $F'_1 \to F_1$. Repitiendo el proceso con $F'_1 \to F_1$, y así sucesivamente, se concluye.

Aditividad: En cada punto x se cumple que $(F \oplus G)_x = F_x \oplus G_x$. Tomando producto directo, se obtiene $\Gamma(U, C^0(F \oplus G)) = \Gamma(U, C^0F) \oplus \Gamma(U, C^0G)$ para cada abierto U y por tanto $C^0(F \oplus G) = C^0F \oplus C^0G$. Este induce una igualdad $(F \oplus G)_1 = F_1 \oplus G_1$, luego reiterando se concluye.

Exactitud: Si $0 \to F' \to F \to F'' \to 0$ es una sucesión exacta de haces, tomando fibra en cada punto y producto directo se obtiene una sucesión exacta

$$0 \to \Gamma(U, C^0F') \to \Gamma(U, C^0F) \to \Gamma(U, C^0F'') \to 0$$

en cada abierto U de X, luego una sucesión exacta

$$0 \to C^0F' \to C^0F \to C^0F'' \to 0$$

que extiende a la de partida y por tanto induce una sucesión exacta

$$0 \to F'_1 \to F_1 \to F''_1 \to 0$$

Reiterando sucesivamente se concluye. □

2. Definición: Llamaremos i-ésimo grupo de cohomología de X con valores en un haz F, y lo denotaremos $H^i(X,F)$, al i-ésimo grupo de cohomología del complejo de grupos abelianos $\Gamma(X,C^{\cdot}F)$, es decir:

$$H^i(X,F) = H^i(\Gamma(X,C^{\cdot}F)).$$

De la proposición anterior se deduce que $F \rightsquigarrow H^i(X,F)$ es un funtor covariante y aditivo de la categoría de haces de grupos abelianos sobre X en la categoría de grupos abelianos.

3. Proposición: $H^0(X,F) = \Gamma(X,F)$.

Demostración. Tomando secciones globales en la sucesión exacta

$$0 \to F \to C^0F \to C^1F$$

se obtiene una sucesión exacta

$$0 \to \Gamma(X,F) \to \Gamma(X,C^0F) \to \Gamma(X,C^1F)$$

y se concluye. □

4. Teorema: *Dada una sucesión exacta* $0 \to F' \to F \to F'' \to 0$ *de haces de grupos abelianos, induce una sucesión exacta larga en cohomología*

$$\begin{aligned} 0 \to H^0(X,F') \to H^0(X,F) \to H^0(X,F'') \to H^1(X,F') \\ \to H^1(X,F) \to H^1(X,F'') \to H^2(X,F') \to \dots \end{aligned}$$

Demostración. Es la sucesión exacta larga de cohomología asociada a la sucesión exacta de complejos de grupos abelianos

$$0 \to \Gamma(X,C^{\cdot}F') \to \Gamma(X,C^{\cdot}F) \to \Gamma(X,C^{\cdot}F'') \to 0$$

□

Veamos ahora que los grupos de cohomología $H^i(X,F)$ son funtoriales en X, en el siguiente sentido.

5. Proposición: *Si* $g\colon X \to Y$ *es una aplicación continua entre espacios topológicos y* F *es un haz sobre* Y*, induce un morfismo de grupos abelianos*

$$H^i(Y,F) \to H^i(X,g^{-1}F)$$

que es funtorial en F*. Este morfismo se denomina imagen inversa y se denota por* g^*.

Demostración. Sea un diagrama conmutativo

$$\begin{array}{ccc} \overline{X} & \xrightarrow{\bar{g}} & \overline{Y} \\ {\scriptstyle \bar{f}}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{g} & Y \end{array}$$

y G un haz en $\overline{Y}$. Tomando f_* en el morfismo natural $G \to \bar{g}_*\bar{g}^{-1}G$ y teniendo en cuenta que $f \circ \bar{g} = g \circ \bar{f}$, obtenemos un morfismo $f_*G \to g_*\bar{f}_*\bar{g}^{-1}G$, luego por adjunción un morfismo

$$g^{-1}f_*G \to \bar{f}_*\bar{g}^{-1}G.$$

En particular, tomando $\overline{X} = X_{\text{dis}}$, $\overline{Y} = Y_{\text{dis}}$, f la identidad en Y, $\bar{f}$ la identidad en X, $\bar{g} = g$ y $G = f^{-1}F$ se obtiene un morfismo

$$g^{-1}C^0F \to C^0(g^{-1}F)$$

y recurrentemente un morfismo $g^{-1}C^\cdot F \to C^\cdot(g^{-1}F)$, que se corresponde por adjunción con un morfismo $C^\cdot F \to g_*C^\cdot(g^{-1}F)$. Explícitamente, es el morfismo

$$C^0F \to g_*C^0g^{-1}F,\ (s_y)_{y\in U} \mapsto (s_{g(x)})_{x\in g^{-1}(U)}.$$

Tomando secciones globales y cohomología obtenemos el morfismo buscado. □

6. Definición: Se dice que un haz F sobre X es flasco cuando para cada pareja de abiertos $V \subseteq U$ el morfismo de restricción $F(U) \to F(V)$ es epiyectivo. Esto equivale a decir que toda sección en un abierto extiende a una sección global.

Es claro que C^0F es un haz flasco para todo haz F, luego C^iF es flasco para todo i.

7. Proposición: *Si* $0 \to F' \xrightarrow{i} F \xrightarrow{p} F'' \to 0$ *es una sucesión exacta de haces sobre* X *y* F' *es flasco, entonces para cada abierto* U *la sucesión*

$$0 \to F'(U) \xrightarrow{i} F(U) \xrightarrow{p} F''(U) \to 0$$

es exacta.

Demostración. Solo hay que ver que p es epiyectiva. Sea $s'' \in F''(U)$. Consideremos la familia formada por las parejas (V,s), donde V es un abierto contenido en U, y s es una sección de F en V cuya imagen por p es $s''_{|V}$. Como para cada $x \in U$, el morfismo $p_x\colon F_x \to F''_x$ es epiyectivo, dicha familia no es vacía. Diremos que $(V,s) \leq (\tilde{V},\tilde{s})$ si $V \subseteq \tilde{V}$ y $\tilde{s}_{|V} = s$. Por el lema de Zorn, existe un elemento (V,s) maximal. Si $V = U$

hemos acabado. Si no fuera así, sea $x \in U \setminus V$. Existe un entorno abierto $W \subseteq U$ de x y una sección $\bar{s} \in F(W)$ de modo que $p(\bar{s}) = s''_{|W}$. Por tanto, $p(s_{|W\cap V}) = p(\bar{s}_{|W\cap V})$ y existe una sección $s'_{W\cap V} \in F'(W \cap V)$ de modo que $i(s'_{W\cap V}) = s_{|W\cap V} - \bar{s}_{|W\cap V}$. Como F' es flasco, existe $s' \in F(W)$ que restringe a $s'_{W\cap V}$. Entonces $\bar{s} + i(s')$ es una sección de F sobre W que se aplica por p en $s''_{|W}$ y que coincide con s sobre $W \cap V$. Por tanto, existe una sección de F sobre $V \cup W$ cuya restricción a V es s y que se aplica por p a $s''_{|V\cup W}$, lo que contradice la maximalidad de (V, s).

□

8. Corolario: *Sea $0 \to F' \to F \to F'' \to 0$ una sucesión de haces. Si F' y F son flascos, entonces F'' es flasco.*

Demostración. Sea $V \subseteq U$ una inclusión de abiertos. Por la proposición anterior, el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F'(U) & \longrightarrow & F(U) & \longrightarrow & F''(U) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle r'} & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r''} & & \\ 0 & \longrightarrow & F'(V) & \longrightarrow & F(V) & \longrightarrow & F''(V) & \longrightarrow & 0 \end{array}$$

tiene filas exactas. Por ser F flasco r es epiyectiva, luego r'' es epiyectiva y F'' es flasco.

□

9. Definición: Se dice que un haz F es acíclico si $H^i(X, F) = 0$ para todo $i > 0$.

10. Teorema: *Los haces flascos son acíclicos.*

Demostración. Si F es flasco, la sucesión $0 \to \Gamma(X, F) \to \Gamma(X, C^0F) \to \Gamma(X, F_1) \to 0$ es exacta. Como F y C^0F son flascos, también lo es F_1 y de nuevo $0 \to \Gamma(X, F_1) \to \Gamma(X, C^0F_1) = \Gamma(X, C^1F) \to \Gamma(X, F_2) \to 0$ es exacta. Reiterando, se sigue que $\Gamma(X, C^\cdot F)$ es una sucesión exacta, luego su cohomología es nula. □

11. Teorema de De Rham: *Sea $R^\cdot$ una resolución de F por haces acíclicos, es decir una sucesión exacta*

$$R^0 \xrightarrow{d_0} R^1 \xrightarrow{d_1} R^2 \xrightarrow{d_2} \dots$$

de modo que cada R^i es acíclico y $\operatorname{Ker} d_0 = F$. Entonces la cohomología de X con valores en F coincide con la cohomología del complejo de secciones globales de $R^\cdot$; es decir:

$$H^i(X, F) = H^i(\Gamma(X, R^\cdot))$$

Demostración. Sea $\Gamma(X, C^{\cdot}R^{\cdot})$ el complejo simple asociado al bicomplejo $\bigoplus_{p,q} \Gamma(X, C^pR^q)$. Los morfismos de haces $C^pF \to C^pR^0$, $R^q \to C^0R^q$ inducen morfismos de complejos

$$\Gamma(X, C^{\cdot}F) \to \Gamma(X, C^{\cdot}R^{\cdot}) \leftarrow \Gamma(X, R^{\cdot})$$

y basta ver para concluir que son quasi-isomorfismos.

El morfismo $\Gamma(X, C^{\cdot}F) \to \Gamma(X, C^{\cdot}R^{\cdot})$ es un quasi-isomorfismo por el teorema 7.2.17, pues la columna i-ésima del bicomplejo es una resolución de $\Gamma(X, C^iF)$ (Proposición 10.4.1).

El morfismo $\Gamma(X, R^{\cdot}) \to \Gamma(X, C^{\cdot}R^{\cdot})$ es un quasi-isomorfismo de nuevo por el teorema 7.2.17, pues la fila i-ésima del bicomplejo es una resolución de $\Gamma(X, R^i)$, por ser R^i acíclico. □

12. Teorema : *Sea X un espacio topológico con una base de abiertos compactos y tal que la intersección de dos abiertos compactos cualesquiera es compacto. Sea $\{F_i\}$ un sistema inductivo de haces de grupos. Entonces, para todo abierto compacto U,*

$$\varinjlim_i H^n(U, F_i) = H^n(U, \varinjlim_i F_i).$$

Demostración. $\varinjlim C^{\cdot}F_i$ es una resolución de $\varinjlim F_i$ por haces flascos. Por el teorema de De Rham,

$$\begin{aligned} H^n(U, \varinjlim F_i) = H^n(\Gamma(U, \varinjlim C^{\cdot}F_i)) &\overset{10.1.26}{=} H^n(\varinjlim \Gamma(U, C^{\cdot}F_i)) = \varinjlim H^n(\Gamma(U, C^{\cdot}F_i)) \\ &= \varinjlim H^n(U, F_i). \end{aligned}$$

□

10.5. Cohomología local

Sea Φ un conjunto de cerrados del espacio topológico X, estable por uniones finitas y tal que si $C \in \Phi$ y $C' \subset C$ entonces $C' \in \Phi$. Dado un haz F de grupos abelianos, denotemos por $\Gamma_\Phi(X, F)$ las secciones de F sobre X con soporte un cerrado de Φ. Igual que $F \rightsquigarrow \Gamma(X, C^{\cdot}F)$, se cumple que $F \rightsquigarrow \Gamma_\Phi(X, C^{\cdot}F)$ es un funtor covariante aditivo, exacto con valores en grupos abelianos. Se define el i-ésimo grupo de cohomología de F con soportes en Φ por

$$H^i_\Phi(X, F) := H^i(\Gamma_\Phi(X, C^{\cdot}F))$$

y se cumple que $H^0_\Phi(X, F) = \Gamma_\Phi(X, F)$.

1. Teorema: *Dada una sucesión exacta* $0 \to F' \to F \to F'' \to 0$ *de haces de grupos abelianos, induce una sucesión exacta larga en cohomología*

$$\begin{aligned} 0 \to H^0_\Phi(X,F') \to H^0_\Phi(X,F) \to H^0_\Phi(X,F'') \to H^1_\Phi(X,F') \\ \to H^1_\Phi(X,F) \to H^1_\Phi(X,F'') \to H^2_\Phi(X,F') \to \dots \end{aligned}$$

2. Definición: Se dice que un haz F es Γ_Φ-acíclico si $H^i_\Phi(X,F) = 0$ para todo $i > 0$.

3. Teorema: *Los haces flascos son* Γ_Φ*-acíclicos.*

4. Teorema de De Rham: *Sea* $R^\cdot$ *una resolución de* F *por haces* Γ_Φ*-acíclicos. Entonces*

$$H^i_\Phi(X,F) = H^i_\Phi(\Gamma(X,R^\cdot)).$$

5. Sucesión exacta larga de cohomología local: *Sea* $Y \hookrightarrow X$ *un cerrado y* $U = X \backslash Y$*. Denotemos también por* Y *el conjunto de cerrados de* X *contenidos en* Y*. Se tiene la sucesión exacta larga*

$$\begin{aligned} 0 \to H^0_Y(X,F) \to H^0(X,F) \to H^0(U,F_{|U}) \to H^1_Y(X,F) \\ \to H^1(X,F) \to H^1(U,F_{|U}) \to H^2_Y(X,F) \to \dots \end{aligned}$$

Demostración. Se deduce de tomar cohomología en la sucesión exacta de complejos

$$0 \to \Gamma_Y(X,C^\cdot F) \to \Gamma(X,C^\cdot F) \to \Gamma(U,C^\cdot F) \to 0$$

□

10.6. Funtores derivados por la derecha

1. Proposición: *La categoría de los* $\mathcal{O}_X$*-módulos tiene suficientes inyectivos, es decir, todo* $\mathcal{O}_X$*-módulo se resuelve de modo funtorial por* $\mathcal{O}_X$*-módulos inyectivos.*

Demostración. Todo A-módulo M, por 0.12.11, está incluido de modo canónico en un A-módulo inyectivo, denotémoslo $I(M)$. Sea F un $\mathcal{O}_X$-módulo e $I(F)$ el haz definido por $I(F)(U) = \prod_{x \in U} I(F_x)$. Se cumple que $\mathrm{Hom}_{\mathcal{O}_X}(G, I(F)) = \prod_{x \in X} \mathrm{Hom}_{\mathcal{O}_{X,x}}(G_x, I(F_x))$, luego $I(F)$ es inyectivo. Además, tenemos una inclusión natural $F \hookrightarrow I(F)$. Sea $H := I(F)/F$ y consideremos $I(H)$, tenemos la sucesión exacta $0 \to F \to I(F) \to I(H)$. Recurrentemente, dado un haz F podemos construir una resolución canónica de F por haces inyectivos, $I^\cdot(F)$.

□

2. Proposición: *Dado un abierto $U \overset{i}{\hookrightarrow} X$ y un haz de $\mathscr{O}_U$-módulos $\mathscr{M}$, sea $i_!\mathscr{M}$ el haz definido por*

$$i_!\mathscr{M}(V) := \{s \in \mathscr{M}(U \cap V) : \operatorname{sop}(s) \text{ es un cerrado de } V\}.$$

Entonces, el morfismo

$$\operatorname{Hom}_{\mathscr{O}_X}(i_!\mathscr{M}, \mathscr{N}) \to \operatorname{Hom}_{\mathscr{O}_U}(\mathscr{M}, \mathscr{N}_{|U}),\ f \mapsto f_{|U}$$

es un isomorfismo, para todo $\mathscr{O}_X$-módulo $\mathscr{N}$.

Demostración. Dado $g \in \operatorname{Hom}_{\mathscr{O}_U}(\mathscr{M}, \mathscr{N}_{|U})$, definamos $G \in \operatorname{Hom}_{\mathscr{O}_X}(i_!\mathscr{M}, \mathscr{N})$ como sigue: Dado $s \in (i_!\mathscr{M})(V) \subset \mathscr{M}(U \cap V)$ sea $t \in \mathscr{M}(V)$ tal que $g(t)_x = 0$ para todo $x \in V - U \cap V$ y $g(t)_{|U \cap V} = g(s)$, entonces $G(s) := t$. Ambas asignaciones son inversas entre sí. □

3. Corolario: *Sea $U \hookrightarrow X$ un abierto e I un $\mathscr{O}_X$-módulo inyectivo. Entonces, $I_{|U}$ es un $\mathscr{O}_U$-módulo inyectivo.*

Demostración. Sea $F_1 \hookrightarrow F_2$ un morfismo de $\mathscr{O}_U$-módulos inyectivos. Entonces, el morfismo de $\mathscr{O}_X$-módulos $i_!F_1 \hookrightarrow i_!F_2$ es inyectivo y

$$\operatorname{Hom}_{\mathscr{O}_U}(F_2, I_{|U}) = \operatorname{Hom}_{\mathscr{O}_X}(i_!F_2, I) \to \operatorname{Hom}_{\mathscr{O}_X}(i_!F_1, I) = \operatorname{Hom}_{\mathscr{O}_U}(F_1, I_{|U})$$

es epiyectivo, luego $I_{|U}$ es inyectivo. □

4. Proposición: *Si $\mathscr{M}$ es un haz de $\mathscr{O}_X$-módulos e I un $\mathscr{O}_X$-módulo inyectivo, entonces $\underline{\operatorname{Hom}}_X(\mathscr{M}, I)$ es un haz flasco. En particular, tomando $\mathscr{M} = \mathscr{O}_X$, obtenemos que los $\mathscr{O}_X$-módulos inyectivos son flascos.*

Demostración. Dado un $\mathscr{O}_X$-módulo inyectivo I, si tomamos $\operatorname{Hom}_{\mathscr{O}_X}(-, I)$, en la inclusión $i_!\mathscr{M}_{|U} \hookrightarrow \mathscr{M}$ probaremos que $\underline{\operatorname{Hom}}_{\mathscr{O}_X}(\mathscr{M}, I)$ es flasco. □

Supongamos que la categoría abeliana que consideramos tiene suficientes inyectivos, es decir, cada objeto M se inyecta, de modo funtorial, en un objeto inyectivo $I(M)$. Así sucede, por ejemplo, en la categoría de los A-módulos, o más en general, en la categoría de $\mathscr{O}_X$-módulos. Supóngase además que $I(0) = 0$. Denotemos $M_1 = I(M)/M$ y definimos, recurrentemente, $I^n(M) = I^{n-1}(M_1)$. Obtenemos así una resolución $I^\cdot(M)$ de M por objetos inyectivos. Si $M^\cdot$ es un complejo, denotaremos $I^\cdot(M^\cdot)$ al complejo simple asociado al bicomplejo $I^p(M^q)$. El teorema 7.2.16 nos dice que el morfismo natural $M^\cdot \to I^\cdot(M^\cdot)$ es un quasi-isomorfismo. Por ello, diremos que $I^\cdot(M^\cdot)$ es una resolución de $M^\cdot$ por inyectivos.

Observemos que si bien $I^\cdot(M^\cdot \oplus N^\cdot)$ no es en general isomorfo a $I^\cdot(M^\cdot) \oplus I^\cdot(N^\cdot)$, el morfismo natural $I^\cdot(M^\cdot) \oplus I^\cdot(N^\cdot) \to I^\cdot(M^\cdot \oplus N^\cdot)$, que tiene retracto natural, es un quasi-isomorfismo, porque ambos complejos son quasi-isomorfos a $M^\cdot \oplus N^\cdot$.

5. Definición: Dado un funtor $F: \mathscr{C} \to \mathscr{C}'$ covariante y aditivo entre categorías abelianas, llamaremos funtor derivado por la derecha de F al funtor

$$\mathbb{R}F: K_{\mathscr{C}} \to K_{\mathscr{C}'}$$

entre las categorías de complejos, definido por $\mathbb{R}F(M^{\cdot}) = F(I^{\cdot}(M^{\cdot}))$. Denotaremos

$$\mathbb{R}^n F(M^{\cdot}) := H^n(\mathbb{R}F(M^{\cdot}))$$

y diremos que es el hiperfuntor derivado n-ésimo de F. La restricción del funtor $\mathbb{R}^n F$ a la categoría $\mathscr{C}$ se denota $R^n F$ y se denomina funtor derivado n-ésimo de F.

Dado un morfismo de complejos $f: M^{\cdot} \to N^{\cdot}$, denotaremos $\mathbb{R}F(f): \mathbb{R}F(M^{\cdot}) \to \mathbb{R}F(N^{\cdot})$ al morfismo inducido.

6. Definición: Diremos que un complejo $K^{\cdot}$ es F-acíclico cuando el morfismo natural $F(K^{\cdot}) \to \mathbb{R}F(K^{\cdot})$ es un quasi-isomorfismo.

7. Observación: A partir de ahora supondremos que los complejos están acotados inferiormente, y por sencillez, supondremos que $M^i = 0$ para $i < 0$.

8. Teorema: *Se cumple que:*

1. *$\mathbb{R}F$ conserva quasi-isomorfismos.*
2. *Todos los complejos de inyectivos son F-acíclicos.*
3. *(De Rham) Si $M^{\cdot} \to J^{\cdot}$ es un quasi-isomorfismo y $J^{\cdot}$ es F-acíclico (por ejemplo, si $J^{\cdot}$ es un complejo de inyectivos), entonces $\mathbb{R}^n F(M^{\cdot}) \simeq H^n(F(J^{\cdot}))$.*
4. *Los isomorfismos del apartado anterior son naturales, en el siguiente sentido: Dado un diagrama conmutativo,*

$$\begin{array}{ccc} M^{\cdot} & \xrightarrow{f} & N^{\cdot} \\ \downarrow & & \downarrow \\ J^{\cdot} & \xrightarrow{\phi} & K^{\cdot} \end{array}$$

donde $J^{\cdot}$ y $K^{\cdot}$ son F-acíclicos y las flechas verticales son quasi-isomorfismos, se tiene para cada n un diagrama conmutativo:

$$\begin{array}{ccc} \mathbb{R}^n F(M^{\cdot}) & \xrightarrow{\mathbb{R}^n F(f)} & \mathbb{R}^n F(N^{\cdot}) \\ \wr\downarrow & & \downarrow\wr \\ H^n(F(J^{\cdot})) & \xrightarrow{\phi} & H^n(F(K^{\cdot})) \end{array}$$

Demostración. 1. Sea $f: K^\cdot \to L^\cdot$ un quasi-isomorfismo. El morfismo inducido

$$I_f: I^\cdot(K^\cdot) \to I^\cdot(L^\cdot)$$

es un quasi-isomorfismo, pues $I^\cdot(K^\cdot)$ y $I^\cdot(L^\cdot)$ son quasi-isomorfos a $K^\cdot$ y $L^\cdot$. En consecuencia, el cono del morfismo I_f es un complejo acíclico, inyectivo y acotado inferiormente, luego escindido. Entonces $F(\mathrm{Cono}(I_f))$ es un complejo acíclico, porque F es aditivo y transforma sucesiones exactas acotadas inferiormente de inyectivos en sucesiones exactas. De las igualdades $F(\mathrm{Cono}(I_f)) = \mathrm{Cono}(F(I_f)) = \mathrm{Cono}(\mathbb{R}F(f))$ concluimos que $\mathbb{R}F(f): \mathbb{R}F(K^\cdot) \to \mathbb{R}F(L^\cdot)$ es un quasi-isomorfismo.

2. Sea $J^\cdot$ un complejo de inyectivos e $i: J^\cdot \to I^\cdot(J^\cdot)$ la inclusión. $\mathrm{Cono}(i)$ es un complejo de inyectivos, acíclico y acotado inferiormente, luego $F(\mathrm{Cono}(i)) = \mathrm{Cono}(F(i))$ es un complejo acíclico y por tanto $F(i): F(J^\cdot) \to \mathbb{R}F(J^\cdot)$ es un quasi-isomorfismo.

3. Es consecuencia de 1.

4. Se verifican los diagramas conmutativos

$$\begin{array}{ccc} \mathbb{R}F(M^\cdot) & \xrightarrow{\mathbb{R}F(f)} & \mathbb{R}F(N^\cdot) \\ \downarrow & & \downarrow \\ \mathbb{R}F(J^\cdot) & \xrightarrow{\mathbb{R}F(\phi)} & \mathbb{R}F(K^\cdot) \end{array} \qquad \begin{array}{ccc} F(J^\cdot) & \xrightarrow{\phi} & F(K^\cdot) \\ \downarrow & & \downarrow \\ \mathbb{R}F(J^\cdot) & \xrightarrow{\mathbb{R}F(\phi)} & \mathbb{R}F(K^\cdot) \end{array}$$

donde las flechas verticales son quasi-isomorfismos, de donde se concluye. □

9. Teorema: *Se cumple que:*

1. *Los (hiper)funtores derivados $\mathbb{R}^iF$ son aditivos.*
2. *Sucesión exacta de (hiper)funtores derivados: Si $0 \to M_1^\cdot \to M_2^\cdot \to M_3^\cdot \to 0$ es una sucesión exacta de complejos inferiormente acotados, existen morfismos de conexión $\delta_i: \mathbb{R}^iF(M_3^\cdot) \to \mathbb{R}^{i+1}F(M_1^\cdot)$ tales que se tiene una sucesión exacta larga:*

$$\cdots \to \mathbb{R}^{i-1}F(M_3^\cdot) \xrightarrow{\delta_{i-1}} \mathbb{R}^iF(M_1^\cdot) \to \mathbb{R}^iF(M_2^\cdot) \to \mathbb{R}^iF(M_3^\cdot) \xrightarrow{\delta_i} \mathbb{R}^{i+1}F(M_1^\cdot) \to \cdots$$

3. *F es exacto por la izquierda si y solo si $F \simeq R^0F$.*
4. *F es exacto si y solo si $R^iF = 0$ para todo $i > 0$.*

Demostración. 1. Si $f, g: M^\cdot \to N^\cdot$ son morfismos de complejos, se verifica un diagrama conmutativo

$$\begin{array}{ccc} M^\cdot & \xrightarrow{f+g} & N^\cdot \\ \downarrow & & \downarrow \\ I^\cdot(M^\cdot) & \xrightarrow{I^\cdot(f)+I^\cdot(g)} & I^\cdot(N^\cdot) \end{array}$$

y se concluye por 4. del Teorema 10.6.8.

2. Sea $\pi\colon M_2^{\cdot} \to M_3^{\cdot}$. El morfismo natural $M_1^{\cdot} \to \mathrm{Cono}(\pi)$, $m_1 \mapsto (m_1, 0)$, es un quasi-isomorfismo, como se deduce de la sucesión exacta de complejos

$$0 \to M_1^{\cdot} \to \mathrm{Cono}(\pi) \to \mathrm{Cono}(\mathrm{Id}_{M_3}) \to 0$$

Por 1) del Teorema 10.6.8, $\mathbb{R}^i F(M_1^{\cdot}) \simeq \mathbb{R}^i F(\mathrm{Cono}(\pi))$.

Por otra parte, consideremos la sucesión exacta de complejos

$$0 \to \mathbb{R}F(M_3^{\cdot}) \to \mathrm{Cono}(\mathbb{R}F(\pi)) \to \mathbb{R}F(M_2^{\cdot})[1] \to 0 \qquad (*)$$

Como $\mathbb{R}F(\mathrm{Cono}(\pi))$ es quasi-isomorfo a $\mathrm{Cono}(\mathbb{R}F(\pi))$, se concluye tomando la sucesión exacta larga de cohomología asociada. (Dejamos que el lector pruebe que el connecting asociado a la sucesión exacta (*) coincide con el morfismo natural $\mathbb{R}^i F(M_2^{\cdot}) \to \mathbb{R}^i F(M_3^{\cdot})$).

3. y 4. son inmediatos a partir de la sucesión exacta de funtores derivados. □

10. Teorema del funtor compuesto de Grothendieck: *Si F transforma módulos inyectivos en G-acíclicos, entonces para cada complejo inferiormente acotado $M^{\cdot}$ se tiene un quasi-isomorfismo $\mathbb{R}(GF)(M^{\cdot}) \to \mathbb{R}G(\mathbb{R}F(M^{\cdot}))$, funtorial en $M^{\cdot}$.*

Demostración. Por la hipótesis y el teorema 7.2.16, $G(F(I^{\cdot}(M^{\cdot}))) \to \mathbb{R}G(F(I^{\cdot}(M^{\cdot})))$ es un quasi-isomorfismo. □

11. Corolario: *Si F transforma módulos inyectivos en módulos G-acíclicos, $M^{\cdot}$ es un complejo inferiormente acotado y $R^p F M^{\cdot} = 0$ para todo $p \neq q$, entonces $\mathbb{R}^{n+q}(GF)(M^{\cdot}) = \mathbb{R}^n G(\mathbb{R}^q F(M^{\cdot}))$.*

Demostración. Sea $B^{\cdot} = \mathbb{R}F(M^{\cdot})$. Sea $B^{\leq q}$ el complejo

$$B^{\leq q} := \cdots \to B^{q-2} \to B^{q-1} \to \mathrm{Ker}\, \mathrm{d}^q \to 0 \cdots$$

Es inmediato que

$$H^i(B^{\leq q}) = \begin{cases} RF^i(M^{\cdot}) \text{ para } i \leq q \\ 0 \quad \text{para } i > q \end{cases}$$

Por las hipótesis,

$$H^q(B^{\cdot})[-q] \leftarrow B^{\leq q} \to B^{\cdot}$$

son quasi-isomorfismos, luego $\mathbb{R}G(R^q F(M^{\cdot})[-q])$ es quasi-isomorfo a $\mathbb{R}G(\mathbb{R}F(M^{\cdot}))$, que es quasi-isomorfo a $\mathbb{R}(G \circ F)(M^{\cdot})$, por el teorema del funtor compuesto de Grothendieck. Luego,

$$R^n G(R^q F(M^{\cdot})) = R^{n+q}(G \circ F)(M^{\cdot}).$$

□

10.6.1. Funtores derivados por la izquierda

Supongamos ahora que C es una categoría abeliana con suficientes proyectivos, es decir, cada objeto M es cociente de un proyectivo $P(M) \to M$, que depende funtorialmente de él. Puede desarrollarse entonces una teoría de hiperfuntores derivados por la izquierda análoga al caso anterior, pero ahora para complejos superiormente acotados.

Así el (hiper)funtor derivado por la izquierda de un funtor covariante aditivo F será $\mathbb{L}F(M^{\cdot}) = F(P^{\cdot}(M))$, y el n-ésimo hiperfuntor derivado por la izquierda de F será

$$\mathbb{L}_n F(M^{\cdot}) = H^{-n}(\mathbb{L}F(M^{\cdot})).$$

Como antes, la restricción a C serán los funtores derivados por la izquierda $\mathscr{L}_n F$.

Análogamente se prueba que los hiperfuntores derivados se calculan con cualquier resolución F-acíclica (es decir, $\mathbb{L}F(M^{\cdot}) \to F(M^{\cdot})$ es quasi-isomorfismo), que son aditivos y además $\mathscr{L}_0 F \simeq F$ si y solo si F es exacto por la derecha y $\mathscr{L}_i F = 0$ para todo $i \neq 0$ si y solo si F es exacto.

Se tiene la sucesión exacta larga de hiperfuntores derivados por la izquierda: Si $0 \to M_1^{\cdot} \to M_2^{\cdot} \to M_3^{\cdot} \to 0$ es una sucesión exacta de complejos superiormente acotados, se tiene una sucesión exacta larga

$$\cdots \to \mathbb{L}_{n+1}F(M_3^{\cdot}) \to \mathbb{L}_n F(M_1^{\cdot}) \to \mathbb{L}_n F(M_2^{\cdot}) \to \mathbb{L}_n F(M_3^{\cdot}) \to \mathbb{L}_{n-1}F(M_1^{\cdot}) \to \cdots$$

Por último, se verifica el teorema del funtor compuesto: si F transforma módulos proyectivos en módulos G-acíclicos, se tiene un quasi-isomorfismo $\mathbb{L}(GF)(M^{\cdot}) \to \mathbb{L}G(\mathbb{L}F(M^{\cdot}))$.

La teoría de funtores derivados de un funtor contravariante se desarrolla considerándolo como un funtor covariante sobre la categoría dual.

10.6.2. Ejemplos

1. **Hipercohomología.**

Sea X un espacio topológico, $\mathscr{C}$ la categoría de haces de grupos abelianos sobre X y Ab la categoría de grupos abelianos. Consideremos el funtor de secciones globales:

$$\begin{aligned} \Gamma(X,-)\colon \mathscr{C} &\rightsquigarrow \mathrm{Ab} \\ F &\rightsquigarrow \Gamma(X,F) \end{aligned}$$

que es un funtor exacto por la izquierda. Para cada complejo $K^{\cdot}$ de haces, denotaremos $\mathbb{R}\Gamma(X,K^{\cdot})$ su hiperfuntor derivado por la derecha, y $\mathbb{H}^i(X,K^{\cdot})$ su i-ésimo funtor derivado. El grupo abeliano $\mathbb{H}^i(X,K^{\cdot})$ se denomina i-ésimo grupo de hipercohomología

de $K^{\cdot}$. Los funtores derivados por la derecha $R^i\Gamma(X,-)$ coinciden con los grupos de cohomología:

$$R^i\Gamma(X,-) = H^i(X,-).$$

Esto se deduce de que los haces inyectivos son flascos y del teorema de De Rham (10.4.11). La sucesión exacta larga de funtores derivados es la sucesión exacta larga de cohomología. Los haces $\Gamma(X,F)$-acíclicos son exactamente los haces acíclicos (es decir, los haces de cohomología nula).

Más generalmente, si $(X,\mathscr{O}_X)$ es un espacio anillado (es decir, $\mathscr{O}_X$ es un haz de anillos en X) y $\mathscr{C}$ es la categoría de $\mathscr{O}_X$-módulos, los funtores derivados por la derecha del funtor $\Gamma(X,-)\colon \mathscr{C} \rightsquigarrow \mathrm{Ab}$ son los grupos de cohomología, pues los $\mathscr{O}_X$-módulos inyectivos son flascos.

2. **Extens locales y globales.**

12. Definición: Sea $(X,\mathscr{O}_X)$ un espacio anillado (es decir, $\mathscr{O}_X$ es un haz de anillos en X) y $\mathscr{C}$ la categoría de $\mathscr{O}_X$-módulos. Definimos los funtores $\mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{M},-)$ (resp. $\underline{\mathrm{Ext}}^i_{\mathscr{O}_X}(\mathscr{M},-)$) como los funtores derivados por la derecha del funtor $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},-)$ (resp. del funtor $\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M},-)$).

Dado que $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},-)$ es exacto por la izquierda, se tiene que $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}) = \mathrm{Ext}^0_{\mathscr{O}_X}(\mathscr{M},\mathscr{N})$ (análogamente para $\underline{\mathrm{Hom}}$). Si $0 \to \mathscr{N}_1 \to \mathscr{N}_2 \to \mathscr{N}_3 \to 0$ es una sucesión exacta de $\mathscr{O}_X$-módulos, induce una sucesión exacta larga de grupos Ext

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_1) \to \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_2) \to \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_3) \to \\ \to \mathrm{Ext}^1_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_1) \to \mathrm{Ext}^1_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_2) \to \mathrm{Ext}^1_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}_3) \to \cdots \end{aligned}$$

Análogamente, para los haces $\underline{\mathrm{Ext}}$.

Si X es un sólo punto, entonces $\mathscr{O}_X$ es un anillo A, y la categoría de $\mathscr{O}_X$-módulos es la categoría de A-módulos. En este caso se obtienen los extens de A-módulos definidos en el capítulo 7, sección 7.3.

El funtor $\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M},-)$ transforma inyectivos en flascos, por 10.6.4 y estos son $\Gamma(X,-)$-acíclicos. De la igualdad $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}) = \Gamma(X,\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}))$ y el teorema del funtor compuesto de Gothendieck, tenemos el quasi-isomorfismo $\mathbb{R}\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}) \to \mathbb{R}\Gamma(X,\mathbb{R}\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N}))$.

De la igualdad $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{O}_X,\mathscr{M}) = \Gamma(X,\mathscr{M})$ se deduce la igualdad $\mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{O}_X,\mathscr{M}) = H^i(X,\mathscr{M})$. Sea $\mathscr{L}$ es un $\mathscr{O}_X$-módulo tal que para todo punto x existe un entorno abierto U_x tal que $\mathscr{L}_{|U_x} \simeq \mathscr{O}_{U_x}$. Denotemos $\mathscr{L}^* = \underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{L},\mathscr{O}_X)$. Entonces, $\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{L},\mathscr{M}) = \Gamma(X,\mathscr{M}\otimes\mathscr{L}^*)$ y se deduce fácilmente la igualdad $\mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{L},\mathscr{M}) = H^i(X,\mathscr{M}\otimes\mathscr{L}^*)$.

3. **Imágenes directas superiores.**

Sea $f: X \to Y$ una aplicación continua, $\mathscr{C}_X$, $\mathscr{C}_Y$ las categorías de haces de grupos abelianos en X e Y respectivamente. Consideremos el funtor imagen directa

$$f_*: \mathscr{C}_X \rightsquigarrow \mathscr{C}_Y$$

que es exacto por la izquierda. Sus funtores derivados por la derecha, $R^i f_*$, coinciden con las imágenes directas superiores definidas en la sección 13.2. La sucesión exacta larga de funtores derivados coincide con la sucesión exacta larga de las imágenes directas superiores.

Sea $g: Y \to Z$ es una aplicación continua. Como f_* transforma haces inyectivos en haces g_*-acíclicos (pues la imagen directa de un inyectivo es inyectivo), podemos aplicar el teorema del funtor compuesto y obtenemos un quasi-isomorfismo $\mathbb{R}g_*(\mathbb{R}f_*(K^\cdot)) \to \mathbb{R}(g\circ f)_*(K^\cdot)$.

4. **Tores.**

Sea A un anillo y $\mathscr{C}$ la categoría de A-módulos. Dado un A-módulo M, definimos el funtor:

$$\begin{aligned} M\otimes_A -: \mathscr{C} &\rightsquigarrow \mathscr{C} \\ N &\rightsquigarrow M\otimes_A N \end{aligned}$$

que es exacto por la derecha. Sus funtores derivados por la derecha son los funtores $\mathrm{Tor}_i^A(M,-)$, definidos en la sección 7.3. La sucesión exacta de funtores derivados es la sucesión exacta de tores. La anulación de estos funtores para $i>0$ equivale a la exactitud del funtor $M\otimes_A -$, es decir, a la platitud de M.

10.7. Problemas

1. Sea X un espacio topológico y $U, V \subset X$ dos abiertos disjuntos. Si F es un haz en X, prueba que $F(U\cup V) = F(U)\times F(V)$.

2. Sea Σ un haz de anillos constante, y $F\subseteq\Sigma$ un subprehaz de anillos. Demuestra que el prehaz $\tilde{F}$, definido por $\tilde{F}(U) = \bigcap\limits_{x\in U} F_x$, es un haz de anillos y coincide con el hacificado de F.

3. Prueba que un prehaz F sobre un espacio topológico X es un haz, si y solo si para todo abierto U, todo recubrimiento $\{U_i\}$ por abiertos de U y un recubrimiento $\{U_{ijk}\}$ por abiertos de $U_i\cap U_j$, la sucesión

$$F(U) \to \prod_i F(U_i) \rightrightarrows \prod_{i,j,k} F(U_{ijk})$$

es exacta.

4. Sea $\mathscr{B}$ una base de la topología de X y F un prehaz en X. Prueba que F es un haz si y solo si para todo abierto U, todo recubrimiento $\{U_i \in \mathscr{B}\}$ por abiertos de U y un recubrimiento $\{U_{ijk} \in \mathscr{B}\}$ por abiertos de $U_i \cap U_j$, la sucesión

$$F(U) \to \prod_i F(U_i) \rightrightarrows \prod_{i,j,k} F(U_{ijk})$$

es exacta.

5. Dado un prehaz P se le puede asociar de modo natural un prehaz $\tilde{P}$:

$$\tilde{P}(U) := \coprod_{\{U_\alpha\}_\alpha : \bigcup_\alpha U_\alpha = U} \left\{ (s_\alpha) \in \prod_\alpha P(U_\alpha) \colon s_{\alpha x} = s_{\beta_x} \text{ para todo } x \in U_\alpha \cap U_\beta \right\} / \sim$$

donde $\sim$ es la siguiente relación de equivalencia: $(s_\alpha) \sim (s'_{\alpha'})$ si $s_{\alpha x} = s'_{\alpha' x}$ para todo $x \in U_\alpha \cap U_{\alpha'}$. Demuestra que $\tilde{P}$ es el haz asociado a P.

6. Prueba que la propiedad de ser flasco es local. Es decir, dado un haz F sobre X, si $\{U_i\}$ un recubrimiento por abiertos de X tal que $F_{|U_i}$ es flasco para todo i, entonces F es flasco.

Capítulo 11

Esquemas

11.1. Espacios anillados

Es obvio que cuando miramos una esfera no estamos viendo simplemente un conjunto de puntos, sino que además, estamos añadiendo una estructura topológica. Es decir, vemos la esfera como un conjunto con una topología (un espacio topológico). Ahora bien la estructura que vemos en la esfera depende del tipo de observaciones (= funciones) que admitamos sobre ella. Si admitimos todas las observaciones continuas, la esfera es equivalente (= homeomorfa) a un cubo. No ocurre lo mismo si solo admitimos observaciones diferenciables; en este caso la esfera es localmente equivalente (=difeomorfa) a un disco y no es globalmente equivalente a un cubo. La geometría de la esfera depende del tipo de observaciones que admitimos sobre ella. Cuando hemos definido una variedad algebraica, los únicos conjuntos que "observamos" son los definidos a partir de las funciones algebraicas. Es decir, cuando escribíamos $\operatorname{Spec} A$, en realidad siempre teníamos presente la pareja $(\operatorname{Spec} A, A)$.[1]

Así pues, un espacio es la pareja formada por un espacio topológico y un cierto anillo de observaciones sobre él, que están definidas o determinadas localmente.

H. Cartan expresó la analogía entre variedades algebraicas y analíticas afirmando que en todos los casos se trataban de espacios anillados. Serre introdujo la teoría de haces y la cohomología de haces en el estudio de las variedades algebraicas abstractas. Finalmente, Grothendieck presentó la definición de esquema como espacio anillado que localmente es un esquema afín. Los esquemas son los objetos básicos de estudio

[1] Desde un punto de vista epistemológico las observaciones del espacio son previas a toda concepción del espacio y éste se obtiene como objetivación de aquéllas. El problema de cómo puede haber observaciones sin tener previamente el espacio aquí queda desdibujado, pues no encontramos ninguna dificultad en la definición de A sin tener $\operatorname{Spec} A$, si bien, para definir A siempre necesitaremos de los conjuntos o al menos del conjunto $\mathbb{N}$.

de la Geometría Algebraica Abstracta actual.

1. Definición: Un espacio anillado es una pareja $(X,\mathscr{O}_X)$ formada por un espacio topológico X y un haz de anillos $\mathscr{O}_X$ sobre X.

Si $(X,\mathscr{O}_X)$ es un espacio anillado, diremos que X es el espacio topológico subyacente y que $\mathscr{O}_X$ es el haz estructural. Por brevedad diremos que X es un espacio anillado.

2. Definición: Un espacio anillado en anillos locales es un espacio anillado $(X,\mathscr{O}_X)$ tal que las fibras $\mathscr{O}_{X,x}$ son anillos locales.

3. Ejemplos: Las variedades diferenciales y las variedades topológicas son espacios anillados en anillos locales.

4. Definición: Un morfismo de espacios anillados $(X,\mathscr{O}_X)\to(Y,\mathscr{O}_Y)$ es una pareja formada por una aplicación continua $f\colon X\to Y$, y un morfismo de haces de anillos $\phi\colon \mathscr{O}_Y\to f_*\mathscr{O}_X$ (que equivale por adjunción a un morfismo $f^{-1}\mathscr{O}_Y\to\mathscr{O}_X$ de haces de anillos).

Si $(f,\phi)\colon (X,\mathscr{O}_X)\to(Y,\mathscr{O}_Y)$ es un morfismo de espacios anillados, para cada punto $x\in X$ se tiene un morfismo de anillos $\phi_x\colon \mathscr{O}_{Y,f(x)}\to\mathscr{O}_{X,x}$, sin más que tomar fibra en el morfismo $f^{-1}\mathscr{O}_Y\to\mathscr{O}_X$.

5. Definición: Un morfismo $(X,\mathscr{O}_X)\to(Y,\mathscr{O}_Y)$ de espacios anillados entre espacios anillados en anillos locales se dice que es un morfismo en anillos locales, si los morfismos $\mathscr{O}_{Y,f(x)}\to\mathscr{O}_{X,x}$ son dominantes, es decir, aplican el ideal maximal del primer anillo dentro del ideal maximal del segundo.

6. Ejemplo: Sea $f\colon X\to Y$ es una aplicación diferenciable entre variedades diferenciales. Para cada abierto $U\subseteq Y$, tenemos un morfismo de anillos $\mathscr{C}^\infty_Y(U)\to\mathscr{C}^\infty_X(f^{-1}(U))$, $g\mapsto g\circ f_{|f^{-1}(U)}$. Estos morfismos definen un morfismo de haces de anillos $\mathscr{C}^\infty_Y\to f_*\mathscr{C}^\infty_X$. En fibra tenemos el morfismo $\mathscr{C}^\infty_{Y,f(x)}\to\mathscr{C}^\infty_{X,x}$, $[g]\mapsto[g\circ f]$, que aplica el ideal maximal de los gérmenes de funciones que se anulan en $f(x)$ en el ideal maximal de los gérmenes de funciones que se anulan en x. Recíprocamente, dado un morfismo de espacios anillados en anillos locales $(X,\mathscr{C}^\infty_X)\to(Y,\mathscr{C}^\infty_Y)$ tenemos una aplicación continua $f\colon X\to Y$ y un morfismo $\varphi\colon \mathscr{C}^\infty_Y\to f_*\mathscr{C}^\infty_X$. Para cada $x\in X$ tenemos que $\mathscr{C}^\infty_{Y,f(x)}/\mathfrak{m}_{f(x)}=\mathbb{R}=\mathscr{C}^\infty_{X,x}/\mathfrak{m}_x$, luego $h(f(x))=\phi(h)(x)$, para toda función diferenciable h de Y. Por tanto, $\phi(h)=h\circ f$ y f es una aplicación diferenciable. En conclusión, las aplicaciones diferenciables de X en Y coinciden con los morfismos de espacios anillados en anillos locales $(X,\mathscr{C}^\infty_X)\to(Y,\mathscr{C}^\infty_Y)$.

7. Notación: Dados dos espacios anillados en anillos locales $(X,\mathscr{O}_X)$ e $(Y,\mathscr{O}_Y)$, al conjunto de los morfismos en anillos locales del primero en el segundo, lo denotaremos $\mathrm{Hom}_{loc}(X,Y)$.

11.1.1. Esquemas afines

En los primeros capítulos decíamos que A es el anillo de funciones de $\mathrm{Spec}\,A$ y A_a el anillo de funciones del abierto básico $U_a = \mathrm{Spec}\,A_a$. Estábamos aproximándonos al hecho de que $\mathrm{Spec}\,A$ tiene una estructura natural de espacio anillado.

8. Definición: Denotaremos por $\widetilde{A}$ al haz sobre $\mathrm{Spec}\,A$ asociado al prehaz de localización de A (ver 10.1.3, ejemplo 4.). Diremos que $\widetilde{A}$ es el haz de localizaciones en abiertos de $\mathrm{Spec}\,A$.

9. Proposición: *Para todo $x \in \mathrm{Spec}\,A$, $\widetilde{A}_x = A_x$. Por tanto, $(\mathrm{Spec}\,A, \widetilde{A})$ es un espacio anillado en anillos locales.*

Demostración. Se deduce de la Proposición 10.1.5 y de que un prehaz tiene las mismas fibras que su haz asociado. □

10. Definición: Diremos que un espacio anillado en anillos locales $(X,\mathscr{O}_X)$ es un esquema afín si es isomorfo, como espacio anillado en anillos locales, a $(\mathrm{Spec}\,A, \widetilde{A})$.

11. Lema: *Si $i\colon A \to B$ es un morfismo fielmente plano, la sucesión*

$$A \to B \underset{i_2}{\overset{i_1}{\rightrightarrows}} B \otimes_A B$$

donde $i_1(b) := b \otimes 1$ e $i_2(b) = 1 \otimes b$, es exacta.

Demostración. Tensando por $\otimes_A B$, basta probar que la sucesión

$$B \overset{i\otimes 1}{\to} B \otimes_A B \rightrightarrows (B \otimes_A B) \otimes_A B = (B \otimes_A B) \otimes_B (B \otimes_A B)$$

es exacta. Ahora bien, $B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$ es un retracto de $i \otimes 1$.

En conclusión, basta demostrar el lema cuando i (que lo vamos a pensar como una inclusión) tiene un retracto, llamémoslo r. Ahora ya, si $b \otimes 1 = i_1(b) = i_2(b) = 1 \otimes b$, entonces si consideramos el morfismo $B \otimes_A B \to B$, $b \otimes b' \mapsto r(b)b'$ tenemos que $r(b)\cdot 1 = 1 \cdot b$ y $b \in A$ y hemos terminado. □

12. Teorema: *Si U_f es un abierto básico de $X = \operatorname{Spec} A$, entonces*

$$\widetilde{A}(U_f) = A_f$$

En particular, $\widetilde{A}(X) = A$.

Demostración. Tenemos que ver que el morfismo natural $A_f \to \widetilde{A}(U_f)$ entre las secciones (en U_f) del prehaz de localizaciones y las de su haz asociado es isomorfismo. Por la observación 10.1.14, basta ver que el prehaz de localizaciones es haz sobre los abiertos básicos, es decir, que para todo abierto básico U_f y todo recubrimiento $U_{f_1}, \ldots, U_{f_n}$ de U_f por abiertos básicos, la siguiente sucesión es exacta

$$A_f \to \prod_{i=1}^{n} A_{f_i} \rightrightarrows \prod_{i,j}^{n} (A_{f_i} \otimes_{A_f} A_{f_j})$$

Denotemos $B = \prod_{i=1}^{n} A_{f_i}$. Como $A_f \to B$ es fielmente plano y $B \otimes_{A_f} B = \prod_{i,j}^{n} (A_{f_i} \otimes_{A_f} A_{f_j})$ hemos terminado por el lema anterior.

□

13. Proposición: *Se cumple que*

$$\operatorname{Hom}_{loc}(\operatorname{Spec} B, \operatorname{Spec} A) = \operatorname{Hom}_{anillos}(A, B)$$

Es decir, categoría de los esquemas afines es anti-equivalente a la categoría de los anillos.

Demostración. Denotemos $X = \operatorname{Spec} B$, $Y = \operatorname{Spec} A$. Todo morfismo de espacios anillados en anillos locales $(f, \phi) \colon (X, \widetilde{B}) \to (Y, \widetilde{A})$, induce, tomando secciones globales en el morfismo $\phi \colon \widetilde{A} \to f_* \widetilde{B}$, un morfismo de anillos $\phi_Y : A \to B$. Veamos que el morfismo (f, ϕ) está unívocamente determinado por ϕ_Y.

1. $f : X \to Y$ coincide con el morfismo inducido entre espectros por $\phi_Y : A \to B$. Esto se deduce del diagrama conmutativo

$$\begin{array}{ccc} A & \xrightarrow{\phi_Y} & B \\ \downarrow & & \downarrow \\ \widetilde{A}_{f(x)} = A_{f(x)} & \xrightarrow{\phi_x} & \widetilde{B}_x = B_x \end{array}$$

y de que $\phi_x \colon A_{f(x)} \to B_x$ es local.

2. ϕ está determinado por ϕ_Y: en efecto, si U_a es un abierto básico de Y, y denotamos $b = \phi_Y(a)$, entonces $f^{-1}(U_a) = U_b$ (por 1.) y el diagrama

$$\begin{array}{ccc} A & \xrightarrow{\phi_Y} & B \\ \downarrow & & \downarrow \\ \widetilde{A}(U_a) = A_a & \xrightarrow{\phi_{U_a}} & \widetilde{B}(U_b) = B_b \end{array}$$

es conmutativo, luego ϕ_{U_a} es la localización de ϕ_Y, y en conclusión ϕ está determinado por ϕ_Y.

Recíprocamente, dado un morfismo de anillos $h: A \to B$, induce por paso al espectro una aplicación continua $h^* = f: X \to Y$. Para cada abierto U de Y se obtiene por localización de h un morfismo

$$A_U \to B_{f^{-1}(U)}$$

y por tanto un morfismo de haces $\phi: \widetilde{A} \to f_*\widetilde{B}$. Es inmediato comprobar que (f, ϕ) es un morfismo de espacios anillados en anillos locales y que $\phi(Y) = h$. Con todo concluimos. □

Sea $(X, \mathcal{O}_X)$ un espacio anillado en anillos locales. Denotemos $A = \Gamma(X, \mathcal{O}_X)$. Para cada $x \in X$ tenemos el morfismo $A \to \mathcal{O}_{X,x}$, $a \mapsto a_x$. Denotemos $\mathfrak{p}_{f(x)} \subset A$ la antimagen del maximal $\mathfrak{p}_x \subset \mathcal{O}_{X,x}$ por dicho morfismo. Tenemos entonces la aplicación

$$f: X \to \operatorname{Spec} A,\ x \mapsto f(x).$$

14. Proposición: *La aplicación $f: X \to \operatorname{Spec} A$ es continua.*

Demostración. Basta ver que la antimagen de un abierto básico es un abierto. Sea U_a un abierto básico de $\operatorname{Spec} A$. Entonces

$$f^{-1}(U_a) = \{x \in X \text{ tales que } a \text{ es invertible en } \mathcal{O}_{X,x}\}$$

y esto es un abierto porque si a es invertible en $\mathcal{O}_{X,x}$, existe un entorno U_x de x tal que a es invertible en $\mathcal{O}_{X,y}$ para todo $y \in U_x$. □

Definamos ahora un morfismo de haces $\widetilde{A} \to f_*\mathcal{O}_X$. Sea V un abierto de $\operatorname{Spec} A$ y $U = f^{-1}(V)$. Consideremos el morfismo de restricción $A \to \mathcal{O}_X(U)$, $a \mapsto a_{|U}$. Si $a \in A$ no se anula en ningún punto de V, entonces $a_{|U}$ es invertible. En efecto, para todo $x \in U$ tenemos un diagrama conmutativo

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{O}_X(U) \\ \downarrow & & \downarrow \\ A_{f(x)} & \longrightarrow & \mathcal{O}_{X,x} \end{array}$$

y como a es invertible en $A_{f(x)}$, también lo es en $\mathcal{O}_{X,x}$.

Por la propiedad universal de la localización, el morfismo $A \to \mathcal{O}_X(U)$ factoriza por la localización en V, es decir, induce un morfismo $A_V \to \mathcal{O}_X(U)$. En conclusión, hemos definido un morfismo del prehaz de localizaciones de A en $f_*\mathcal{O}_X$, y por tanto un morfismo de haces $\widetilde{A} \to f_*\mathcal{O}_X$.

Por construcción, el morfismo $\widetilde{A}_{f(x)} \to \mathcal{O}_{X,x}$ inducido en fibras por el morfismo de haces de anillos $\widetilde{A} \to f_*\mathcal{O}_X$ no es otro que el morfismo $A_{f(x)} \to \mathcal{O}_{X,x}$ inducido por el morfismo de anillos $A \to \mathcal{O}_{X,x}$ por localización.

En conclusión, hemos definido un morfismo de espacios anillados en anillos locales

$$X \to \operatorname{Spec}\Gamma(X,\mathcal{O}_X).$$

15. Definición: Diremos que $\operatorname{Spec}\Gamma(X,\mathcal{O}_X)$ es el esquema afín asociado a X o el afinizado de X. Lo denotaremos por X_{af}. El morfismo $X \to X_{\mathrm{af}}$ se denomina morfismo de afinización.

Sea $f\colon X \to Y$ un morfismo de espacios anillados en anillos locales. Por definición, se tiene un morfismo de haces $\mathcal{O}_Y \to f_*\mathcal{O}_X$, que al tomar secciones globales define un morfismo $\mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ y para cada $x \in X$ un diagrama conmutativo

$$\begin{array}{ccc} \mathcal{O}_Y(Y) & \longrightarrow & \mathcal{O}_X(X) \\ \downarrow & & \downarrow \\ \mathcal{O}_{Y,f(x)} & \longrightarrow & \mathcal{O}_{X,x} \end{array}$$

El morfismo $\mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ define un morfismo de espacios anillados $X_{\mathrm{af}} \to Y_{\mathrm{af}}$ y se tiene un diagrama conmutativo

$$\begin{array}{ccc} X & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X_{\mathrm{af}} & \longrightarrow & Y_{\mathrm{af}} \end{array}$$

16. Ejercicio: Prueba que si X es un esquema afín, entonces $X \to X_{\mathrm{af}}$ es un isomorfismo de espacios anillados en anillos locales.

17. Proposición: *Para todo esquema afín* $\operatorname{Spec}B$ *y todo espacio anillado en anillos locales* X *se verifica*

$$\operatorname{Hom}_{loc}(X,\operatorname{Spec}B) = \operatorname{Hom}_{loc}(X_{af},\operatorname{Spec}B) = \operatorname{Hom}_{anillos}(B,\mathcal{O}_X(X))$$

Demostración. Dado un morfismo de espacios anillados en anillos locales $f: X \to Y = \operatorname{Spec} B$ se tiene el diagrama conmutativo

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle \pi} & & \Vert{\scriptstyle \pi} \\ X_{\mathrm{af}} & \longrightarrow & Y_{\mathrm{af}} \end{array}$$

donde π es el morfismo de afinización. Así pues, todo morfismo $X \to \operatorname{Spec} B$ factoriza vía un morfismo $X_{\mathrm{af}} \to \operatorname{Spec} B$. Dados dos morfismos $g, g': X_{\mathrm{af}} \to \operatorname{Spec} B$ distintos, entonces $g \circ \pi \neq g' \circ \pi$, porque $g, g', g \circ \pi, g' \circ \pi$ están determinados por el morfismo de anillos inducido entre las secciones globales. □

11.2. Esquemas

Si $(X, \mathscr{O}_X)$ es un espacio anillado, para cada abierto U denotaremos $\mathscr{O}_U$ la restricción de $\mathscr{O}_X$ a U.

1. Definición: Si $(X, \mathscr{O}_X)$ es un espacio anillado, se dice que un abierto U de X es un abierto afín cuando $(U, \mathscr{O}_U)$ es un esquema afín.

Llamaremos esquema a un espacio anillado en anillos locales $(X, \mathscr{O}_X)$ localmente isomorfo a un esquema afín (es decir, existe un recubrimiento de X por abiertos afines).

2. Ejercicio: Prueba que un abierto de un esquema es un esquema. Demuéstrese que $\mathbb{A}_2 \setminus \{0\}$ no es un esquema afín (Pista: prueba que $\Gamma(\mathbb{A}_2 \setminus \{0\}, \mathscr{O}_{\mathbb{A}_2 \setminus \{0\}}) = k[x, y]$).

3. Definición: Un esquema X se dice reducido si para todo abierto U, $\mathscr{O}_X(U)$ es un anillo reducido.

4. Proposición: *Un esquema X es reducido si y solo si $\mathscr{O}_{X,x}$ es reducido para todo $x \in X$.*

Demostración. Si X es reducido entonces $\mathscr{O}_{X,x}$ es reducido porque dada $\bar{a} \in \mathscr{O}_{X,x}$, $a \in \mathscr{O}_X(U)$ si $\bar{a}^n = 0$ entonces $a^n = 0$ en un entorno abierto de x, $V \subset U$, luego $a = 0$ en V y $\bar{a} = 0$. Recíprocamente, si $\mathscr{O}_{X,x}$ son anillos reducidos para todo $x \in X$, dado un abierto U tenemos el morfismo inyectivo $\mathscr{O}_X(U) \hookrightarrow \prod_{x \in U} \mathscr{O}_{X,x}$, luego $\mathscr{O}_X(U)$ es un anillo reducido. □

5. Definición: Un esquema se dice irreducible cuando no es unión de dos cerrados propios, es decir, cuando el espacio topológico subyacente es irreducible.

6. Ejercicio: Prueba que todo abierto de un espacio topológico irreducible es irreducible.

7. Definición: Un esquema X se dice íntegro si $\mathcal{O}_X(U)$ es íntegro para todo abierto U.

8. Proposición: *Un esquema es íntegro $\Leftrightarrow$ es irreducible y reducido.*

Demostración. Supongamos X íntegro. Obviamente X es reducido. Si X no es irreducible, entonces existen dos abiertos U, V no vacíos de intersección vacía. Entonces, $\mathcal{O}_X(U \cup V) = \mathcal{O}_X(U) \times \mathcal{O}_X(V)$, que no es íntegro y llegamos a contradicción.

Recíprocamente, supongamos X reducido e irreducible. Dado un abierto $U \subseteq X$, sean $f, g \in \mathcal{O}_X(U)$, tales que $f \cdot g = 0$. Sea $(f)_0 := \{x \in U$ tal que el germen de f en x pertenece al maximal de $\mathcal{O}_{X,x}\}$, que es un cerrado de U. Análogamente se define $(g)_0$. Como $f \cdot g = 0$, se deduce que $(f)_0 \cup (g)_0 = U$. Por ser U irreducible, podemos suponer que $U = (f)_0$. Por tanto, para todo abierto afín $V \subset U$, $f_{|V}$ es nilpotente. Como X es reducido, debe ser $f_{|V} = 0$, luego $f = 0$. Por tanto, $\mathcal{O}_X(U)$ es íntegro.

□

Si X es irreducible, existe un punto p (único) cuyo cierre es todo X. En efecto, sea U un abierto afín. Como U es irreducible, sabemos que existe un punto $p \in U$ cuyo cierre en U es U. Entonces $X = \bar{p} \cup U^c$, luego $\bar{p} = X$. En particular, todo abierto V de X contiene a p. Además p es único, pues lo es en cada abierto afín. Diremos que p es el punto genérico de X. Si un esquema X es íntegro y $g \in X$ es el punto genérico, llamaremos cuerpo de funciones de X a $\mathcal{O}_{X,g}$, y coincide con el cuerpo de fracciones del anillo de funciones de cualquier abierto afín. Denotaremos $\Sigma_X = \mathcal{O}_{X,g}$.

9. Definición: Diremos que un esquema X es noetheriano si existe un recubrimiento finito de X por abiertos afines $U_i = \operatorname{Spec} A_i$, con A_i noetherianos.

Obsérvese que los esquemas noetherianos son espacios topológicos noetherianos.

10. Proposición: $(\operatorname{Spec} A, \widetilde{A})$ *es noetheriano si y solo si A es un anillo noetheriano.*

Demostración. Si $(\operatorname{Spec} A, \widetilde{A})$ es noetheriano, sea $\{U_i = \operatorname{Spec} A_i\}$ un recubrimiento abierto finito de $\operatorname{Spec} A$, con A_i noetherianos. Sea $I_1 \subseteq \cdots \subseteq I_n \subseteq \ldots$ una cadena de ideales de A. La restricción de esta cadena a cada abierto U_i define una cadena de ideales de A_i, que estabiliza a partir de un n_i. Si n es el máximo de los n_i, la cadena de ideales de partida estabiliza a partir de n, porque así sucede localmente. En conclusión, A es noetheriano. □

11. Definición: Diremos que un esquema es localmente noetheriano si admite un recubrimiento (finito o no) por abiertos afines noetherianos.

12. Definición: Los morfismos de esquemas son los morfismos como espacios anillados en anillos locales.

El teorema 11.1.12 junto con la proposición 11.1.13 dice que la categoría de esquemas afines es equivalente a la categoría de anillos.

13. Definición: Diremos que un morfismo de esquemas $f: X \to Y$ es un morfismo afín si existe un recubrimiento de Y por abiertos afines U_i tales que $f^{-1}(U_i)$ son abiertos afines de X.

14. Lema: *Sea X un esquema. Para cada $f \in \Gamma(X,\mathcal{O}_X)$ denotemos X_f el abierto de X formado por los puntos donde f no se anula (es decir, f_x no pertenece al ideal maximal de $\mathcal{O}_{X,x}$). Si $(f_1,\dots,f_n) = \Gamma(X,\mathcal{O}_X)$ y los X_{f_i} son afines, entonces X es un esquema afín.*

Demostración. Observemos que $\cap_i (f_i)_0 = (f_1,\dots,f_n)_0 = \emptyset$, luego $\cup_i X_{f_i} = X$.

$X_{f_j} = \operatorname{Spec}\mathcal{O}(X_{f_j})$ es afín y $X_{f_j} \cap X_{f_i} = X_{f_j} - (f_i)_0$, luego

$$\mathcal{O}(X_{f_j} \cap X_{f_i}) = \mathcal{O}(X_{f_j})_{f_i}.$$

$X_{f_k} \cap X_{f_j} = X_{f_k} - (f_j)_0$ es afín y $X_{f_k} \cap X_{f_j} \cap X_{f_i} = X_{f_k} \cap X_{f_j} - (f_i)_0$, luego

$$\mathcal{O}(X_{f_k} \cap X_{f_j} \cap X_{f_i}) = \mathcal{O}(X_{f_k} \cap X_{f_j})_{f_i}.$$

Consideremos la sucesión exacta

$$0 \to \mathcal{O}(X) \to \prod_j \mathcal{O}(X_{f_j}) \rightrightarrows \prod_{j,k} \mathcal{O}(X_{f_j} \cap X_{f_k}).$$

Tensando por $\otimes_{\mathcal{O}(X)} \mathcal{O}(X)_{f_i}$, obtenemos la sucesión exacta

$$0 \to \mathcal{O}(X)_{f_i} \to \prod_i \mathcal{O}(X_{f_j} \cap X_{f_i}) \rightrightarrows \prod_{i,j,k} \mathcal{O}(X_{f_k} \cap X_{f_j} \cap X_{f_i}),$$

que muestra que $\mathcal{O}(X_{f_i}) = \mathcal{O}(X)_{f_i}$ y $X_{f_i} = \operatorname{Spec}\mathcal{O}(X_{f_i}) = \operatorname{Spec}\mathcal{O}(X)_{f_i} = \operatorname{Spec}\mathcal{O}(X) - (f_i)_0$.

Por tanto, el morfismo de espacios anillados natural $X \xrightarrow{\pi} X_{af} = \operatorname{Spec}\mathcal{O}(X)$ es topológicamente un homeomorfismo (con abuso de notación diremos que es la identidad) y el morfismo $\widetilde{\mathcal{O}(X)} \to \mathcal{O}_X$ es un isomorfismo porque dado $x \in X_{f_i} = \operatorname{Spec}\mathcal{O}(X)_{f_i}$ tenemos que

$$\mathcal{O}(X)_x = \mathcal{O}(X)_{f_i,x} = \mathcal{O}(X_{f_i})_x = \mathcal{O}_{X,x}.$$

□

15. Proposición: *Si un morfismo de esquemas es afín, entonces la antimagen de todo abierto afín es afín.*

Demostración. Sea $f: X \to Y$ el morfismo de esquemas afín y $\{U_i\}$ un recubrimiento de Y por abiertos afines, tales que $f^{-1}(U_i)$ sean afines.

Es fácil ver que si $a \in \mathcal{O}(Y)$ entonces $f^{-1}(Y_a) = X_{f^*(a)}$ (donde $f^*: \mathcal{O}(Y) \to \mathcal{O}(X)$ es el morfismo estructural entre los anillos de funciones). Por tanto, la antimagen de todo abierto básico de U_i es afín porque es un abierto básico de $f^{-1}(U_i)$.

Sea Z un esquema afín y Z_a un abierto básico. Si $V \subseteq Z_a$ es un abierto básico de Z_a entonces es un abierto básico de Z. Si $V \subseteq Z$ es un abierto afín que contiene a Z_a, entonces Z_a es un abierto básico de V: $Z_a = V_{a_{|V}}$.

Sea $U \subseteq Y$ un abierto afín. Dado $y \in U$ sea U_i tal que $y \in U_i$. Existe un abierto básico U_a de U tal que $y \in U_a \subset U_i$. Sea U_y un abierto básico de U_i tal que $y \in U_y \subset U_a$, entonces U_y es un abierto básico de U_a, entonces lo es de U. Sean $y_1, \ldots, y_n \in U$ tales que $U_{y_1} \cup \cdots \cup U_{y_n} = U$. Entonces, $f^1(U) = \cup_i f^{-1}(U_{y_i})$, $f^{-1}(U_{y_i})$ es un abierto afín porque U_{y_i} es un abierto básico de algún U_j, y $f^{-1}(U_{y_i}) = f^{-1}(U)_{f_i}$ para algún $f_i \in \mathcal{O}(f^{-1}(U))$, porque U_{y_i} es un abierto básico de U. Por el lema 11.2.14, $f^{-1}(U)$ es afín.

□

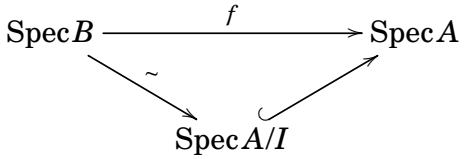
16. Corolario: *La intersección de dos abiertos afines de un esquema afín es afín.*

11.3. Subesquemas

1. Definición: Diremos que un morfismo de esquemas $f: Y \to X$ es una inmersión cerrada, si f como morfismo topológico es una inmersión cerrada (i.e. Y es homeomorfo a $f(Y)$ y éste es un cerrado de X) y los morfismos $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ son epiyectivos, para todo $y \in Y$. Se dice también que Y es un subesquema cerrado de X.

2. Ejemplo: Sea $I \subset A$ un ideal y $A \to A/I$ el morfismo de paso al cociente. El morfismo natural $\operatorname{Spec} A/I \to \operatorname{Spec} A$ es una inmersión cerrada.

3. Proposición: *Sea $f: \operatorname{Spec} B \to \operatorname{Spec} A$ una inmersión cerrada e $I \subset A$ el núcleo del morfismo $f^*: A \to B$ definido por f. Entonces, $A/I \simeq B$, $\bar{a} \mapsto f^*(a)$ y se tiene el diagrama conmutativo*



Demostración. Veamos que el morfismo $A \to B$ inducido por f, es epiyectivo: En efecto, $0 = (f_*\tilde{B})_x = B_x$, para todo $x \in \operatorname{Spec} A \setminus f(\operatorname{Spec} B)$ y $(f_*\tilde{B})_{f(y)} = B_y$, para todo $y \in \operatorname{Spec} B$, luego $A \to B$ es epiyectivo porque localmente lo es. Por tanto, $A/I \simeq B$. □

4. Proposición: *Si $f : Y \to X$ es una inmersión cerrada entonces f es un morfismo afín.*

Demostración. Podemos suponer que $X = \operatorname{Spec} A$ es afín. Si $x \in X \setminus f(Y)$, entonces la antimagen de cualquier abierto afín contenido en $X \setminus f(Y)$ y que contiene a x, es vacía, luego afín. Si $x = f(y)$, sea $V = \operatorname{Spec} B$ un abierto afín de Y que contiene a y. Sea $U_a = X \setminus (a)_0$ un abierto básico que contenga a x y tal que $f^{-1}(U_a) \subset V$. Si denotamos por $f^*(a)$ la imagen de a por el morfismo $\mathcal{O}_X(X) \to f_*\mathcal{O}_Y(X) = \mathcal{O}_Y(Y) \to \mathcal{O}_Y(V)$, se verifica que $f^{-1}(U_a) = V \setminus (f^*(a))_0 = \operatorname{Spec} B_{f^*(a)}$, que es afín. Por tanto, f es un morfismo afín. □

5. Observación: Todo cerrado C de un esquema X tiene una estructura natural de subesquema cerrado. Esta estructura es la siguiente: si X es afín, $X = \operatorname{Spec} A$, entonces se toma $\mathcal{O}_C = \widetilde{A/I}$, siendo I el ideal de A formado por las funciones que se anulan en todo punto de C. El caso general se hace por recollement (ver más adelante), recubriendo X por abiertos afines. Puede probarse que con esta estructura C es un subesquema cerrado y reducido de X.

6. Definición: Diremos que un morfismo de esquemas $f : Y \to X$ es una inmersión abierta, si $f(Y)$ es un abierto de X, e Y es un esquema isomorfo a $f(Y)$.

7. Definición: Diremos que un morfismo de esquemas $f : Y \to X$ es una inmersión de esquemas , si Y es homeomorfo a $f(Y)$ y éste es un cerrado de un abierto de X, y los morfismos $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ son epiyectivos, para todo $y \in Y$. Se dice también que Y es un subesquema de X.

Obviamente, toda inmersión de esquemas $f : Y \to X$ es la composición de una inmersión cerrada $Y \to U$ con una inmersión abierta $U \to X$.

11.4. Ejemplos de esquemas

11.4.1. Variedades algebraicas. Variedades proyectivas

En el capítulo 3 hemos definido el espectro proyectivo de un anillo graduado. Vamos a dotarlo ahora de estructura de esquema.

En Topología o en Geometría Diferencial, el morfismo natural de paso al cociente $\pi : \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ identifica el anillo de las funciones de $U \subset \mathbb{P}^n$ con el anillo de las

funciones de $\pi^{-1}(U) \subset \mathbb{A}^{n+1}$ que son constantes sobre cada recta de $\pi^{-1}(U) \cup \{0\}$ que pasa por el origen. En Geometría Algebraica, diremos que el haz de anillos de las funciones algebraicas de $\mathbb{A}^{n+1}$ constantes sobre cada recta que pasa por el origen es el haz de anillos de las funciones algebraicas de $\mathbb{P}^n$, y con este haz de anillos $\mathbb{P}^n$ será un esquema.

Dado un anillo graduado R, denotamos por R_0 los elementos de grado cero de R.

1. Definición: Sea R un anillo graduado. Para cada abierto U de $\operatorname{Proj} R$, denotemos R_U la localización de R por el sistema multiplicativo de las funciones homogéneas que no se anulan en ningún punto de U. Llamaremos haz de localizaciones homogéneas en $\operatorname{Proj} R$, y lo denotaremos $\widetilde{\widetilde{R}}$, al haz asociado al prehaz

$$U \rightsquigarrow [R_U]_0 := \left\{ \frac{f}{g} \in R_U \text{ con } f, g \in R \text{ homogéneas del mismo grado y } g \text{ no nula en ningún punto de } U. \right\}.$$

Sea $f \in R$ homogénea. Probemos que $R_{U_f^h} = R_f$: Sea S las funciones homogéneas que no se anulan en ningún punto de U_f^h y $S' := \{\frac{h}{f^m} \in R_f : \ m \in \mathbb{Z}, h \in S \text{ y } \operatorname{gr}(h) = \operatorname{gr}(f^m)\}$. Observemos que los elementos de S' no se anulan en ningún punto de $U_f^h = \operatorname{Proj} R_f = \operatorname{Spec}[R_f]_0$, luego son invertibles en R_f. Por lo tanto, $R_{U_f^h} = R_S = (R_f)_{S'} = R_f$.

2. Teorema: $(\operatorname{Proj} R, \widetilde{\widetilde{R}})$ *es un esquema.*

Demostración. Sea $f \in R_m$. Sabemos que $U_f^h = \operatorname{Proj} R \setminus (f)_0^h = \operatorname{Spec}[R_f]_0$. Denotemos $A := [R_f]_0$. Basta ver que $\widetilde{\widetilde{R}}_{|U_f^h} \simeq \widetilde{A}$. Basta ver que para toda $g \in R_{m'}$, las secciones del prehaz de localizaciones homogéneas sobre $U_f^h \cap U_g^h = U_{fg}^h$ coinciden con las secciones de $\widetilde{A}$ en $\operatorname{Spec} A \setminus (g^m/f^{m'})_0$. Cambiando g por g^m y f por $f^{m'}$, podemos suponer que $\operatorname{gr} g = \operatorname{gr} f$ y $(g^m/f^{m'})_0 = (g/f)_0$.

Obsérvese que $R_{U_{fg}^h} = R_{f \cdot g} = (R_f)_{g/f}$, luego

$$[R_{U_{fg}^h}]_0 = [(R_f)_{g/f}]_0 = ([R_f]_0)_{g/f} = A_{g/f}$$

que es lo que queríamos probar.

□

3. Definición: Sea k un anillo. Diremos que un esquema X es un k-esquema si se tiene prefijado un morfismo de esquemas $X \to \operatorname{Spec} k$, que se denomina morfismo estructural. Diremos que un k-esquema es una k-variedad algebraica si el morfismo

estructural $X \to \operatorname{Spec} k$ es de tipo finito, es decir, si existe un recubrimiento finito de X por abiertos afines $U_i = \operatorname{Spec} A_i$ de modo que los A_i son k-álgebras de tipo finito.

4. Ejemplos: 1. Las variedades algebraicas afines $X = \operatorname{Spec} k[\xi_1, \ldots, \xi_n]$ son variedades algebraicas. El esquema afín $\mathbb{A}^n_k = \operatorname{Spec} k[x_1, \ldots, x_n]$ se denomina espacio afín n-dimensional sobre el anillo k.

2. Sea $R = k[\xi_0, \ldots, \xi_n]$ una k-álgebra graduada (con $\operatorname{gr} \xi_i = 1$, para todo i). $(\operatorname{Proj} R, \widetilde{R})$ es una variedad algebraica. Este tipo de variedades se denominan variedades proyectivas (sobre k). El esquema $\mathbb{P}^n_k = \operatorname{Proj} k[x_0, \ldots, x_n]$ se denomina espacio proyectivo n-dimensional sobre el anillo k.

5. Definición: Sea X una variedad algebraica íntegra (sobre un cuerpo k) y sea $\mathcal{O}_v$ un anillo de valoración de Σ_X. Diremos que $\mathcal{O}_v$ es trivial sobre k si $k \subset \mathcal{O}_v$. Diremos que $\mathcal{O}_v$ centra en un punto $x \in X$ si $\mathcal{O}_{X,x} \subseteq \mathcal{O}_v$ y el morfismo es dominante.

6. Definición: Diremos que una variedad algebraica íntegra es completa si todo anillo de valoración de su cuerpo de funciones, trivial sobre k, tiene centro en un único punto de la variedad.

7. Teorema: *Las variedades proyectivas e íntegras son completas.*

Demostración. Sea $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ una variedad proyectiva íntegra. Sea $\mathcal{O}_v \subseteq \Sigma_X$ un anillo de valoración trivial sobre k.

Sea $\frac{\xi_i}{\xi_j} \in \Sigma_X$ la función de valor máximo para todo $i, j \in \{0, \ldots, n\}$. Se verifica que $k[\frac{\xi_0}{\xi_j}, \ldots, \frac{\xi_n}{\xi_j}] \subset \mathcal{O}_v$, porque si $v(\frac{\xi_r}{\xi_j}) < 0$ para algún r, entonces

$$v(\frac{\xi_i}{\xi_j}) < v(\frac{\xi_i}{\xi_j}) + v(\frac{\xi_j}{\xi_r}) = v(\frac{\xi_i}{\xi_j} \cdot \frac{\xi_j}{\xi_r}) = v(\frac{\xi_i}{\xi_r}),$$

que contradice la elección de $\frac{\xi_i}{\xi_j}$. Así pues, $\mathcal{O}_v$ centra en el punto x, donde $\mathfrak{p}_x$ es el corte del ideal de valoración $\mathfrak{p}_V$ con $k[\frac{\xi_0}{\xi_j}, \ldots, \frac{\xi_n}{\xi_j}]$.

Por último, dado un punto $y \neq x$, existe un abierto afín que contiene a x e y, luego el anillo de valoración que centra en x no puede centrar en y.

□

8. Definición: Llamaremos dimensión de un esquema X a la máxima longitud de las cadenas de cerrados irreducibles de X.

9. Proposición: *Si X es una variedad algebraica íntegra entonces la dimensión de X coincide con el grado de trascendencia de su cuerpo de funciones.*

Demostración. Por el teorema 3.5.2, todos los abiertos afines (no vacíos) tienen dimensión el grado de trascendencia el cuerpo de fracciones de X. La dimensión de X es igual a la dimensión de alguno de sus abiertos afines. □

10. Definición: Diremos que una variedad algebraica (sobre un cuerpo k) es una curva si es de dimensión 1.

11. Ejercicio: Demuéstrese que toda curva afín menos un número finito de puntos cerrados es afín.

12. Proposición: *Sea C una curva proyectiva, íntegra y no singular (es decir, $\mathcal{O}_{X,x}$ es un anillo regular para todo punto cerrado $x \in X$). Existe una correspondencia biunívoca entre los puntos de C y los anillos de valoración de Σ_C triviales sobre k.*

Demostración. En el teorema anterior hemos visto que todo anillo de valoración $k \subset \mathcal{O}_v \subseteq \Sigma_C$ centra en un único punto $x \in C$, es decir, $\mathcal{O}_{C,x} \subseteq \mathcal{O}_v$ (y $\mathfrak{p}_x \subseteq \mathfrak{p}_v$). Si x es un punto cerrado, entonces $\mathcal{O}_{C,x}$ es un anillo local regular de dimensión 1, luego es de valoración y $\mathcal{O}_{C,x} = \mathcal{O}_v$. Si es el punto genérico, entonces $\mathcal{O}_{X,x} = \Sigma_C$, que es el anillo de valoración trivial. □

13. Observación: Los anillos de valoración $\mathcal{O}_v$ de la proposición anterior son anillos de valoración discreta.

11.4.2. Variedad de Riemann

Sea k un cuerpo y $k \to \Sigma$ una extensión de cuerpos de tipo finito de grado de trascendencia 1, es decir, existe $t \in \Sigma$ trascendente sobre k tal que $k(t) \to \Sigma$ es una extensión finita.

14. Definición: Llamaremos variedad de Riemann de Σ al espacio anillado $(X, \mathcal{O}_X)$, donde

1. X es el conjunto de anillos de valoración de Σ triviales sobre k, dotado de la siguiente topología: los cerrados propios son los subconjuntos finitos de X que no contienen al anillo de valoración Σ (que será, por tanto, el punto genérico de X).
2. $\mathcal{O}_X$ es el haz de anillos definido por $\mathcal{O}_X(U) = \bigcap_{v \in U} \mathcal{O}_v$, para cada abierto $U \subseteq X$.

15. Teorema: *La variedad de Riemann de Σ es una curva completa y no singular sobre k cuyo cuerpo de funciones es Σ.*

Demostración. Sea $t \in \Sigma$ trascendente. Sea U el conjunto de anillos de valoración que contienen a t y U' el conjunto de anillos de valoración que contienen a t^{-1}. Entonces $X = U \cup U'$. Sea B el cierre entero de $k[t]$ en Σ y B' el cierre entero de $k[t^{-1}]$ en Σ. Se verifica que $U = \mathrm{Spec} B$ (y análogamente $U' = \mathrm{Spec} B'$): En efecto, B es un anillo íntegramente cerrado en Σ, de dimensión 1 (pues el morfismo $k[t] \to B$ es finito) y su cuerpo de fracciones es Σ (porque es íntegramente cerrado en Σ y contiene a $k(t)$). Por tanto, dado $x \in \mathrm{Spec} B$, B_x es un anillo de valoración (discreta) que contiene a t. Recíprocamente, dado un anillo de valoración $\mathcal{O}_v$ que contenga a t, tendremos que $B \hookrightarrow \mathcal{O}_v$ (pues B es la intersección de los anillos de valoración que contienen a $k[t]$). Por tanto, si $\mathfrak{p}_x = B \cap \mathfrak{p}_v$ (donde $\mathfrak{p}_v$ es el ideal de valoración de $\mathcal{O}_v$), tendremos que $B_x = \mathcal{O}_v$, porque B_x es de valoración y los anillos de valoración no admiten morfismos dominantes. Por último, la topología de $\mathrm{Spec} B$ coincide con la de U por ser B un anillo de dimensión 1.

U es un abierto de la variedad de Riemann (y análogamente U'): En efecto, el conjunto de los anillos de valoración de Σ que no contienen a t, es igual al conjunto de los anillos de valoración de Σ cuyo ideal de valoración contiene a t^{-1}, es decir, es igual a $(t^{-1})_0 \subset \mathrm{Spec} B'$, que es un conjunto finito (que no contiene el punto genérico) porque B' es de dimensión 1.

La restricción de $\mathcal{O}_X$ a U (análogamente para U') coincide con $\widetilde{B}$, porque por ser B íntegro se verifica que $\widetilde{B}(V) = \bigcap_{x \in V} B_x = \mathcal{O}_X(V)$ (problema 1 de la sección 11.7).

Por último, X es completa: si $\mathcal{O}_v$ es un anillo de valoración, entonces contiene a t (o a t^{-1}), y por tanto contiene a B (o a B') y $\mathcal{O}_v = B_x$, donde $x \in U$ es la valoración correspondiente a v.

Con todo, X es la unión de los dos abiertos U, U', que son esquemas afines no singulares de cuerpo de funciones Σ y toda valoración centra en un punto y solo uno de $U \cup U'$.

□

16. Ejercicio: La variedad de Riemann de $k(x)$ es la recta proyectiva $\mathbb{P}^1_k$.

17. Definición: Un morfismo entre esquemas íntegros se dice birracional si manda el punto genérico al punto genérico y el morfismo inducido entre los cuerpos de fracciones es un isomorfismo.

Obsérvese que el cuerpo de funciones de toda curva íntegra es una extensión de tipo finito de grado de trascendencia 1.

18. Definición: Un morfismo de esquemas $f : X \to Y$ se dice que es finito, si existe un recubrimiento por abiertos afines de Y, $\{U_i = \mathrm{Spec} A_i\}$ de modo que $f^{-1}(U_i) = \mathrm{Spec} B_i$

es afín y $A_i \to B_i$ es un morfismo de anillos finito, para todo i.[2]

19. Teorema: *Sea C una curva completa sobre un cuerpo k. Sea Σ el cuerpo de funciones de C y $\bar{C}$ la variedad de Riemann de Σ. Existe un epimorfismo finito y birracional $\pi\colon \bar{C} \to C$, que es isomorfismo si y solo si C es no singular. Se dice que $\bar{C}$ es la desingularización de C.*

Demostración. Se define $\pi\colon \bar{C} \to C$ como sigue: $\pi(v)$ es el centro del anillo valoración $\mathcal{O}_v$ en C. Sea U un abierto afín de C y sea $k[t] \to \mathcal{O}_C(U)$ un morfismo finito (existe por el lema de normalización de Noether). Si B es el cierre entero de $k[t]$ (o $\mathcal{O}_C(U)$) en Σ_C, entonces $\pi^{-1}(U) = \operatorname{Spec} B$. En efecto, $\operatorname{Spec} B$ se identifica con los anillos de valoración que dominan a $\mathcal{O}_C(U)$ (o a $k[t]$), que se identifica con los anillos de valoración que centran en U, es decir, con $\pi^{-1}(U)$. Recordando la construcción de los abiertos afines por los que recubríamos la variedad de Riemann, concluimos que $\pi^{-1}(U) = \operatorname{Spec} B$ es un abierto, luego π es continua. Es claro, además, que el morfismo $\pi^{-1}(U) \xrightarrow{\pi} U$ es el inducido por la inclusión $\mathcal{O}_C(U) \to B$.

El morfismo definido entre los haces de anillos es el inducido por las inclusiones naturales

$$\mathcal{O}_C(V) \hookrightarrow \mathcal{O}_{\bar{C}}(\pi^{-1}(V)) = \bigcap_{v \in \pi^{-1}(V)} \mathcal{O}_v$$

Por tanto, tenemos definido un morfismo de esquemas $\pi\colon \bar{C} \to C$, que cumple las condiciones del teorema, como se comprueba afínmente con $\pi^{-1}(U) \xrightarrow{\pi} U$. □

20. Teorema: *La categoría de las curvas completas no singulares sobre un cuerpo k (cuyos morfismos no sean constantes), es equivalente (contravariantemente) a la categoría de las extensiones de cuerpos de tipo finito de k de grado de trascendencia* 1.

Demostración. Sea F el funtor que asigna a cada curva C su cuerpo de funciones Σ_C. Dado un morfismo $f : C \to C'$ no constante (es decir, f aplica el punto genérico g de C en el punto genérico g' de C') tenemos definido un morfismo $\Sigma_{C'} = \mathcal{O}_{C',g'} \to \mathcal{O}_{C,g} = \Sigma_C$, que es por definición $F(f)$. Obviamente, $F(f \circ g) = F(g) \circ F(f)$.

Sea G el funtor que asigna a cada extensión $k \to \Sigma$ de grado de trascendencia 1 su variedad de Riemann V. Dado un morfismo $i\colon \Sigma \to \Sigma'$, sea $G(i)\colon V' \to V$ el morfismo definido entre las variedades de Riemann de Σ' y Σ, del siguiente modo:

- Entre los espacios topológicos, $G(i)(v') = v$, siendo $\mathcal{O}_v = \Sigma \cap \mathcal{O}_{v'}$. Dado $t \in \Sigma$, sea B el cierre entero de $k[t]$ en Σ y B' el cierre entero de B (o $k[t]$) en Σ'. Sean $U = \operatorname{Spec} B$ y $U' = \operatorname{Spec} B'$, que son abiertos de V y V'. Se verifica que $G(i)^{-1}(U) = U'$ y $G(i)_{|U'}$ es el morfismo entre espectros inducido por la inclusión $B \hookrightarrow B'$.

[2] En particular, los morfismos finitos son afines. Más adelante probaremos que para todo abierto afín $U \subseteq Y$, el morfismo de anillos $\mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$ es finito.

- El morfismo entre los haces de anillos es el siguiente: para cada abierto W de V, las inclusiones $\mathcal{O}_V(W) = \bigcap_{v\in W} \mathcal{O}_v \hookrightarrow \bigcap_{v'\in G(i)^{-1}(W)} \mathcal{O}_{v'}$ inducen un morfismo $\mathcal{O}_V \to G(i)_*\mathcal{O}_{V'}$. De nuevo, el morfismo de espacios anillados definido sobre U' es el inducido por el morfismo de anillos $B \hookrightarrow B'$.

Para terminar, tenemos que ver que $G \circ F \simeq \mathrm{Id}$ y $F \circ G \simeq \mathrm{Id}$. El primero es consecuencia del teorema 11.4.19 y el segundo del teorema 11.4.15. □

21. Corolario: *Sea C una curva completa y no singular sobre un cuerpo k. Existe una correspondencia biunívoca entre los morfismos no constantes $C \to \mathbb{P}^1$ y los elementos de Σ_C trascendentes sobre k.*

22. Ejercicio: Dado un morfismo no constante $\pi\colon C' \to C$ entre curvas completas no singulares, demuestra que el número de puntos de las fibras es constante y coincide con el grado entre los cuerpos de funciones.

Solución: Como π es un morfismo afín, se reduce a la proposición 3.8.10.

23. Ejemplo: Sea Σ el cuerpo de funciones de una curva C completa y no singular, y sea $f \in \Sigma_C$ trascendente sobre k. Consideremos el morfismo inducido

$$\widetilde{f}\colon C \to \mathbb{P}^1$$

Sea $U = \mathrm{Spec}\, k[x]$, abierto de $\mathbb{P}^1$. El morfismo $\widetilde{f}^{-1}(U) \xrightarrow{\widetilde{f}} U$ es el inducido entre espectros por el morfismo de anillos $k[x] \hookrightarrow \overline{k[x]}$, $x \mapsto f$, (siendo $\overline{k[x]}$ el cierre entero de $k[x]$ en Σ). Sea $\mathfrak{m}_\alpha \subset \overline{k[x]}$ un ideal maximal racional y denotemos $f(\alpha)$ la clase de f en $\overline{k[x]}/\mathfrak{m}_\alpha = k$. Es fácil comprobar que $\mathfrak{m}_\alpha \cap k[x] = (x - f(\alpha)) = \mathfrak{m}_{f(\alpha)}$. Por tanto, $\widetilde{f}(\alpha) = f(\alpha)$. Por otra parte, $\widetilde{f}^{-1}(0) = \mathrm{Spec}\, \overline{k[x]}/f \cdot \overline{k[x]}$. Por tanto, si $f \cdot \overline{k[x]} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, entonces $\widetilde{f}^{-1}(0) = \{x_1, \ldots, x_r\}$ y el número de puntos de la fibra de 0 es $\sum_i n_i \,\mathrm{gr}\, x_i$.

11.4.3. Recollement de esquemas

Recollement de espacios topológicos

Sea X un espacio topológico. Es muy frecuente estudiar la estructura de X a partir de un recubrimiento por abiertos X_i. Por ejemplo, en el estudio de la superficie terrestre, se construyen una colección de mapas locales, y se hacen las identificaciones pertinentes donde dos mapas se solapen. A partir de los mapas y de las identificaciones reconstruimos la superficie terrestre. La formalización de este proceso para un espacio topológico arbitrario se denomina recollement.

24. Definición: Llamaremos datos de construcción a dar lo siguiente:

1. Una familia $\{X_i\}$ de espacios topológicos.
2. Un recubrimiento de cada X_i por abiertos X_{ij}.
3. Una familia de homeomorfismos $\theta_{ij}\colon X_{ij} \to X_{ji}$ tales que:
   a) $\theta_{ij} = \theta_{ji}^{-1}$ y $\theta_{ii} = \mathrm{Id}$.
   b) Para cualesquiera i,j,k se verifica $\theta_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$ y se tiene un diagrama conmutativo:

$$\begin{array}{ccc} X_{ij} \cap X_{ik} & \xrightarrow{\theta_{ij}} & X_{ji} \cap X_{jk} \\ & {\scriptstyle \theta_{ik}} \searrow \quad \swarrow {\scriptstyle \theta_{jk}} & \\ & X_{kj} \cap X_{ki} & \end{array}$$

   Es decir, se cumple la condición de "cociclo" $\theta_{jk} \circ \theta_{ij} = \theta_{ik}$.[3]

25. Definición: Unos datos de construcción $\{X_i, \theta_{ij}\}$ se dicen efectivos si existen un espacio topológico X, un recubrimiento abierto $X = \bigcup_i U_i$ y homeomorfismos $g_i\colon U_i \simeq X_i$ de modo que $g_i^{-1}(X_{ij}) = U_i \cap U_j$ y $\theta_{ij} = g_j \circ g_i^{-1}$ sobre $U_i \cap U_j$. Se dice que X es un descenso de los datos de construcción.

26. Teorema: *Todo dato de construcción es efectivo y los descensos son únicos salvo isomorfismos.*

Demostración. Sea $\{X_i, \theta_{ij}\}$ unos datos de construcción. Cada X_{ij} tiene un morfismo a X_i (la inclusión) y otro a X_j (la composición de θ_{ij} con la inclusión). Por tanto tenemos dos morfismos

$$\coprod_{i,j} X_{ij} \underset{\theta}{\overset{\mathrm{id}}{\rightrightarrows}} \coprod_i X_i$$

Definimos X como el conúcleo de (id, θ), es decir, X es el cociente (topológico) de $\coprod_i X_i$ por la siguiente relación: dados $x_i \in X_i$ y $x_j \in X_j$, diremos que $x_i \sim x_j$ si $x_j = \theta_{ij}(x_j)$, que es una relación de equivalencia por la condición de cociclo.

La composición de los morfismos naturales $X_i \hookrightarrow \coprod_i X_i \to X$ es una inmersión abierta cuya imagen denotamos por U_i. Si denotamos g_i al homeomorfismo $U_i \simeq X_i$, es

[3] Puede comprobarse que (b) implica (a).

inmediato comprobar que $g_i^{-1}(X_{ij}) = U_i \cap U_j$ y $\theta_{ij} = g_j \circ g_i^{-1}$ sobre $U_i \cap U_j$. Por tanto, X es un descenso y el dato de construcción es efectivo.

Sea $X' = \underset{i}{\cup} U'_i$ otro descenso, con homeomorfismos $g'_i : U'_i \simeq X_i$, tales que ${g'_i}^{-1}(X_{ij}) = U'_i \cap U'_j$ y $\theta_{ij} = g'_j \circ {g'_i}^{-1}$ sobre $U'_i \cap U'_j$. Se tiene un diagrama conmutativo (compruébese)

$$\begin{array}{ccccc} \coprod_{i,j} X_{ij} & \overset{\text{id}}{\underset{\theta}{\rightrightarrows}} & \coprod_i X_i & \longrightarrow & X \\ \uparrow{\scriptstyle \coprod_{i,j} g'_i} & & \uparrow{\scriptstyle \coprod_i g'_i} & & \\ \coprod_{i,j} U'_i \cap U'_j & \rightrightarrows & \coprod_i U'_i & \longrightarrow & X' \end{array}$$

cuyas flechas verticales son homeomorfismos, luego induce un homeomorfismo $X' \simeq X$. □

Recollement de esquemas

El recollement de haces puede ser entendido esencialmente como un caso particular del recollement de espacios topológicos, sin más que considerar, en vez de los haces, los espacios étale asociados. Puede verse después que, en la categoría de los haces, el recollement "deja estable" las subcategorías de los espacios anillados, y la de esquemas. Podríamos así desarrollar esta sección. Sin embargo, para la comprensión de la teoría del descenso fielmente plano, que más adelante estudiaremos, conviene proceder de otro modo, igualmente natural.

27. Definición: Unos datos de construcción, en la categoría de esquemas, es dar

1. Una familia de esquemas $(X_i, \mathcal{O}_{X_i})$.
2. Un recubrimiento abierto $X_i = \underset{j}{\cup} X_{ij}$ de cada X_i.
3. Una familia de isomorfismos de esquemas $\theta_{ij} : X_{ij} \to X_{ji}$ tales que
   a) $\theta_{ij} = \theta_{ji}^{-1}$ y $\theta_{ii} = \mathrm{Id}$.
   b) Para cualesquiera i, j, k se verifica $\theta_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$ y se tiene un diagrama conmutativo:

$$\begin{array}{ccc} X_{ij} \cap X_{ik} & \xrightarrow{\theta_{ij}} & X_{ji} \cap X_{jk} \\ & {\scriptstyle \theta_{ik}} \searrow \quad \swarrow {\scriptstyle \theta_{jk}} & \\ & X_{kj} \cap X_{ki} & \end{array}$$

   Es decir, se cumple la condición de "cociclo" $\theta_{jk} \circ \theta_{ij} = \theta_{ik}$.

28. Definición: Unos datos de construcción $\{X_i, \theta_{ij}\}$ se dicen efectivos si existen un esquema X, un recubrimiento abierto $X = \bigcup_i U_i$ y unos isomorfismos de esquemas $g_i : U_i \simeq X_i$, de modo que $g_i^{-1}(X_{ij}) = U_i \cap U_j$ y $\theta_{ij} \circ g_i = g_j$ sobre $U_i \cap U_j$. Se dice que X es un descenso de los datos de construcción.

29. Teorema: *Todo dato de construcción es efectivo y los descensos son únicos salvo isomorfismos de esquemas.*

Demostración. Repetimos la misma demostración que en el caso topológico. Definimos la unión disjunta de dos esquemas X e Y como el esquema cuyo espacio topológico subyacente es $X \coprod Y$ (con la topología inicial de las inclusiones $X \to X \coprod Y$ e $Y \to X \coprod Y$) y cuyo haz de anillos es $\mathscr{O}_{X \coprod Y}(U) = \mathscr{O}_X(X \cap U) \times \mathscr{O}_Y(Y \cap U)$.

Sea $\{X_i, \theta_{ij}\}$ unos datos de construcción. Cada X_{ij} tiene un morfismo a X_i (la inclusión) y otro a X_j (la composición de θ_{ij} con la inclusión). Por tanto tenemos dos morfismos

$$\coprod_{i,j} X_{ij} \underset{\theta}{\overset{\mathrm{id}}{\rightrightarrows}} \coprod_i X_i$$

Definimos X como el conúcleo de (id, θ), es decir:

- El espacio topológico X es el conúcleo (topológico) de las aplicaciones continuas (id, θ). Se tienen entonces inmersiones abiertas $X_i \to X$.

- El haz estructural $\mathscr{O}_X$ se define de la siguiente manera: para cada abierto $V \subset X$, sea $V_i = V \cap X_i$ y $V_{ij} = V \cap X_{ij}$; definimos $\mathscr{O}_X(V)$ como el núcleo de los morfismos

$$\prod_i \mathscr{O}_{X_i}(V_i) \rightrightarrows \prod_{i,j} \mathscr{O}_{X_{ij}}(V_{ij})$$

inducidos por $\coprod_{i,j} X_{ij} \underset{\theta}{\overset{\mathrm{id}}{\rightrightarrows}} \coprod_i X_i$.

Se tienen morfismos naturales de esquemas $X_i \to X$ que son inmersiones abiertas y cuyas imágenes denotamos por U_i. Se tiene un isomorfismo de esquemas (compruébese) $g_i : U_i \simeq X_i$, y es inmediato comprobar que $g_i^{-1}(X_{ij}) = U_i \cap U_j$ y $\theta_{ij} = g_j \circ g_i^{-1}$ sobre $U_i \cap U_j$. Por tanto, X es un descenso y el dato de construcción es efectivo.

Sea $X' = \bigcup_i U_i'$ otro descenso, con isomorfismos $g_i' : U_i' \simeq X_i$, tales que ${g_i'}^{-1}(X_{ij}) = U_i' \cap U_j'$ y $\theta_{ij} = g_j' \circ {g_i'}^{-1}$ sobre $U_i' \cap U_j'$. Se tiene un diagrama conmutativo (compruébese)

$$\begin{array}{ccccc} \coprod_{i,j} X_{ij} & \overset{\text{id}}{\underset{\theta}{\rightrightarrows}} & \coprod_i X_i & \longrightarrow & X \\ \uparrow{\scriptstyle \coprod_{i,j} g'_i} & & \uparrow{\scriptstyle \coprod_i g'_i} & & \\ \coprod_{i,j} U'_i \cap U'_j & \rightrightarrows & \coprod_i U'_i & \longrightarrow & X' \end{array}$$

cuyas flechas verticales son isomorfismos, luego induce un isomorfismo de esquemas $X' \simeq X$: en efecto, el diagrama conmutativo induce un homeomorfismo $\phi\colon X' \simeq X$ y para todo abierto V de X se tiene un diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{O}_X(V) & \longrightarrow & \prod_i \mathcal{O}_{X_i}(V_i) & \rightrightarrows & \prod_{i,j} \mathcal{O}_{X_{ij}}(V_{ij}) \\ & & \downarrow & & \downarrow \\ \mathcal{O}_{X'}(V') & \longrightarrow & \prod_i \mathcal{O}_{X'}(V'_i) & \rightrightarrows & \prod_{i,j} \mathcal{O}_{X'}(V'_{ij}) \end{array}$$

donde $V' = \phi^{-1}(V)$, $V'_i = V' \cap U'_i$ y $V'_{ij} = V' \cap U'_i \cap U'_j$, y cuyas flechas verticales son isomorfismos, luego define un isomorfismo entre los núcleos $\mathcal{O}_X(V) \to \mathcal{O}_{X'}(V')$, y por tanto un isomorfismo de haces $\mathcal{O}_X \to \phi_* \mathcal{O}_{X'}$. □

30. Ejemplo: Podemos construir $\mathbb{P}^n$ como un recollement de esquemas. Sea $A^i = k[\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}]$, $X_i = \operatorname{Spec} A^i$ y $X_{ij} = X_i \setminus (\frac{x_j}{x_i})_0 = \operatorname{Spec} A^i_{x_j/x_i}$. Sea $\theta_{ij}\colon X_{ij} \to X_{ji}$ el morfismo inducido por el morfismo de anillos

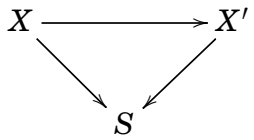
$$A^j_{x_i/x_j} \to A^i_{x_j/x_i}, \quad \frac{x_k}{x_j} \mapsto \frac{x_k/x_i}{x_j/x_i}$$

Entonces los θ_{ij} cumplen la condición de cociclo y el recollement de los X_i es $\mathbb{P}^n$.

11.5. Un teorema de construcción local de esquemas

Sea S un esquema.

1. Definición: Un esquema sobre S (o un S-esquema) es la pareja formada por un esquema X y un morfismo de esquemas $X \to S$. Si X, X' son dos S-esquemas sobre S, diremos que un morfismo de esquemas $X \to X'$ es un morfismo de S-esquemas si el diagrama



es conmutativo. Denotaremos por $\mathrm{Hom}_S(X,X')$ el conjunto de morfismos de S-esquemas de X en X'.

Los esquemas sobre S, con los morfismos de S-esquemas, forman una categoría que denotamos $\mathscr{C}_S$.

2. Ejemplo: Todo esquema es un esquema sobre $\mathrm{Spec}\,\mathbb{Z}$. Por tanto $\mathscr{C}_{\mathrm{Spec}\,\mathbb{Z}}$ es la categoría de esquemas.

Sea X un S-esquema y $X^{\cdot} = \mathrm{Hom}_S(-,X)$ el funtor contravariante de la categoría de S-esquemas en la categoría de conjuntos definido por

$$X^{\cdot}(Y) := \mathrm{Hom}_S(Y,X)$$

El funtor $X^{\cdot}$ se denomina funtor de puntos de X.

Sea $F\colon \mathscr{C}_S \to \mathscr{C}_{\mathrm{Conj}}$ un funtor contravariante. Un morfismo de funtores $\theta\colon X^{\cdot} \to F$, está determinado por $\theta(X)(\mathrm{Id}_X) \in F(X)$, como vimos en la demostración de 0.7.6. Es decir,

$$\mathrm{Hom}(X^{\cdot},F) = F(X)$$

En particular, tenemos el siguiente teorema.

3. Teorema: *Para cualesquiera S-esquemas X e Y se verifica*

$$\mathrm{Hom}(X^{\cdot},Y^{\cdot}) = \mathrm{Hom}_S(X,Y)$$

Además, $X^{\cdot} \simeq Y^{\cdot}$ si y solo si $X \simeq Y$ (isomorfismo de S-esquemas).

Con la noción de funtor de puntos podemos hablar de un esquema en términos de su "conjunto de puntos", y los morfismos de esquemas quedan reducidos a aplicaciones (funtoriales) entre conjuntos.

4. Definición: Se dice que un funtor contravariante $F\colon \mathscr{C}_S \to \mathscr{C}_{\mathrm{Conj}}$ es un haz (para la topología de Zariski) si verifica la condición de haz para todo S-esquema T; es decir, para todo recubrimiento de T por abiertos U_i la sucesión

$$F(T) \to \prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \cap U_j)$$

es exacta.

5. Ejercicio: Prueba que el funtor de puntos $X^\cdot$ de un S-esquema X es un haz. Utilícese esto, y la proposición 11.1.13 para probar que dar un morfismo de esquemas $X \to \operatorname{Spec} A$ equivale a dar un morfismo de anillos $A \to \Gamma(X, \mathscr{O}_X)$.

6. Definición: Se dice que un funtor contravariante $F\colon \mathscr{C}_S \to \mathscr{C}_{\mathrm{Conj}}$ es representable si existe un S-esquema X y un isomorfismo de funtores $X^\cdot \simeq F$.

7. Definición: Se dice que un morfismo de funtores contravariantes $F' \to F$ sobre la categoría de S-esquemas es una inmersión abierta si para todo S-esquema X y todo morfismo de funtores $X^\cdot \to F$, el funtor producto fibrado $F' \times_F X^\cdot$ es representable por un esquema X' y el morfismo $X' \to X$ deducido de la proyección $F' \times_F X^\cdot \to X^\cdot$ es una inmersión abierta.

8. Ejemplo: Si $U \hookrightarrow X$ es una inmersión abierta de S-esquemas, el morfismo inducido $U^\cdot \to X^\cdot$ es una inmersión abierta de funtores. En efecto, si Z es un S-esquema y $p\colon Z^\cdot \to X^\cdot$ es un morfismo de funtores, entonces $U^\cdot \times_{X^\cdot} Z^\cdot$ es representable por el abierto $p^{-1}(U)$ de Z.

9. Definición: Una familia de inmersiones abiertas de funtores $F_i \to F$ es un recubrimiento si para cada S-esquema X y cada morfismo de funtores $X^\cdot \to F$ las inmersiones abiertas $X_i \to X$ (deducidas de $X_i^\cdot = F_i \times_F X^\cdot \to X^\cdot$) son un recubrimiento de X.

10. Definición: Se dice que un funtor contravariante sobre la categoría de S-esquemas es localmente representable si tiene un recubrimiento por funtores representables.

11. Construcción local de esquemas: *Un funtor contravariante sobre la categoría de S-esquemas es representable si y solo si es un haz y es localmente representable.*

Demostración. Sea F un funtor contravariante sobre la categoría de S-esquemas, y $X_i^\cdot = F_i \to F$ un recubrimiento de F por funtores representables. Tenemos pues una familia de esquemas X_i, para cada X_j un recubrimiento X_{ij}, deducido de $F_i \times_F F_j \to F_j$, e isomorfismos $\theta_{ij}\colon X_{ij} \to X_{ji}$, deducidos de los isomorfismos naturales $F_i \times_F F_j = F_j \times_F F_i$. Obviamente los θ_{ij} verifican la condición de cociclo. El recollement de los X_i es un esquema X cuyo funtor de puntos es F: En efecto, un morfismo de funtores $T^\cdot \to F$ induce morfismos $T_i^\cdot = T^\cdot \times_F F_i \to F_i = X_i^\cdot \hookrightarrow X^\cdot$, que por ser $X^\cdot$ haz definen un morfismo $T^\cdot \to X^\cdot$. Recíprocamente, un morfismo $T^\cdot \to X^\cdot$ de funtores induce morfismos $T_i^\cdot = T^\cdot \times_{X^\cdot} X_i^\cdot \to X_i^\cdot = F_i \hookrightarrow F$, que por ser F haz define un morfismo $T^\cdot \to F$. En conclusión, $F(T) = X^\cdot(T)$.

□

12. Ejemplos: 1. Si $\{U_i\}$ es un recubrimiento abierto de X y F es un haz sobre X, entonces $F_{|U_i} := F \times_X U_i^\cdot$ es un recubrimiento de F. Por tanto, si los $F_{|U_i}$ son representables, F también.

2. *Producto directo de esquemas:* Sean X e Y dos esquemas sobre S. El funtor $X^\cdot \times_{S^\cdot} Y^\cdot$ es un haz. Veamos que es representable por un S-esquema, que denotaremos $X \times_S Y$.

Sea $S = \underset{i}{\cup} S_i$ un recubrimiento de S por abiertos afines. Denotemos $\pi_X : X \to S$, $\pi_Y : Y \to S$ los morfismos estructurales, $X_i = \pi_X^{-1}(S_i)$, $Y_i = \pi_Y^{-1}(S_i)$. Sean $X_i = \underset{j}{\cup} X_{ij}$, $Y_i = \underset{k}{\cup} Y_{ik}$ recubrimientos por abiertos afines de X_i e Y_i respectivamente. Entonces $X_{ij}^\cdot \times_{S_i^\cdot} Y_{ik}^\cdot \to X^\cdot \times_{S^\cdot} Y^\cdot$ es un recubrimiento de $X^\cdot \times_{S^\cdot} Y^\cdot$. Por el teorema anterior, basta probar que $X_{ij}^\cdot \times_{S_i^\cdot} Y_{ik}^\cdot$ son representables. Es decir, dadas dos A-álgebras B, C tenemos que ver que $(\operatorname{Spec} B)^\cdot \underset{(\operatorname{Spec} A)^\cdot}{\times} (\operatorname{Spec} C)^\cdot$ es representable. Denotemos $X = \operatorname{Spec} B$, $Y = \operatorname{Spec} C$, $T = \operatorname{Spec} A$. Entonces

$$\begin{aligned}(X^\cdot \times_{T^\cdot} Y^\cdot)(Z) &= \operatorname{Hom}_T(Z,X) \times \operatorname{Hom}_T(Z,Y) = \operatorname{Hom}_A(B, \mathscr{O}_Z(Z)) \times \operatorname{Hom}_A(C, \mathscr{O}_Z(Z)) \\ &= \operatorname{Hom}_A(B \otimes_A C, \mathscr{O}_Z(Z)) = \operatorname{Hom}_T(Z, \operatorname{Spec} B \otimes_A C) = (\operatorname{Spec} B \otimes_A C)^\cdot(Z)\end{aligned}$$

luego $(\operatorname{Spec} B)^\cdot \underset{(\operatorname{Spec} A)^\cdot}{\times} (\operatorname{Spec} C)^\cdot$ es representable por $\operatorname{Spec}(B \otimes_A C)$.

13. Ejercicio: 1. Sea $\pi : X \to S$ un morfismo de esquemas y $V \hookrightarrow S$ un abierto. Prueba que se tiene un isomorfismo de esquemas: $\pi^{-1}(V) = X \times_S V$. En particular, esto nos dice quién es el funtor de puntos de $\pi^{-1}(V)$.

2. Si V es un abierto de S y X, Y son esquemas sobre V, prueba que $X \times_V Y = X \times_S Y$.

11.6. Apéndice: Esquemas separados y propios

Es bien conocido en Topología que el espacio proyectivo $\mathbb{P}^n$ es un espacio topológico separado y compacto (el morfismo de $\mathbb{P}^n$ en un punto es propio). Vamos a ver que en Geometría Algebraica las variedades proyectivas son separadas (precisaremos más adelante este concepto) y compactas (propias). El hecho fundamental que vamos a usar para demostrar estas propiedades es que las variedades proyectivas son completas. Las variedades que sean completas serán, pues, separadas y propias.

1. Definición: Se dice que un morfismo $X \to Y$ es cerrado si la imagen de todo cerrado es cerrado. Se dice que es universalmente cerrado si para todo cambio de base $Y' \to Y$, el morfismo inducido $X \times_Y Y' \to Y'$ es cerrado.

2. Proposición: *Se cumple::*

1. *Las inmersiones cerradas son morfismos universalmente cerrados.*
2. *Los morfismos universalmente cerrados son estables por cambio de base.*
3. *La composición de dos morfismos universalmente cerrados es un morfismo universalmente cerrado.*
4. *Si $f: X \to Y$ y $f': X' \to Y'$ son morfismos universalmente cerrados de S-esquemas, entonces el morfismo $f \times f': X \times_S X' \to Y \times_S Y'$ es universalmente cerrado.*
5. *Un morfismo $f: X \to Y$ es universalmente cerrado si y solo si existe un recubrimiento de Y por abiertos U_i , tales que $f^{-1}(U_i) \to U_i$ es universalmente cerrado para todo i.*

Demostración. 4. $f \times f'$ es la composición de los morfismos $X \times_S X' \to Y \times_S X' \to Y \times_S Y'$, que son universalmente cerrados por 2. Se concluye por 3. □

3. Definición: Un morfismo de esquemas $X \to Y$ se dice quasi-compacto si la antimagen de todo abierto compacto es compacto.

4. Proposición: *Un morfismo de esquemas $\pi: X \to Y$ es quasi-compacto si y solo si existe un recubrimiento de Y por abiertos afines (que son compactos) cuyas antimágenes son compactos de X.*

Demostración. La condición necesaria de la proposición es obvia. Demostremos la condición suficiente. Sea $\{U_i\}$ un recubrimiento por abiertos afines de Y tales que $\pi^{-1}(U_i)$ sea compacto. Observemos que cada abierto $\pi^{-1}(U_i)$ es unión de un número finito de abiertos afines V_{ij}. Dado un abierto básico $U_a \subset U_i$ $\pi^{-1}(U_a) \cap V_{ij}$ es un abierto básico de V_{ij}. Luego $\pi^{-1}(U_a) = \cup_j(\pi^{-1}(U_a) \cap V_{ij})$ es unión de un número finito de abiertos afines. Dado un abierto compacto U de Y, es unión de un número finito de abiertos básicos de los U_i, luego $\pi^{-1}(U)$ es unión de un número finito de abiertos afines, luego es compacto. □

Los morfismos afines son quasi-compactos. Si X es un esquema noetheriano, todo morfismo $X \to Y$ es quasi-compacto, pues los abiertos de un espacio noetheriano son noetherianos. La composición de morfismos quasi-compactos es quasi-compacto. Los morfismos quasi-compactos $X \to Y$ son estables por cambio de la base Y.

5. Proposición: *Sea $\pi: X \to Y$ un morfismo quasi-compacto y $C \subset X$ un cerrado. Entonces, $\pi(C)$ contiene los puntos genéricos de $\overline{\pi(C)}$.*

Demostración. Si $f\colon \operatorname{Spec} A \to \operatorname{Spec} B$ es un morfismo de imagen densa, entonces $\operatorname{Im} f$ contiene los puntos genéricos de $\operatorname{Spec} B$: haciendo cociente por los nilpotentes en A y B, podemos suponer que el morfismo $B \to A$ es inyectivo; por la fórmula de la fibra es fácil ver que los puntos genéricos de $\operatorname{Spec} B$ tienen fibra no vacía.

El morfismo $\pi\colon C \to \overline{\pi(C)}$ es quasi-compacto. Por tanto, podemos suponer que $C = X$ y $\overline{\pi(C)} = Y$.

Para probar que $\pi(X)$ contiene los puntos genéricos de Y, podemos suponer, por cambio de base a abiertos afines, que Y es afín. En tal caso $X = \pi^{-1}(Y)$ es unión de un número finito de abiertos afines, $U_1, \ldots, U_n$. Sea f la composición de los morfismos naturales

$$U_1 \coprod \ldots \coprod U_n \to X \xrightarrow{\pi} Y$$

Observemos que f es un morfismo entre esquemas afines y es de imagen densa, pues $\operatorname{Im} f = \pi(X)$. Por tanto, $\pi(X) = \operatorname{Im} f$ contiene los puntos genéricos de Y. □

6. Lema: *Sea X un esquema. Si $\mathcal{O}$ es un anillo local, dar un morfismo de esquemas $\operatorname{Spec}\mathcal{O} \to X$ equivale a dar un punto $x \in X$ y un morfismo dominante $\mathcal{O}_{X,x} \to \mathcal{O}$. Si Σ es un cuerpo, dar un morfismo $\operatorname{Spec}\Sigma \to X$ equivale a dar un punto $x \in X$ y un morfismo inyectivo $k(x) \hookrightarrow \Sigma$, donde $k(x) = \mathcal{O}_{X,x}/\mathfrak{p}_x$ es el cuerpo residual de x.*

Demostración. Dado un morfismo $\mathcal{O}_{X,x} \to \mathcal{O}$, y un abierto U afín que contiene a x, tenemos un morfismo $\mathcal{O}_X(U) \to \mathcal{O}_{X,x} \to \mathcal{O}$. Por tanto, tenemos $\operatorname{Spec}\mathcal{O} \to U \subseteq X$. Recíprocamente, dado un morfismo $f\colon \operatorname{Spec}\mathcal{O} \to X$, sea y el punto cerrado de $\operatorname{Spec}\mathcal{O}$. Tenemos en fibras el morfismo dominante $\mathcal{O}_{X,f(y)} \to \mathcal{O}$. El resto es trivial. □

7. Criterio valorativo de morfismo universalmente cerrado: *Un morfismo quasi-compacto de esquemas $X \to Y$ es universalmente cerrado si y solo si cumple la siguiente condición: Para todo anillo de valoración $\mathcal{O}_v$ de cuerpo de fracciones Σ_v y todo diagrama conmutativo*

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & X \\ \downarrow{\scriptstyle i} & & \downarrow \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & Y \end{array}$$

donde i es el morfismo inducido por la inclusión $\mathcal{O}_v \hookrightarrow \Sigma_v$, existe un morfismo

$$f\colon \operatorname{Spec}\mathcal{O}_v \to X,$$

que añadido al diagrama anterior, hace los triángulos conmutativos.

Demostración. Supongamos $X \to Y$ universalmente cerrado y probemos la existencia de f. Cambiando la base Y por $\operatorname{Spec}\mathcal{O}_v$ podemos suponer que $Y = \operatorname{Spec}\mathcal{O}_v$. Tenemos el diagrama

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \xrightarrow{j} & X \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \pi} \\ \operatorname{Spec}\mathcal{O}_v & = & \operatorname{Spec}\mathcal{O}_v \end{array}$$

Sean g, v el punto genérico y el punto cerrado de $\operatorname{Spec}\mathcal{O}_v$ respectivamente. Como π es cerrado $\pi(\overline{j(g)}) = \overline{g}$. Sea $x' \in \overline{j(g)}$ tal que $\pi(x') = v$. Consideremos el diagrama conmutativo

$$\begin{array}{ccc} \Sigma_v & \hookleftarrow & \mathcal{O}_{\overline{j(g)},x'} \\ \uparrow & & \uparrow{\scriptstyle \pi^*} \\ \mathcal{O}_v & = & \mathcal{O}_v \end{array}$$

Por ser $\mathcal{O}_v$ un anillo de valoración, $\mathcal{O}_{\overline{j(g)},x'} = \mathcal{O}_v$. Por tanto, tenemos el morfismo buscado $\operatorname{Spec}\mathcal{O}_v \to \overline{j(g)} \subset X$.

Veamos el recíproco. Sea C un cerrado de X. Por la Proposición 11.6.5, dado $y' \in \overline{\pi(C)}$ existe un $x \in C$ de modo que $y' \in \overline{\pi(x)} =: Y'$. Tenemos los morfismos naturales $k(\pi(x)) \hookrightarrow k(x)$ y $\mathcal{O}_{Y',y'} \hookrightarrow k(\pi(x))$. Sea $\mathcal{O}_v \subset k(x)$ un anillo de valoración de $k(x)$ que domine a $\mathcal{O}_{Y',y'}$. Tenemos el diagrama conmutativo

$$\begin{array}{ccccccc} \operatorname{Spec}k(x) & & & & & \longrightarrow & X \\ \downarrow & & & & & & \downarrow{\scriptstyle \pi} \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & \operatorname{Spec}\mathcal{O}_{Y',y'} & \longrightarrow & Y' & \hookrightarrow & Y \end{array}$$

Por tanto, existe un morfismo $f\colon \operatorname{Spec}\mathcal{O}_v \to X$, de modo que $\pi(f(v)) = y'$.

□

En Topología se dice que un espacio topológico X es separado si la diagonal $\Delta = \{(x,x), x \in X\}$ es un subespacio cerrado de $X \times X$. En esquemas adoptaremos esta definición, pero hay que advertir que el producto de esquemas no es el producto cartesiano de esquemas.

Sea $\pi\colon X \to S$ un S-esquema. El morfismo natural de funtores (sobre los S-esquemas) $X^{\cdot} \to X^{\cdot} \times X^{\cdot}$, $f \mapsto (f,f)$, define un morfismo de S-esquemas

$$\delta\colon X \to X \times_S X$$

que se denomina morfismo diagonal. Sea $V = \mathrm{Spec}\, A$ un abierto afín de S y $U = \mathrm{Spec}\, B$ un abierto afín de X contenido en $\pi^{-1}(V)$. Entonces $\delta^{-1}(U \times U) = U$ y $\delta_{|U} : U \to U \times U$ es el morfismo diagonal de U, que viene definido por el morfismo de anillos $B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$. Por tanto, $\delta_{|U}$ establece un isomorfismo de esquemas de $U = \mathrm{Spec}\, B$ con $\mathrm{Spec}(B \otimes_A B/\Delta) = (\Delta)_0$, donde Δ es el ideal de la diagonal de $B \otimes_A B$. En conclusión, δ establece un isomorfismo de esquemas de X con un cerrado de un abierto de $X \times_S X$.

8. Definición: Diremos que un morfismo $X \to S$ es separado, o que X es un S-esquema separado, si δ establece un isomorfismo de esquemas de X con un cerrado de $X \times_S X$, es decir, si δ es una inmersión cerrada. Se dice que un esquema X es separado si el morfismo estructural $X \to \mathrm{Spec}\, \mathbb{Z}$ es separado.

9. Ejemplo: Si X e Y son afines, entonces todo morfismo $X \to Y$ es separado. En particular, las variedades algebraicas afines sobre k, son separadas sobre $\mathrm{Spec}\, k$.

10. Ejercicio: Demuestra que si X es separado, entonces la intersección de dos abiertos afines de X es un abierto afín de X.

11. Definición: Se dice que un morfismo de esquemas $f : X \to Y$ es quasi-separado si el morfismo diagonal $\delta : X \to X \times_Y X$ es quasi-compacto. Se dice que un esquema es quasi-separado si el morfismo estructural $\pi : X \to \mathrm{Spec}\, \mathbb{Z}$ es quasi-separado.

Los morfismos separados son quasi-separados. Un esquema es quasi-separado si y solo si la intersección de dos abiertos compactos cualesquiera es compacto.

12. Proposición: *Si X es un esquema compacto quasi-separado entonces existe un recubrimiento finito $\{U_i\}$ de X por abiertos afines tal que $U_i \cap U_j = \bigcup_{U_k \subseteq U_i \cap U_j} U_k$, $\forall\, i, j$.*

Demostración. Sea $\{V_i\}$ un recubrimiento finito de X por abiertos afines. Como X es quasi-separado $V_i \cap V_j$ es compacto para todo i, j, y existe un número finito de abiertos afines V_{ij}^k tales que $V_i \cap V_j = \bigcup_k V_{ij}^k$. Sea $\{U_l\}$ el conjunto de los abiertos que se obtienen como intersecciones de abiertos $\{V_{ij}^k\}$. Veamos que $U_l = V_{i_1 j_1}^{k_1} \cap \cdots \cap V_{i_n j_n}^{k_n}$ es unión de los abiertos afines U_k tales que $U_k \subset U_l$. Observemos que

$$V_{i_r j_r}^{k_r} \cap V_{i_{r+1} j_{r+1}}^{k_{r+1}} = V_{i_r j_r}^{k_r} \cap (V_{j_r} \cap V_{i_{r+1}}) \cap V_{i_{r+1} j_{r+1}}^{k_{r+1}} = \bigcup_k (V_{i_r j_r}^{k_r} \cap V_{j_r i_{r+1}}^{k} \cap V_{i_{r+1} j_{r+1}}^{k_{r+1}}).$$

Es fácil concluir que U_l es unión de abiertos $U_{l'} = V_{i_1 i_2}^{k_1} \cap V_{i_2 i_3}^{k_2} \cap \cdots \cap V_{i_n i_{n+1}}^{k_n}$. Ahora, $V_{i_1 i_2}^{k_1}$ es afín, $V_{i_1 i_2}^{k_1} \cap V_{i_2 i_3}^{k_2}$ es afín porque $V_{i_1 i_2}^{k_1}$ y $V_{i_2 i_3}^{k_2}$ son abiertos afines del abierto afín V_{i_2}. Entonces, $V_{i_1 i_2}^{k_1} \cap V_{i_2 i_3}^{k_2} \cap V_{i_3 i_4}^{k_3}$ es afín porque $V_{i_1 i_2}^{k_1} \cap V_{i_2 i_3}^{k_2}$ y $V_{i_3 i_4}^{k_3}$ son abiertos afines del abierto afín V_{i_3}. Así sucesivamente probamos que $U_{l'}$ es afín.

El recubrimiento buscado es el conjunto de los abiertos afines que se obtienen como intersecciones finitas de los abiertos $\{V_{ij}^k\}$.

□

13. Criterio valorativo de separación: *Sea $X \to Y$ un morfismo de esquemas quasi-separado. El morfismo $X \to Y$ es separado si y solo si cumple la siguiente condición: Para todo anillo de valoración $\mathcal{O}_v$ de cuerpo de fracciones Σ_v y todo diagrama conmutativo*

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & X \\ \downarrow{\scriptstyle i} & & \downarrow \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & Y \end{array}$$

donde i es el morfismo inducido por la inclusión $\mathcal{O}_v \hookrightarrow \Sigma_v$, existe a lo más un morfismo $\operatorname{Spec}\mathcal{O}_v \to X$, que añadido al diagrama anterior, hace los triángulos conmutativos.

Demostración. El morfismo $X \to Y$ cumple el criterio valorativo de separación si y solo si el morfismo diagonal $\delta\colon X \to X \times_Y X$ cumple el criterio valorativo de los morfismos universalmente cerrados. En efecto, cada pareja de Y-morfismos $f_1, f_2\colon \operatorname{Spec}\mathcal{O}_v \to X$, define el morfismo obvio $(f_1, f_2)\colon \operatorname{Spec}\mathcal{O}_v \to X \times_Y X$, y $f_1 = f_2$ si y solo si existe un morfismo $f\colon \operatorname{Spec}\mathcal{O}_v \to X$ tal que $(f_1, f_2) = \delta \circ f$.

Por otra parte, el morfismo diagonal $X \to X \times_Y X$ es universalmente cerrado si y solo si es cerrado, es decir, si y solo si $X \to Y$ es separado.

□

14. Corolario: *Se cumple:*

1. *Las inmersiones abiertas son morfismos separados.*
2. *Las inmersiones cerradas son morfismos separados.*
3. *Los morfismos separados son estables por cambio de base.*
4. *La composición de dos morfismos separados es un morfismo separado.*
5. *Si $f\colon X \to Y$ y $f'\colon X' \to Y'$ son morfismos separados de S-esquemas, entonces $f \times f'\colon X \times_S X' \to Y \times_S Y'$ es separado.*
6. *Sean $f\colon X \to Y$ y $g\colon Y \to Z$ morfismo de esquemas. Si $g \circ f$ es separado entonces f es separado.*

7. *Un morfismo $f : X \to Y$ es separado si y solo si existe un recubrimiento de Y por abiertos U_i , tales que $f^{-1}(U_i) \to U_i$ es separado para todo i.*

Demostración. 4. Sean $f : X \to Y$, $g : Y \to Z$ morfismos separados. Demostremos que $g \circ f : X \to Z$ es separado. Si tenemos un diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & X \\ \downarrow & \overset{f_1}{\nearrow} & \downarrow{\scriptstyle g\circ f} \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & Z \end{array}$$

tenemos el diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & Y \\ \downarrow & \overset{f\circ f_1}{\nearrow} & \downarrow{\scriptstyle g} \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & Z \end{array}$$

Por tanto, $f \circ f_1 = f \circ f_2$, por ser g separado. Ahora, del primer diagrama, obtenemos diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & X \\ \downarrow & \overset{f_1}{\nearrow} & \downarrow{\scriptstyle f} \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & Y \end{array}$$

Por tanto, $f_1 = f_2$, por ser f separado. En conclusión, $g \circ f$ es separado.

5. El morfismo $f \times f'$ es separado porque es la composición de los morfismos separados $X \times_S X' \to Y \times_S X' \to Y \times_S Y'$, que son separados por 3.

6. Sea Δ_Z la diagonal de $X \times_Z X$, que es un subesquema cerrado isomorfo a X e $I : X \times_Y X \to X \times_Z X$ el morfismo obvio. . Del diagrama conmutativo

$$\begin{array}{ccccc} X^{\cdot} & \longrightarrow & (I^{-1}(\Delta_Z))^{\cdot} & \hookrightarrow & \Delta_Z^{\cdot} \\ & & \downarrow & & \downarrow \\ & & (X \times_Y X)^{\cdot} & \hookrightarrow & (X \times_Z X)^{\cdot} \end{array}$$

se deduce que $X^{\cdot} = (I^{-1}(\Delta_Z))^{\cdot}$, luego el subesquema cerrado $I^{-1}(\Delta_Z)$ de $X \times_Y X$ coincide con la diagonal y f es separado.

□

15. Definición: Se dice que un morfismo de esquemas $f: X \to Y$ es de tipo finito, si existe un recubrimiento de Y por abiertos afines U_i y para cada i un recubrimiento finito de $f^{-1}(U_i)$ por abiertos afines V_{ij} de modo que los morfismos $\mathscr{O}_Y(U_i) \to \mathscr{O}_X(V_{ij})$ son de tipo finito. Es decir, un morfismo de tipo finito es un morfismo quasi-compacto de modo que localmente en X e Y, f es un morfismo entre esquemas afines tal que entre los anillos de funciones es un morfismo de tipo finito.

16. Definición: Se dice que un morfismo de esquemas $X \to S$ es propio, o que X es un S-esquema propio, si es de tipo finito, separado y universalmente cerrado.

El teorema que sigue es consecuencia inmediata de los criterios valorativos 11.6.13, 11.6.7.

17. Criterio valorativo de propiedad: *Sea $X \to Y$ un morfismo de esquemas de tipo finito quasi-separado. Entonces $X \to Y$ es propio si y solo si cumple la siguiente condición: Para todo anillo de valoración $\mathscr{O}_v$ de cuerpo de fracciones Σ_v y todo diagrama conmutativo*

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \xrightarrow{j} & X \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \pi} \\ \operatorname{Spec}\mathscr{O}_v & \longrightarrow & Y \end{array}$$

donde i es el morfismo inducido por la inclusión $\mathscr{O}_v \hookrightarrow \Sigma_v$, existe un único morfismo $f: \operatorname{Spec}\mathscr{O}_v \to X$, que añadido al diagrama anterior, hace los triángulos conmutativos.

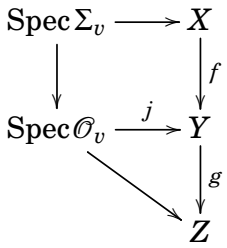
18. Ejemplo: El morfismo $\mathbb{A}^1_k \to \operatorname{Spec} k$ no es propio porque no es universalmente cerrado. En efecto, al cambiar de base por sí mismo se obtiene el morfismo $\mathbb{A}^1 \times_k \mathbb{A}^1 = \mathbb{A}^2 \to \mathbb{A}^1$ de proyección en el segundo factor. La proyección de la hipérbola $(xy-1)_0$ es toda la recta afín menos el origen, que no es un cerrado.

19. Corolario: *Se cumple que:*

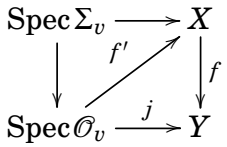
1. *Las inmersiones cerradas son morfismos propios.*
2. *Los morfismos propios son estables por cambio de base.*
3. *La composición de dos morfismos propios es un morfismo propio.*
4. *Si $f: X \to Y$ y $f': X' \to Y'$ son morfismos propios de S-esquemas, entonces el morfismo $f \times f': X \times_S X' \to Y \times_S Y'$ es propio.*
5. *Un morfismo $f: X \to Y$ es propio si y solo si existe un recubrimiento de Y por abiertos U_i , tales que $f^{-1}(U_i) \to U_i$ es propio para todo i.*

6. *Sea $f: X \to Y$ un morfismo quasi-compacto y $g: Y \to Z$ un morfismo separado. Si $g \circ f$ es propio, entonces f es propio.*

Demostración. Las afirmaciones 1-5 son consecuencia de 11.6.2 y 11.6.14. Probemos la afirmación 6. Por 11.6.14 6., f es separado. Si tenemos un diagrama conmutativo



por ser $g \circ f$ propio, existe un $f': \operatorname{Spec} \mathscr{O}_v \to X$, que añadido al diagrama anterior (ignorando Y), lo hace conmutativo. Ahora bien, $f \circ f'$ ha de ser igual a j, por ser g separado. Tenemos por tanto el diagrama conmutativo



La unicidad de f' se deduce de que f es separado. En conclusión, f es propio. □

20. Ejemplo: Los morfismos finitos de esquemas son propios: son separados porque son afines y son universalmente cerrados porque son cerrados y porque por cambio de base son finitos.

21. Definición: Sea $R = A[\xi_1, \ldots, \xi_n]$ una A-álgebra graduada, con $\operatorname{gr} \xi_i = 1$, para todo i. Diremos que el morfismo $\operatorname{Proj} R \to \operatorname{Spec} A$ es un morfismo proyectivo. Diremos que un morfismo de esquemas $f: X \to Y$ es localmente proyectivo si existe un recubrimiento de Y por abiertos afines U_i, tales que $f^{-1}(U_i) \to U_i$ son morfismos proyectivos.

22. Teorema: *Si $f: X \to Y$ es un morfismo localmente proyectivo entonces f es propio.*

Demostración. Por 11.6.19.5 podemos suponer que f es un morfismo proyectivo. Argumentando como en 11.4.7 es sencillo probar que f cumple el criterio valorativo de propiedad. □

23. Definición: Sea $\mathcal{O}$ un anillo local íntegro de cuerpo de fracciones Σ y X un esquema. Sea g el punto genérico de $\operatorname{Spec}\mathcal{O}$ y v el punto cerrado. Fijemos un morfismo $f\colon \operatorname{Spec}\Sigma \to X$. Diremos que $\mathcal{O}$ centra en un punto $x \in X$, si existe un diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec}\Sigma & \xrightarrow{f} & X \\ \downarrow & \nearrow_{f'} & \\ \operatorname{Spec}\mathcal{O} & & \end{array}$$

de modo que $f'(v) = x$ (luego $x \in \overline{f(g)}$).

En otras palabras, si consideramos la inclusión $k(f(g)) \subseteq \Sigma$ resulta que el anillo $\mathcal{O}$ domina al subanillo $\mathcal{O}_{\overline{f(g)},x} \subset k(f(g))$.

24. Lema: *Sea $\mathcal{O}_v$ un anillo de valoración, de cuerpo de fracciones Σ_v y de ideal de valoración $\mathfrak{p}_v$. Sea $\pi\colon \mathcal{O}_v \to \mathcal{O}_v/\mathfrak{p}_v$ el morfismo de paso al cociente. Las aplicaciones*

$$\begin{array}{rcl} \{\textit{Anillos de val. de } \Sigma_v\textit{, contenidos en } \mathcal{O}_v\} & = & \{\textit{Anillos de val. de } \mathcal{O}_v/\mathfrak{p}_v\} \\ B & \longmapsto & \bar{B} \\ \pi^{-1}(\mathcal{O}_{v'}) & \longmapsfrom & \mathcal{O}_{v'} \end{array}$$

establecen una biyección entre los anillos de valoración de Σ_v contenidos en $\mathcal{O}_v$ y los anillos de valoración de $\mathcal{O}_v/\mathfrak{p}_v$.

Demostración. La proposición se deduce inmediatamente de los siguientes puntos.

1. Si $\mathcal{O}_{\bar{v}}$ es un subanillo de valoración de Σ_v contenido en $\mathcal{O}_v$ tenemos que $\mathfrak{p}_v \subset \mathfrak{p}_{\bar{v}}$, porque si $f \in \mathfrak{p}_v$ y $f \notin \mathfrak{p}_{\bar{v}}$, entonces $f^{-1} \in \mathcal{O}_{\bar{v}} \subset \mathcal{O}_v$, luego $f \notin \mathfrak{p}_v$. Además, si denotamos $\mathfrak{p}_x = \mathfrak{p}_v \subset \mathcal{O}_{\bar{v}}$ entonces $\mathcal{O}_v = (\mathcal{O}_{\bar{v}})_x$.

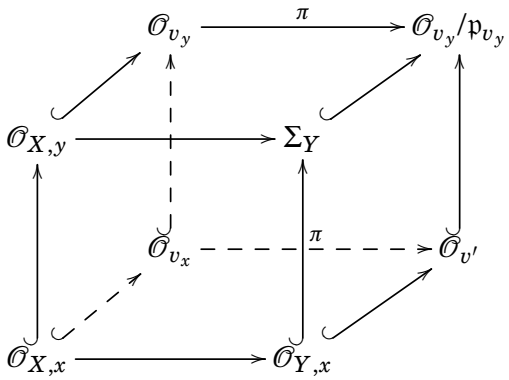
2. Si $\mathfrak{p}_x$ es un ideal primo de un anillo de valoración B, entonces $B/\mathfrak{p}_x$ es un anillo de valoración (de $B_x/(\mathfrak{p}_x)$): Dado $0 \neq \bar{b}/\bar{c}$ (con $b, c \in B$), entonces o $b/c = d \in B$ o $c/b = e \in B$, luego o $\bar{b}/\bar{c} = \bar{d} \in B/\mathfrak{p}_x$ o $(\bar{b}/\bar{c})^{-1} = \bar{e} \in B/\mathfrak{p}_x$.

3. Si C es un subanillo de valoración de $\mathcal{O}_v/\mathfrak{p}_v$ entonces $\pi^{-1}(C)$ es un subanillo valoración de Σ_v: Sea $c \in \Sigma_v$. Si $v(c) = 0$ entonces $c, c^{-1} \in \mathcal{O}_v$ y $\bar{c}, \bar{c}^{-1} \in \mathcal{O}_v/\mathfrak{p}_v$. Por tanto, $\bar{c} \in C$ o $\bar{c}^{-1} \in C$, y $c \in \pi^{-1}(C)$ o $c^{-1} \in \pi^{-1}(C)$. Si $v(c) > 0$ entonces $c \in \mathfrak{p}_v$ y $\bar{c} = 0$, luego $c \in \pi^{-1}(C)$. Si $v(c) < 0$ entonces $v(c^{-1}) > 0$ y $c^{-1} \in \pi^{-1}(C)$.

□

25. Proposición : *Toda subvariedad cerrada íntegra de una variedad completa es completa.*

Demostración. Sea X la variedad completa e $Y \subset X$ la subvariedad cerrada, de punto genérico y.



Sea $\mathcal{O}_{v_y}$ el anillo de valoración de Σ_X que centre en y. Dado un subanillo de valoración $\mathcal{O}_{v_x} \subset \mathcal{O}_v$ de Σ_X, sabemos que centra en un punto $x \in X$. Como $\mathcal{O}_{X,x} \subset \mathcal{O}_{v_y}$, v_y centra en un punto de $\operatorname{Spec}\mathcal{O}_x$, que es y. Por tanto, $x \in \bar{y} = Y$. Consideremos las inclusiones $\mathcal{O}_{X,x} \subset \mathcal{O}_{v_x} \subset \mathcal{O}_{v_y}$ y $\mathcal{O}_{X,y} \subset \mathcal{O}_{v_y}$. Haciendo cociente por $\mathfrak{p}_{v_y}$, obtenemos las inclusiones $\mathcal{O}_{Y,x} \subset \mathcal{O}_{v_y}/\mathfrak{p}_{v_y} = \mathcal{O}_{v'} \subset \mathcal{O}_{v_y}/\mathfrak{p}_v$ y $\Sigma_Y \subset \mathcal{O}_{v_y}/\mathfrak{p}_{v_y}$. Es claro que $\mathcal{O}_v := \mathcal{O}_{v'} \cap \Sigma_Y$ centra en x. Si $\mathcal{O}_v$ centra además en otro punto $x' \in Y$, tendríamos morfismos $\mathcal{O}_{X,x'} \to \mathcal{O}_{Y,x'} \to \mathcal{O}_{v'}$ y $\mathcal{O}_{X,x'} \to \mathcal{O}_{X,y} \to \mathcal{O}_{v_y}$, que definirían un morfismo $\mathcal{O}_{X,x'} \to \mathcal{O}_{v_x}$ de modo que v_x centraría en x', luego $x' = x$.

Sea $\mathcal{O}_w$ un anillo de valoración de Σ_Y y $\pi\colon \mathcal{O}_{v_y} \to \mathcal{O}_{v_y}/\mathfrak{p}_{v_y}$ el morfismo de paso al cociente. $\pi^{-1}(\mathcal{O}_w) \subset \mathcal{O}_{v_y}$ es un anillo de valoración que centra en un punto $x \in Y$, luego $\mathcal{O}_w$ centra únicamente en x, por el párrafo anterior.

□

26. Teorema: *Sea X una k-variedad algebraica íntegra. X es una variedad algebraica completa si y solo si el morfismo estructural $X \to \operatorname{Spec} k$ es propio .*

Demostración. Obviamente si el morfismo estructural es propio la variedad algebraica es completa. Supongamos que X es completa. Consideremos un diagrama conmutativo,

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_v & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & \operatorname{Spec} k \end{array}$$

Sea $y = \operatorname{Im} j$ e $Y = \bar{y}$. Podemos reducir el problema al caso en que $\Sigma_v = \Sigma_Y$ y $\mathcal{O}_v = \mathcal{O}_v \cap \Sigma_Y$. Como Y es completa, existe un único punto $x \in Y$ en el que v centra, es decir, existe un único morfismo $f\colon \operatorname{Spec} O_v \to X$ que hace el diagrama

$$\begin{array}{ccc} \operatorname{Spec}\Sigma_Y & \longrightarrow & X \\ \downarrow & \overset{f}{\nearrow} & \downarrow \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & \operatorname{Spec} k \end{array}$$

conmutativo, luego $X \to \operatorname{Spec} k$ es un morfismo propio.

□

11.7. Problemas

1. Sea A un anillo íntegro. Demuestra que $A = \bigcap_{x \in \operatorname{Spec} A} A_x$. Más en general, prueba que $\Gamma(U, \widetilde{A}) = \bigcap_{x \in U} A_x$, para todo abierto U de $\operatorname{Spec} A$.

2. Sea $(X, \mathcal{O}_X)$ un esquema. Sea X_{red} el espacio anillado cuyo espacio topológico subyacente es X y cuyo haz estructural es $\mathcal{O}_{X_{\text{red}}}$= haz asociado al prehaz de anillos $U \rightsquigarrow \mathcal{O}_X(U)/\operatorname{Rad}(\mathcal{O}_X(U))$. Prueba que X_{red} es un esquema y es reducido. Prueba que X_{red} es un subesquema cerrado de X y que para todo esquema reducido Y se verifica la igualdad $\operatorname{Hom}(Y, X) = \operatorname{Hom}(Y, X_{\text{red}})$.

3. Sea $(X, \mathcal{O}_X)$ un espacio anillado, $\operatorname{Aut}(X)$ el grupo de automorfismos (de espacios anillados) de X y G un subgrupo de $\operatorname{Aut}(X)$. Sea X/G el espacio topológico cociente de X por la relación de equivalencia definida por la operación de G en X. Sea $\pi\colon X \to X/G$ el morfismo de paso al cociente y $\mathcal{O}_{X/G}$ el prehaz definido por $\mathcal{O}_{X/G}(U) = \mathcal{O}_X(\pi^{-1}(U))^G = \{s \in \mathcal{O}_X(\pi^{-1}(U))$, tales que $gs = s$, para todo $g \in G\}$.

   a) Prueba que $(X/G, \mathcal{O}_{X/G})$ es un espacio anillado.

   b) Si $(X, \mathcal{O}_X) = (\operatorname{Spec} A, \widetilde{A})$ y G es un grupo finito, prueba que $(X/G, \mathcal{O}_{X/G}) = (\operatorname{Spec} A^G, \widetilde{A^G})$.

   c) Si G es finito y X es una variedad algebraica afín (sobre k), prueba que X/G también lo es (se supone que los elementos de G son automorfismos de k-esquemas).

4. Prueba que C es un cerrado irreducible de un esquema si y solo si existe un único punto $x \in C$, tal que $\bar{x} = C$.

5. Prueba que $\Gamma(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}) = k$. Concluir que $\mathbb{P}^n_k$ no es un esquema afín, para $n > 0$.

6. Prueba que $X = \mathbb{A}^3_k - (x, y)_0$ no es un esquema afín.

7. Prueba que para todo k-esquema Z se verifica $\operatorname{Hom}_{\text{k-esq}}(Z, \mathbb{A}^1_k) = \Gamma(Z, \mathcal{O}_Z)$.

8. Prueba que las variedades algebraicas sobre un cuerpo k son catenarias.

9. Se dice que un punto x de una k-variedad algebraica es racional si $k = \mathcal{O}_{X,x}/\mathfrak{p}_x$. Prueba que si $f: X \to Y$ es un morfismo entre k-variedades algebraicas, entonces f transforma puntos racionales en puntos racionales. Prueba además que f transforma puntos cerrados en puntos cerrados.

10. Define el morfismo de esquemas $\mathbb{A}^3\setminus\{0\} \to \mathbb{P}^2$, que sobre los puntos racionales aplica (a_0, a_1, a_2) en $\overline{(a_0, a_1, a_2)}$.

11. Sea A un anillo local. Prueba que

$$\mathrm{Hom}_{k-\mathrm{esq}}(\mathrm{Spec}\, A, \mathbb{P}^n_k) = \{(a_0, \ldots, a_n), \text{algún } a_i \in A \text{ invertible}\}/\sim$$

donde $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ si y solo si existe un $c \in A$ invertible tal que $a_i = c \cdot b_i$, para todo i.

12. Prueba que toda curva completa y no singular sobre un cuerpo algebraicamente cerrado es birracional a una curva plana.

13. Sea $\pi: C' \to C$ un morfismo entre curvas afines, íntegras y no singulares. Demuestra que π es un morfismo finito si y solo si el número de puntos de las fibras es constante.

14. Sea $f: X \to X'$ un morfismo de S-esquemas, con X' separado sobre S. Prueba que la gráfica $\Gamma_f: X \to X \times_S X'$, $x \mapsto (x, f(x))$, es una inmersión cerrada.

15. Sean $f, g: X \to X'$ dos morfismos de S-esquemas. Supongamos que X' es separado sobre S y X es irreducible. Prueba que si existe un abierto no vacío de X sobre el que coinciden f y g entonces $f = g$.

Capítulo 12

Módulos quasi-coherentes y coherentes

12.1. Módulos quasi-coherentes

En el capítulo anterior definimos los esquemas como aquellas estructuras que localmente son $(\operatorname{Spec} A, \tilde{A})$. En capítulos anteriores, hemos definido y estudiado los A-módulos. El objetivo principal de este capítulo es el estudio de los haces de módulos sobre un esquema, que localmente sean A-módulos. Estos haces los denominaremos módulos quasi-coherentes. Posteriormente estudiaremos la estructura de estos módulos en los esquemas proyectivos. Acabaremos con el estudio de los haces de línea, y demostraremos el teorema de Bézout.

1. Definición: Sea $(\operatorname{Spec} A, \tilde{A})$ un esquema afín y M un A-módulo. Llamaremos haz de localizaciones de M, y lo denotaremos $\widetilde{M}$, al haz de $\tilde{A}$-módulos asociado al prehaz de localizaciones de M: $U \rightsquigarrow M_U = M \otimes_A A_U$ (véase 10.1.3, ejemplo 5).

2. Proposición: *Para cada $x \in \operatorname{Spec} A$, se cumple que $\widetilde{M}_x = M_x$.*

Demostración. Es consecuencia de 10.1.5. □

3. Proposición: *Sea $X = \operatorname{Spec} A$ un esquema afín y M un A-módulo. Para todo abierto básico U_a se cumple que*

$$\Gamma(U_a, \widetilde{M}) = M_a$$

En particular, $\Gamma(X, \widetilde{M}) = M$.

Demostración. Se argumenta como en 11.1.12.

□

Es fácil ver que $\widetilde{M}_{|U_a} = \widetilde{M_a}$ en $U_a \subset \operatorname{Spec} A$.

Nuestro siguiente objetivo es probar que si un haz de $\widetilde{A}$-módulos es localmente el haz de localizaciones de ciertos módulos, entonces lo es globalmente. Así pues, el concepto de módulo de localizaciones es esencialmente local, luego podremos introducirlo (con el nombre de "módulos quasi-coherentes") en esquemas no afines.

4. Definición: Sea X un esquema. Se dice que un $\mathscr{O}_X$-módulo $\mathscr{M}$ es quasi-coherente, si existe un recubrimiento de X por abiertos afines U_i tales que $\mathscr{M}_{|U_i} = \widetilde{\mathscr{M}(U_i)}$ (recuérdese 12.1.3).

5. Teorema: *Sea $X = \operatorname{Spec} A$ un esquema afín. El funtor*

$$\mathscr{M} \rightsquigarrow \Gamma(X, \mathscr{M})$$

establece una equivalencia entre la categoría de $\mathscr{O}_X$-módulos quasi-coherentes y la categoría de A-módulos (cuyo funtor inverso es $M \rightsquigarrow \widetilde{M}$).

Demostración. Veamos que para todo módulo quasi-coherente $\mathscr{M}$ se cumple que $\mathscr{M} = \widetilde{\mathscr{M}(X)}$. Dada $f \in A$, f es invertible en $U_f = \operatorname{Spec} A_f$, luego el morfismo de restricción $\mathscr{M}(X) \to \mathscr{M}(U_f)$ induce por localización un morfismo $\mathscr{M}(X)_f \to \mathscr{M}(U_f)$. En conclusión, tenemos un morfismo de $\mathscr{O}_X$-módulos $\widetilde{\Gamma(X, \mathscr{M})} \to \mathscr{M}$. Veamos que es isomorfismo.

Por ser $\mathscr{M}$ quasi-coherente, existe un recubrimiento de X por abiertos básicos U_i tales que $\mathscr{M}_{|U_i} \overset{*}{=} \widetilde{\mathscr{M}(U_i)}$. Localizando por $f \in A$ la sucesión exacta

$$\Gamma(X, \mathscr{M}) \to \bigoplus_i \Gamma(U_i, \mathscr{M}) \rightrightarrows \bigoplus_{i,j} \Gamma(U_i \cap U_j, \mathscr{M})$$

obtenemos

$$\begin{array}{ccc} \Gamma(X, \mathscr{M})_f \to \bigoplus_i \Gamma(U_i, \mathscr{M})_f & \rightrightarrows & \bigoplus_{i,j} \Gamma(U_i \cap U_j, \mathscr{M})_f \\ \| \text{ por } * & & \| \text{ por } * \\ \Gamma(U_f, \mathscr{M}) \to \bigoplus_i \Gamma(U_i \cap U_f, \mathscr{M}) & \rightrightarrows & \bigoplus_{i,j} \Gamma(U_i \cap U_j \cap U_f, \mathscr{M}) \end{array}$$

y por tanto $\Gamma(X, \mathscr{M})_f = \Gamma(U_f, \mathscr{M})$. En conclusión $\mathscr{M}$ coincide con $\widetilde{\Gamma(X, \mathscr{M})}$ sobre abiertos básicos, luego $\mathscr{M} = \widetilde{\Gamma(X, \mathscr{M})}$. El resto de la demostración se lo dejamos al lector.

□

6. Corolario: *Sea X un esquema. El producto tensorial y el límite inductivo de $\mathscr{O}_X$-módulos quasi-coherentes es quasi-coherente. Si $U = \operatorname{Spec} A \subseteq X$ es un abierto afín, entonces*

$$\Gamma(U, \mathscr{M} \underset{\mathscr{O}_X}{\otimes} \mathscr{N}) = \Gamma(U, \mathscr{M}) \otimes_A \Gamma(U, \mathscr{N})$$

$$\Gamma(U, \varinjlim_i \mathscr{M}_i) = \varinjlim_i \Gamma(U, \mathscr{M}_i)$$

Demostración. Podemos suponer que X es afín y $U = X$. Sea $M = \mathscr{M}(X)$, $N = \mathscr{N}(X)$. El prehaz de localizaciones de $M \otimes_A N$ coincide con el prehaz producto tensorial de los prehaces de localizaciones de M y N, porque $(M \otimes_A N)_S = M_S \otimes_{A_S} N_S$. Por lo tanto, se cumple que $\mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N} = \widetilde{M \otimes_A N}$ es quasi-coherente y $\Gamma(X, \mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N}) = M \otimes_A N$ (por 12.1.3). Arguméntese de modo análogo con el límite inductivo. □

7. Corolario: *Sea X un esquema afín. Una sucesión de $\mathscr{O}_X$-módulos quasi-coherentes*

$$0 \to \mathscr{M}' \to \mathscr{M} \to \mathscr{M}'' \to 0$$

es exacta si y solo si

$$0 \to \Gamma(X, \mathscr{M}') \to \Gamma(X, \mathscr{M}) \to \Gamma(X, \mathscr{M}'') \to 0$$

es exacta.

Demostración. Es inmediato de la equivalencia categorial dada por el Teorema 12.1.5. □

8. Corolario: *Sea X un esquema. Entonces, el núcleo y conúcleo de un morfismo entre haces quasi-coherentes son quasi-coherentes.*

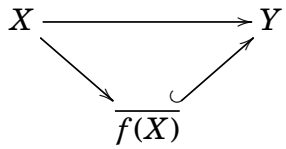
Demostración. Podemos suponer que X es afín y concluimos por 12.1.5. □

Sea X un esquema e $I \subseteq \mathscr{O}_X$ un haz de ideales quasi-coherente. Sea

$$(I)_0 := \{x \in X : I_x \subseteq \mathfrak{p}_x \subset \mathscr{O}_{X,x}\}$$

$(I)_0$ es un cerrado de X, porque si $U = \operatorname{Spec} A$ es un abierto afín de X, entonces $U \cap (I)_0 = (I(U))_0 \subset \operatorname{Spec} A$. Si $V \subseteq X$ es otro abierto afín tal que $V \cap (I)_0 = U \cap (I)_0$, entonces $\mathscr{O}_X(V)/I(V) = \mathscr{O}_X(U)/I(U)$, porque en gérmenes coinciden. Consideremos el haz sobre $(I)_0$, $\mathscr{O}_X/I$, que asigna a cada abierto $U \cap (I)_0$ ($U \subset X$ afín) el anillo $\mathscr{O}_X(U)/I(U)$. Entonces, $((I)_0, \mathscr{O}_X/I)$ es un subesquema cerrado de $(X, \mathscr{O}_X)$. Recíprocamente, dado un subesquema cerrado $i : (Y, \mathscr{O}_Y) \subseteq (X, \mathscr{O}_X)$ el núcleo del morfismo $\mathscr{O}_X \to i_* \mathscr{O}_Y$ es un ideal quasi-coherente de $\mathscr{O}_X$. Tenemos una correspondencia biunívoca entre haces de ideales quasi-coherentes de $\mathscr{O}_X$ y subesquemas cerrados de X. Dado un esquema $(X, \mathscr{O}_X)$, denotamos $\operatorname{rad}\mathscr{O}_X$, el haz de ideales quasi-coherente de $\mathscr{O}_X$, definido por $(\operatorname{rad}\mathscr{O}_X)(U) = \operatorname{rad}(\mathscr{O}_X(U))$, para todo abierto $U \subseteq X$. Obviamente, $(\operatorname{rad}\mathscr{O}_X)_0 = X$ y diremos que $(X, \mathscr{O}_X/\operatorname{rad}\mathscr{O}_X)$ es el esquema reducido de X, que denotaremos X_{red}.

9. Proposición: *Sea $f : X \to Y$ un morfismo de esquemas cuasicompacto. El núcleo, I, del morfismo $\mathcal{O}_Y \to f_*\mathcal{O}_X$ es un haz de ideales quasi-coherente de $\mathcal{O}_Y$ y $(I)_0 = \overline{f(X)}$. Diremos que $(\overline{f(X)}, \mathcal{O}_Y/I)$ es la imagen esquemática de f y tenemos un diagrama conmutativo*



.

Demostración. El problema es local en Y, luego podemos suponer que Y es afín. Por ser f cuasicompacto X es unión de un número finito de abiertos afines $\{U_i\}$. Podemos sustituir X por $\bar{X} := \coprod_i U_i$, porque si denotamos por $\bar{f}$ la composición de los morfismos $\bar{X} \to X \to Y$, se cumple que el núcleo del morfismo $\mathcal{O}_Y \to \bar{f}_*\mathcal{O}_{\bar{X}}$ es I, y $\bar{f}(\bar{X}) = f(X)$. Por tanto, podemos suponer que X es afín. Ahora ya, la proposición es trivial.

□

12.1.1. Módulos coherentes

10. Definición: Sea X un esquema y $\mathcal{M}$ un $\mathcal{O}_X$-módulo quasi-coherente.

1. Diremos que $\mathcal{M}$ es finito generado si existe un recubrimiento de X por abiertos afines $\{U_i\}$ tales que $\mathcal{M}(U_i)$ es $\mathcal{O}_X(U_i)$-módulo finito generado.

2. Diremos que $\mathcal{M}$ es de presentación finita si existe un recubrimiento de X por abiertos afines $\{U_i\}$ tales que $\mathcal{M}(U_i)$ es un $\mathcal{O}_X(U_i)$-módulo de presentación finita.

3. Diremos que $\mathcal{M}$ es coherente si existe un recubrimiento de X por abiertos afines $\{U_i\}$ tales que $\mathcal{M}(U_i)$ es $\mathcal{O}_X(U_i)$-módulo finito generado y todo submódulo finito generado de $\mathcal{M}(U_i)$ es de presentación finita.

Si X es un esquema localmente noetheriano los tres conceptos anteriores son equivalentes.

11. Teorema: *Sea $X = \operatorname{Spec} A$ un esquema afín. La categoría de $\mathcal{O}_X$-módulos de presentación finita (resp. finito generados, coherentes) es equivalente a la categoría de A-módulos de presentación finita (resp. finito generados, coherentes).*

Demostración. Probemos solo que la categoría de $\mathscr{O}_X$-módulos de presentación finita es equivalente a la categoría de A-módulos de presentación finita. Por el Teorema 12.1.5, basta ver que si $\widetilde{M}$ es un módulo de presentación finita, entonces M es un A-módulo de presentación finita. Por definición, existe un recubrimiento de X por abiertos básicos $U_{a_1},\dots,U_{a_r}$ tales que M_{a_i} es un A_{a_i}-módulo de presentación finita. Si $m_{i1},\dots,m_{in_i}$ son elementos de M cuyas imágenes en M_{a_i} son generadores, entonces $m_{11}\dots,m_{rn_r}$ generan M. Entonces existe un epimorfismo de A-módulos $\pi\colon A^n \to M$. $\operatorname{Ker}\pi$ es un A-módulo finito generado porque $(\operatorname{Ker}\pi)_{a_i}$ es un A_{a_i}-módulo finito generado para todo a_i. Es decir, M es de presentación finita. □

Sea $f\colon \mathscr{M} \to \mathscr{N}$ es un morfismo de módulos. Si $\mathscr{M}$ es finito generado entonces $\operatorname{Im} f$ es finito generado. Si $\mathscr{M}$ es coherente entonces $\operatorname{Ker} f$ es coherente. Si $\mathscr{M}$ es finito generado y $\mathscr{N}$ de presentación finita (resp. coherente) entonces $\operatorname{Coker} f$ es de presentación finita (resp. finito coherente).

12. Proposición: *Si X es un esquema, $\mathscr{M}$ un módulo de presentación finita y $\mathscr{N}$ un módulo quasi-coherente, entonces $\underline{\operatorname{Hom}}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N})$ es un módulo quasi-coherente.*

Demostración. Si M es un A-módulo de presentación finita y S un sistema multiplicativo S, entonces $\operatorname{Hom}_A(M,N)_S = \operatorname{Hom}_{A_S}(M_S,N_S)$ (ver 0.9.20). Se concluye por el Teorema 12.1.5. □

13. Corolario: *Sea X un esquema y $\mathscr{M}$ y $\mathscr{N}$ módulos quasi-coherentes. Entonces,*

1. *Si $\mathscr{M}$ y $\mathscr{N}$ son de presentación finita (resp. finito generados), entonces $\mathscr{M}\otimes_{\mathscr{O}_X}\mathscr{N}$ es de presentación finita (resp. finito generado).*

2. *Si $\mathscr{M}$ es de presentación finita y $\mathscr{N}$ es coherente, entonces $\underline{\operatorname{Hom}}_{\mathscr{O}_X}(\mathscr{M},\mathscr{N})$ es coherente.*

Demostración. Podemos suponer que X es afín y trabajar en la categoría de A-módulos por 12.1.11. Se deja al lector. □

14. Corolario: *Sea X un esquema compacto y quasi-separado y sea $\mathscr{M}$ un $\mathscr{O}_X$-módulo quasi-coherente. Sea $U \overset{\phi}{\subseteq} X$ un abierto compacto y $\mathscr{N}$ es un submódulo finito generado de $\mathscr{M}_{|U}$. Entonces, existe un submódulo finito generado $\mathscr{N}' \subseteq \mathscr{M}$ de modo que $\mathscr{N}'_{|U} = \mathscr{N}$.*

Demostración. 1. Supongamos $X = U \cup V$ donde V es afín.

Existe un submódulo finito generado $N' \subset \mathscr{M}(V)$ tal que $\tilde{N}'_{|U\cap V} = \mathscr{N}_{|U\cap V}$. En efecto, sea $V_{a_1},\dots,V_{a_n}$ un recubrimiento de $U\cap V$ por abiertos básicos de V. Sea M' el núcleo del morfismo obvio $M \to \prod_i M(V_{a_i})/\mathscr{N}(V_{a_i})$. $\tilde{M}'$ es un submódulo quasi-coherente de

$\mathscr{M}$ tal que $\tilde{M}'_{|V_{a_i}} = \mathscr{N}_{|V_{a_i}}$, luego $\tilde{M}'_{|U\cap V} = \mathscr{N}_{|U\cap V}$. M' es unión de submódulos finito generados y para uno de éstos, N', suficientemente grande tendremos que M'_{a_i} es igual al módulo finito generado $M'_{a_i} = \mathscr{N}(V_{a_i})$, para todo i, luego $\tilde{N}'_{U\cap V} = \mathscr{N}_{|U\cap V}$.

Sea $\mathscr{N}'$ el submódulo finito generado de $\mathscr{M}$ tal que $\mathscr{N}'_{|U} = \mathscr{N}$ y $\mathscr{N}'_V = \tilde{N}'$.

2. Aplicando 1. reiteradamente acabamos la demostración □

15. Corolario: *Sea X un esquema quasi-compacto y quasi-separado. Todo $\mathscr{O}_X$-módulo quasi-coherente es el límite inductivo de sus submódulos finito generados.*

16. Corolario : *Sea X un esquema quasi-compacto y quasi-separado. Los módulos finito generados (que módulo isomorfismos son un conjunto) son generadores de la categoría de los moódulos quasi-coherentes. Por tanto, la categoría de los módulos quasi-coherentes de X tiene un generador.*

12.1.2. Imágenes directa e inversa de módulos quasi-coherentes

17. Lema: *Sea f : $\mathrm{Spec}B \to \mathrm{Spec}A$ un morfismo de esquemas y M un B-módulo (luego un A-módulo). Entonces, $f_*\tilde{M} = \tilde{M}$.*

Demostración. Es inmediato. □

18. Proposición : *Sae $f : X \to Y$ un morfismo finito de esquemas. La imagen directa por f de un módulo finito generado es finito generado.*

Demostración. La cuestión es local en Y, luego podemos suponer que Y es afín. Por tanto, X será también afín y concluimos por el lema 12.1.17. □

19. Proposición : *Sea $f : X \to Y$ un morfismo de esquemas quasi-compacto y quasi-separado. Si $\mathscr{M}$ es un $\mathscr{O}_X$-módulo quasi-coherente, entonces $f_*\mathscr{M}$ es quasi-coherente.*

Demostración. Podemos suponer que Y es afín. Consideremos un recubrimiento finito de X por abiertos afines V_i, y para cada $V_i \cap V_j$ un recubrimiento finito por abiertos afines V_{ijk}. Dado un abierto $W \overset{i}{\hookrightarrow} X$ denotemos $\mathscr{M}_W = i_*(\mathscr{M}_{|W})$. Explícitamente, $\mathscr{M}_W(U) = \mathscr{M}(U \cap W)$. Dado un módulo quasi-coherente $\mathscr{M}$ sobre X se tiene la sucesión exacta

$$\mathscr{M} \to \oplus \mathscr{M}_{V_i} \rightrightarrows \oplus \mathscr{M}_{V_{ijk}}$$

Tomando imágenes directas por f (que es exacto por la izquierda), obtenemos la sucesión exacta

$$f_*\mathscr{M} \to \oplus f_*\mathscr{M}_{V_i} \rightrightarrows \oplus f_*\mathscr{M}_{V_{ijk}}$$

Ahora bien, $f_*\mathscr{M}_{V_i} = f_*(i_*(\mathscr{M}_{|V_i}))$ son quasi-coherentes porque $f \circ i : V_i \to Y$ es un morfismo entre esquemas afines. Por la misma razón $f_*\mathscr{M}_{V_{ijk}}$ son quasi-coherentes. Con todo f_*M es quasi-coherente. □

20. Corolario: *Sea X un esquema quasi-compacto y quasi-separado y $i : U \hookrightarrow X$ un abierto compacto. Para todo módulo finito generado $\mathscr{N}$ en U existe un módulo finito generado $\mathscr{N}'$ en X, tal que $\mathscr{N}'_{|U} = \mathscr{N}$.*

Demostración. Por 12.1.14, existe un submódulo finito generado $\mathscr{N}'$ de $i_*\mathscr{M}$ tal que $\mathscr{N}'_{|U} = \mathscr{N}$. □

21. Definición: Sea $f : X \to Y$ un morfismo de esquemas y $\mathscr{M}$ un $\mathscr{O}_Y$-módulo. Llamaremos imagen inversa de $\mathscr{M}$ por f, y lo denotaremos $f^*\mathscr{M}$, al $\mathscr{O}_X$-módulo $f^*\mathscr{M} = f^{-1}\mathscr{M} \otimes_{f^{-1}\mathscr{O}_Y} \mathscr{O}_X$.

Si $S \overset{i}{\hookrightarrow} X$ es un subesquema, entonces denotaremos $\mathscr{M}_{|S}$ a $i^*\mathscr{M}$ y diremos que es la restricción de $\mathscr{M}$ a S. Si S es un abierto, entonces $i^*\mathscr{M} = i^{-1}\mathscr{M}$, es decir la restricción como haces coincide con la restricción como módulos.

22. Proposición: *Sea $f : X \to Y$ un morfismo de esquemas. Para todo $\mathscr{O}_Y$-módulo $\mathscr{M}$ y todo $\mathscr{O}_X$-módulo $\mathscr{N}$ se cumple que*

$$\mathrm{Hom}_{\mathscr{O}_Y}(\mathscr{M}, f_*\mathscr{N}) = \mathrm{Hom}_{\mathscr{O}_X}(f^*\mathscr{M}, \mathscr{N})$$

funtorialmente en $\mathscr{M}$ y $\mathscr{N}$.

Demostración. $\mathrm{Hom}_{\mathscr{O}_Y}(\mathscr{M}, f_*\mathscr{N}) = \mathrm{Hom}_{f^{-1}\mathscr{O}_Y}(f^{-1}\mathscr{M}, \mathscr{N})$, por la fórmula de adjunción de haces. Hemos concluido, ya que $\mathrm{Hom}_{f^{-1}\mathscr{O}_Y}(f^{-1}\mathscr{M}, \mathscr{N}) = \mathrm{Hom}_{\mathscr{O}_X}(f^*\mathscr{M}, \mathscr{N})$. □

23. Lema: *Sea $f : \mathrm{Spec}B \to \mathrm{Spec}A$ un morfismo entre esquemas afines. Sea M un A-módulo y N un B-módulo (en particular es un A-módulo). Se cumple que $f^*\widetilde{M} = \widetilde{M_B}$, con $M_B = M \otimes_A B$.*

Demostración. Observemos que

$$\begin{aligned}\mathrm{Hom}_{\widetilde{B}}(f^*\widetilde{M}, \mathscr{N}) &= \mathrm{Hom}_{\widetilde{A}}(\widetilde{M}, f_*\mathscr{N}) = \mathrm{Hom}_A(M, \mathscr{N}(\mathrm{Spec}B)) = \mathrm{Hom}_B(M_B, \mathscr{N}(\mathrm{Spec}B)) \\ &= \mathrm{Hom}_{\widetilde{B}}(\widetilde{M_B}, \mathscr{N})\end{aligned}$$

□

24. Ejemplos: En esquemas afines, la categoría de A-módulos es equivalente a la categoría de los módulos quasi-coherentes sobre $\operatorname{Spec} A$. Identifiquemos por un momento M con $\tilde{M}$.

1. Si $C = \operatorname{Spec} A/I \overset{i}{\hookrightarrow} \operatorname{Spec} A$ es un cerrado, entonces $M_{|C} := i^*M = M \otimes_A A/I = M/IM$. En particular, si x es un punto cerrado, entonces $M_{|x} = M/\mathfrak{m}_x M$.

2. Si $U_a \overset{i}{\hookrightarrow} \operatorname{Spec} A$ es un abierto básico, entonces $M_{|U_a} := i^*M = M \otimes_A A_a = M_a$.

25. Teorema: *Sea $X \to Y$ un morfismo de esquemas. Se cumple que:*

1. *La imagen inversa de un haz quasi-coherente es quasi-coherente.*

2. *La imagen inversa de un módulo de presentación finita es de presentación finita.*

Demostración. La cuestión es local en X y en Y. Por tanto, podemos suponer que X e Y son afines y concluimos por el lema anterior. □

12.1.3. Módulos quasi-coherentes inyectivos

26. Proposición: *Sea X un esquema compacto quasi-separado. La categoría de $\mathcal{O}_X$-módulos quasi-coherentes tiene suficientes inyectivos.*

Demostración. Sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo quasi-coherente. Sea $\{U_1, \ldots, U_n\}$ un recubrimiento de X por abiertos afines. Sea $i_j \colon U_j \hookrightarrow X$ el morfismo de inclusión. Observemos que $i_j^*\mathcal{M} = \widetilde{\mathcal{M}(U_j)}$. Sea I_j un $\mathcal{O}_X(U_j)$-módulo inyectivo que contiene a $\mathcal{M}(U_j)$, $\tilde{I}_j$ es un $\mathcal{O}_{U_j}$-módulo quasi-coherente inyectivo y tenemos un morfismo inyectivo $i_j^*\mathcal{M} \hookrightarrow \tilde{I}_j$. Por la fórmula de adjunción, $i_{j*}\tilde{I}_j$ es un $\mathcal{O}_X$-módulo quasi-coherente inyectivo y la composición

$$\mathcal{M} \hookrightarrow \prod_j i_{j*} i_j^* \mathcal{M} \hookrightarrow \prod_j i_{j*} \tilde{I}_j$$

es una inyección de $\mathcal{M}$ en un módulo quasi-coherente inyectivo. □

27. Proposición: *Sea X un esquema noetheriano y $\mathfrak{p} \subseteq \mathcal{O}_X$ un haz de ideales coherente. Denotemos $U = X \setminus (\mathfrak{p})_0$. Para todo módulo coherente $\mathcal{N}$ y todo módulo quasi-coherente $\mathcal{M}$ se cumple*

$$\varinjlim_n \operatorname{Hom}_X(\mathfrak{p}^n \mathcal{N}, \mathcal{M}) = \operatorname{Hom}_U(\mathcal{N}_{|U}, \mathcal{M}_{|U})$$

"Los morfismos con polos de orden n (variable) en $(\mathfrak{p})_0$ son los morfismos sobre $X \setminus (\mathfrak{p})_0$".

Demostración. 1. Supongamos X afín, $X = \operatorname{Spec} A$. Con las notaciones obvias, tenemos que probar que $\varinjlim_n \operatorname{Hom}_A(I^n N, M) = \Gamma(U, \underline{\operatorname{Hom}}_{\mathscr{A}}(\mathscr{N}, \mathscr{M}))$.

1.a. Supongamos que I es un ideal principal, $I = (a)$. Tenemos que probar entonces que

$$\varinjlim_n \operatorname{Hom}_A((a^n)N, M) = \operatorname{Hom}_{A_a}(N_a, M_a).$$

Se cumple que $\operatorname{Hom}_A(N_1, \varinjlim_i M_i) = \varinjlim_i \operatorname{Hom}_A(N_1, M_i)$, para todo módulo finito generado N_1. Podemos suponer que M es finito generado.

Para todo $n >> 0$ se cumple que $a^n \cdot M = \frac{a^n \cdot M}{1} \subset M_a$: Sea M' el núcleo de $M \to M_a$ y $m \in \mathbb{N}$ tal que $a^m \cdot M' = 0$. Si $n \geq m$ y $\frac{a^n \cdot m}{1} = 0$, entonces $a^n \cdot m \in M'$, luego $m \in M'$ y $a^n \cdot m = 0$.

Dado un morfismo $f : N_a \to M_a$, sea m tal que $f(a^m \cdot N) \subset \frac{M}{1}$, entonces tenemos $a^{n+m} \cdot N \to \frac{a^n \cdot M}{1} = a^n \cdot M \subset M$. Recíprocamente, dado un morfismo $a^n N \to M$, localizando en a, tenemos un morfismo $N_a \to M_a$.

1.b. Si $I = (a_1, \ldots, a_n)$, hacemos inducción sobre n. Sean $I_1 = (a_1)$, $I_2 = (a_2, \ldots, a_n)$ y U_1, U_2 los abiertos complementarios de los ceros de I_1 e I_2 respectivamente. Tenemos la sucesión exacta

$$0 \to (I_1^n N) \cap (I_2^n N) \to I_1^n N \oplus I_2^n N \to I_1^n N + I_2^n N \to 0$$

El sistema $(I_1^n N) \cap (I_2^n N)$ es equivalente a $(I_1 \cdot I_2)^n N$ por el teorema de Artin-Rees, y el sistema $I_1^n N + I_2^n N$ es equivalente a $I^n N$. Por tanto, tomando $\operatorname{Hom}_A(\ \ , M)$ y límite inductivo en la sucesión exacta anterior obtenemos por inducción

$$\begin{aligned} 0 \to \varinjlim_n \operatorname{Hom}_A(I^n N, M) &\to \Gamma(U_1, \underline{\operatorname{Hom}}_{\mathscr{A}}(\mathscr{N}, \mathscr{M})) \oplus \Gamma(U_2, \underline{\operatorname{Hom}}_{\mathscr{A}}(\mathscr{N}, \mathscr{M})) \\ &\to \Gamma(U_1 \cap U_2, \underline{\operatorname{Hom}}_{\mathscr{A}}(\mathscr{N}, \mathscr{M})) \end{aligned}$$

luego se concluye, por la condición de haz.

2. Veamos ahora el caso general. Para cada abierto afín V de X y cada módulo quasi-coherente $\mathscr{M}$, denotemos $\mathscr{M}_V = i_* \mathscr{M}_{|V}$, con $i : V \hookrightarrow X$. Por la fórmula de adjunción y por 1., la fórmula es cierta para todo módulo de la forma $\mathscr{M}_V$. Como todo módulo quasi-coherente se resuelve por módulos que son un suma directa finita de módulos de la forma $\mathscr{M}_V$ y tanto $\varinjlim_n \operatorname{Hom}_X(\mathfrak{p}^n \mathscr{N}, \mathscr{M})$ como $\operatorname{Hom}_U(\mathscr{N}_{|U}, \mathscr{M}_{|U})$ son exactos por la izquierda en $\mathscr{M}$, se concluye. □

28. Proposición: *Si $\mathscr{M}$ es un módulo quasi-coherente sobre un esquema localmente noetheriano X e I un haz quasi-coherente inyectivo, entonces $\underline{\mathrm{Hom}}_X(\mathscr{M},I)$ es un haz flasco. En particular, tomando $\mathscr{M}=\mathscr{O}_X$, obtenemos que los módulos quasi-coherentes inyectivos son flascos.*

Demostración. Un haz es flasco si y solo si es localmente flasco, luego podemos suponer que X es noetheriano.

Supongamos que $\mathscr{M}$ es coherente. Sea $U\subseteq X$ un abierto y $\mathfrak{p}$ el haz de ideales de las funciones que se anulan en $X\setminus U$. El límite inductivo de epiyecciones es una epiyección, luego el morfismo $\mathrm{Hom}_X(\mathscr{M},I)\to \varinjlim_n \mathrm{Hom}_X(\mathfrak{p}^n\mathscr{M},I)=\mathrm{Hom}_U(\mathscr{M}_{|U},I_{|U})$ es epiyectivo.

Supongamos que $\mathscr{M}$ es quasi-coherente. Recordemos que los módulos quasi-coherentes son límite inductivo de sus submódulos coherentes, por la proposición 12.1.15. Dada $s\colon \mathscr{M}_{|U}\to I_{|U}$, sea $\mathscr{N}\subseteq\mathscr{M}$ máximo (que existe por el lema de Zorn) con la condición de que exista $t\colon \mathscr{N}\to I$, de modo que $t_{|U}=s_{|\mathscr{N}_{|U}}$. Tenemos que probar que $\mathscr{N}=\mathscr{M}$. Si $\mathscr{N}\neq\mathscr{M}$, sea $\mathscr{N}'\subset\mathscr{M}$ que contenga a $\mathscr{N}$ y tal que $0\neq\mathscr{N}'/\mathscr{N}$ sea coherente. Sea $t'\colon\mathscr{N}'\to I$, tal que $t'_{|\mathscr{N}}=t$. Tenemos que $t'_{|U}$ coincide con s sobre $\mathscr{N}_{|U}$, luego sobre $\mathscr{N}'_{|U}$ se tiene que $s=t'+(\bar{s}\circ\pi')$, donde $\pi'\colon\mathscr{N}'_{|U}\to(\mathscr{N}'/\mathscr{N})_{|U}$ es el morfismo de paso al cociente y $\bar{s}$ es un morfismo de $(\mathscr{N}'/\mathscr{N})_{|U}$ en $I_{|U}$. Sea $\bar{t}\colon(\mathscr{N}'/\mathscr{N})\to I$, tal que $\bar{t}_{|U}=\bar{s}$. Entonces $t'+(\bar{t}\circ\pi)$, donde $\pi\colon\mathscr{N}'\to\mathscr{N}'/\mathscr{N}$ es el morfismo de paso al cociente, coincide con s sobre U. Contradicción. □

29. Proposición: *Sea X un esquema noetheriano y I un $\mathscr{O}_X$-módulo quasi-coherente inyectivo. Si $U\overset{i}{\subseteq}X$ es un abierto, entonces $I_{|U}$ es un módulo quasi-coherente inyectivo en U.*

Demostración. Sea $\mathscr{N}\hookrightarrow\mathscr{N}'$ una inyección de módulos coherentes en U. Sean $\mathscr{M}\subseteq\mathscr{M}'$ submódulos coherentes de $i_*\mathscr{N}'$, tales que $\mathscr{M}_{|U}=\mathscr{N}$ y $\mathscr{M}'_{|U}=\mathscr{N}'$. Sea $\mathfrak{p}$ el haz de ideales de funciones que se anulan en $X\setminus U$. Tenemos la epiyección

$$\mathrm{Hom}_U(\mathscr{N}',I_{|U})\overset{12.1.27}{=}\varinjlim_n \mathrm{Hom}_X(\mathfrak{p}^n\mathscr{M}',I)\to\varinjlim_n \mathrm{Hom}_X(\mathfrak{p}^n\mathscr{M},I)\overset{12.1.27}{=}\mathrm{Hom}_U(\mathscr{N},I_{|U})$$

que muestra que $I_{|U}$ es inyectivo en U. □

12.2. Divisores y haces de línea

Sea C una curva íntegra sobre un cuerpo k y Σ su cuerpo de funciones.

1. Definición: Un divisor sobre C es una suma formal finita $D = \sum n_x \cdot x$, con $n_x \in \mathbb{Z}$ y $x \in C$ puntos cerrados.

Diremos que $D = \sum n_x \cdot x \leq D' = \sum n_{x'} \cdot x'$ cuando $n_x \leq n_{x'}$ para todo x. Llamaremos soporte de un divisor $D = \sum n_x \cdot x$, al cerrado $|D|$ de los $x \in C$ tales que $n_x \neq 0$. Se dice que D es un divisor efectivo si $n_x \geq 0$ para todo x.

2. Definición: Llamaremos grado de un divisor $D = \sum n_x \cdot x$, que denotamos $\mathrm{gr}\, D$, a

$$\mathrm{gr}\, D = \sum n_x \cdot \mathrm{gr}(x),$$

siendo $\mathrm{gr}(x) = \dim_k(\mathscr{O}_{C,x}/\mathfrak{m}_x)$.

Supongamos de ahora en adelante, en esta sección, que C es no singular. Para cada punto cerrado $x \in C$ sea v_x la valoración definida por el anillo de valoración $\mathscr{O}_{C,x}$. Dada $f \in \Sigma$ sea $n_x = v_x(f)$. Si $n_x > 0$ se dice que f tiene un cero de orden n_x en x, y si $n_x < 0$ se dice que f tiene un polo de orden $-n_x$ en x.

3. Definición: Llamaremos divisor de ceros y polos de $f \in \Sigma$ al divisor

$$D(f) := \sum_{x \in C} v_x(f) \cdot x.$$

Para que esta definición sea correcta la suma $\sum v_x(f) \cdot x$ ha de ser finita. Necesitamos, pues, la siguiente proposición.

4. Proposición: *Una función racional $f \in \Sigma$ tiene un número finito de ceros y polos.*

Demostración. Dado un abierto afín $U = \mathrm{Spec}\, A$ de C, tendremos que $f = \frac{a}{b}$, con $a, b \in \mathscr{O}_C(U)$. Es claro que los ceros de f en U están incluidos en $(a)_0$ y que los polos de f en U están incluidos en $(b)_0$, que son un número finito de puntos. Como C se recubre por un número finito de abiertos afines se concluye. □

5. Proposición: *Si C es completa, entonces $\Gamma(C, \mathscr{O}_C) = \bar{k}$, siendo $\bar{k}$ el cierre entero de k en Σ.*

Demostración. $\Gamma(C, \mathscr{O}_C) = \bigcap_{v \in C} \mathscr{O}_v = \{\text{cierre entero de } k \text{ en } \Sigma\} = \bar{k}$ □

Por tanto, si C es completa, $\bar{k}$ son las únicas funciones $f \in \Sigma$ sin polos. Como $\bar{k}$ es un cuerpo, tendremos que $\bar{k}$ coincide también con las funciones $f \in \Sigma$ sin ceros.

6. Teorema: *Sea C una curva completa y no singular sobre un cuerpo k y Σ su cuerpo de funciones. El grado del divisor de ceros y polos de $f \in \Sigma$ es cero. Es decir, "el número de ceros de f es igual al número de polos".*

Demostración. Si $f \in \bar{k}$, entonces no tiene ni ceros ni polos, y el teorema es inmediato. Sea pues, $f \in \Sigma$ trascendente. El morfismo $k(x) \to \Sigma, x \mapsto f$, induce un morfismo finito entre las variedades de Riemann

$$\begin{aligned} \widetilde{f}\colon C &\to \mathbb{P}^1 \\ \alpha &\mapsto f(\alpha) \end{aligned}$$

Es fácil comprobar que la fibra del "origen" es igual al divisor de ceros de f y la fibra del "infinito" es igual al de divisor de polos de f. Es decir, $D(f) = \tilde{f}^{-1}(0) - \tilde{f}^{-1}(\infty)$. Por el ejercicio 11.4.22, $\mathrm{gr}(D(f)) = 0$.

□

7. Ejemplo: Sea $C = \mathbb{P}^1_k = \mathrm{Proj}\, k[x_0, x_1]$, de cuerpo de fracciones $\Sigma = k[\frac{x_1}{x_0}]$. Calculemos los ceros y polos de la función x^2, $x = x_1/x_0$. Tenemos que $\mathbb{P}^1_k = \mathrm{Spec}\, k[x] \cup \mathrm{Spec}\, k[1/x] = \mathrm{Spec}\, k[x] \cup \infty$, con $\mathfrak{m}_\infty = (1/x) \subset k[1/x]$. En $\mathrm{Spec}\, k[x]$, x^2 no tiene más ceros que el origen $\mathfrak{m}_0 = (x)$ y no tiene polos; además, $v_0(x^2) = 2$. Por último, $v_\infty(x^2) = v_\infty((1/x)^{-2}) = -2$. En conclusión, $D(x^2) = 2 \cdot 0 - 2 \cdot \infty$.

8. Ejercicio: Calcular el divisor de ceros y polos de x sobre la variedad de Riemann del cuerpo de fracciones de $k[x,y]/(y^2 - x^3)$.

Llamaremos suma de dos divisores $D = \sum n_x \cdot x$, $D' = \sum n'_x \cdot x$, a $D + D' = \sum (n_x + n'_x) \cdot x$. El conjunto de todos los divisores de una curva no singular es un grupo abeliano libre que denotaremos $\mathrm{Div}\, C$.

9. Definición: Se dice que dos divisores son linealmente equivalentes si difieren en el divisor de una función. Es decir, D es linealmente equivalente a D' si existe $f \in \Sigma$ tal que $D = D' + D(f)$, y lo denotaremos $D \sim D'$.

Es claro que la equivalencia lineal es una relación de equivalencia. Además, el conjunto de las clases de divisores linealmente equivalentes, con la suma de divisores, es un grupo abeliano.

10. Definición: Sea X un esquema. Diremos que un $\mathscr{O}_X$-módulo $\mathscr{L}$ es un haz de línea si existe un recubrimiento de X por abiertos U_i tales que $\mathscr{L}_{|U_i} \simeq \mathscr{O}_{U_i}$.

Dados dos haces de línea $\mathscr{L}, \mathscr{L}'$, su producto tensorial $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{L}'$ es un haz de línea. El conjunto de clases de isomorfía de los haces de línea, con el producto tensorial, es un grupo abeliano donde:

1. El elemento neutro es $\mathscr{O}_X$.

2. El inverso del haz de línea $\mathscr{L}$ es $\mathscr{L}^{-1} = \underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{L}, \mathscr{O}_X)$. En efecto, se tiene un morfismo natural $\mathscr{L} \otimes_{\mathscr{O}_X} \underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{L}, \mathscr{O}_X) \to \mathscr{O}_X$, $e \otimes w \mapsto w(e)$, que es un isomorfismo, como puede comprobarse localmente, en abiertos donde $\mathscr{L}$ sea libre.

11. Definición: El grupo de las clases de isomorfía de haces de línea sobre X se denomina grupo de Picard de X y se denota $\mathrm{Pic}(X)$.

Para cada número natural n, denotamos $\mathscr{L}^n = \mathscr{L}\otimes\overset{n}{\cdots}\otimes\mathscr{L}$ y $\mathscr{L}^{-n} = \mathscr{L}^{-1}\otimes\overset{n}{\cdots}\otimes\mathscr{L}^{-1} = (\mathscr{L}^n)^{-1}$.

12. Notación: Dado un divisor $D = \sum n_x \cdot x$ sobre una curva C y un abierto $U \subset C$, denotaremos $D_{|U} = \sum_{x\in U} n_x \cdot x$.

13. Ejemplos: 1. Sea $x \in C$ un punto cerrado. Sea $\mathfrak{m}_x$ el subhaz de ideales de $\mathscr{O}_C$ que define x, esto es, el núcleo del epimorfismo $\mathscr{O}_C \to i_*k(x)$, con $i\colon x \hookrightarrow C$ el morfismo obvio. Si U es un abierto que no contiene a x, entonces $\mathfrak{m}_{x|U} = \mathscr{O}_U$. Si $x \in U$, empequeñeciendo U si es preciso, existe $t_x \in \Sigma_C$ tal que $v_y(t_x) = 0$ para todo $y \in U\backslash x$ y $v_x(t_x) = 1$. Entonces $\mathfrak{m}_{x|U} = t_x \cdot \mathscr{O}_{X|U}$. En conclusión, $\mathfrak{m}_x$ es un haz de línea y también se denota $\mathfrak{m}_x = \mathscr{L}_{-x}$.

2. Haz de línea asociado a un divisor: Sea $D = \sum n_x \cdot x$ un divisor sobre una curva C. Sea $\mathscr{L}_D$ el subhaz de $\widetilde{\Sigma}$ definido por

$$\mathscr{L}_D(U) = \{f \in \Sigma \text{ tales que } (Df)_U + D_U \geq 0\}.$$

Veamos que $\mathscr{L}_D$ es un haz de línea. Evidentemente $\mathscr{L}_D$ es un $\mathscr{O}_C$-módulo. Tenemos que ver que localmente es isomorfo a $\mathscr{O}_C$. Dado $x \in |D|$, sea U un abierto afín tal que $U \cap |D| = x$. Empequeñeciendo U si es preciso, podemos suponer que existe una función, $t_x \in \Sigma$, tal que $(Dt_x)_{|U} = x$. Se sigue trivialmente que $(\mathscr{L}_D)_{|U} = t_x^{-n_x} \cdot \mathscr{O}_U$. Por último, $\mathscr{L}_{|C-|D|} = \mathscr{O}_{C-|D|}$.

14. Teorema: *La correspondencia $D \mapsto \mathscr{L}_D$ establece un isomorfismo entre el grupo de las clases de divisores linealmente equivalentes sobre una curva no singular C y el grupo de las clases de isomorfía de los haces de línea.*

Demostración. Si $D' = D + D(g)$, entonces para cada abierto U se tiene un isomorfismo $\mathscr{L}_{D'}(U) \xrightarrow{\cdot g} \mathscr{L}_D(U)$ y por tanto un isomorfismo $\mathscr{L}_{D'} \simeq \mathscr{L}_D$.

La asignación $D \mapsto \mathscr{L}_D$ es de grupos. En efecto, para cada abierto U se tiene un morfismo natural $\mathscr{L}_D(U)\otimes\mathscr{L}_{D'}(U) \to \mathscr{L}_{D+D'}(U)$, $f\otimes g \mapsto f\cdot g$, luego se tiene un morfismo $\mathscr{L}_D \otimes \mathscr{L}_{D'} \to \mathscr{L}_{D+D'}$. Para ver que es isomorfismo, basta verlo localmente, en cuyo caso el morfismo es $t_x^{-n_x}\cdot\mathscr{O}_U \otimes t_x^{-n'_x}\cdot\mathscr{O}_U = t_x^{-n_x-n'_x}\cdot\mathscr{O}_U$.

Construyamos la asignación inversa. Dado un haz de línea $\mathscr{L}$, fijemos un isomorfismo $\phi_g\colon \mathscr{L}_g \simeq \Sigma$ de Σ-espacios vectoriales, siendo g el punto genérico de C. Este isomorfismo define un morfismo inyectivo $\mathscr{L} \hookrightarrow \widetilde{\Sigma}$, que podemos suponer que es una inclusión para simplificar las notaciones. Si U es un abierto afín sobre el que $\mathscr{L}$ es libre, entonces $\mathscr{L}(U) = f_U \cdot \mathscr{O}_C(U)$ para cierta $f_U \in \Sigma$. Obsérvese que $D(f_U)_{|U}$ no depende

del f_U escogido, porque cualquier otro escogido es $\lambda \cdot f_U$, con λ invertible en U, luego $D(\lambda \cdot f_U)_{|U} = D(f_U)_{|U}$.

Asignamos a $\mathscr{L}$ el divisor $D_{\mathscr{L}}$ definido localmente por $(D_{\mathscr{L}})_{|U} = -D(f_U)_{|U}$, para cada abierto afín U sobre el que $\mathscr{L}$ es libre.

1. $D_{\mathscr{L}}$ está bien definido, es decir, $(D_{\mathscr{L}})_{|U}$ coincide con $(D_{\mathscr{L}})_{|U'}$ sobre $U \cap U'$, porque f_U y $f_{U'}$ difieren, en $U \cap U'$, en una función invertible.

2. Si $\phi' : \mathscr{L}_g \to \Sigma_C$ es otro isomorfismo, entonces $\phi' = g \cdot \phi$ para alguna función $g \in \Sigma$. Por tanto, si $D'_{\mathscr{L}}$ es el divisor construido a partir de ϕ', entonces $D'_{\mathscr{L}} = D_{\mathscr{L}} - D(g)$.

Para concluir, es fácil comprobar que el haz de línea asociado a $D_{\mathscr{L}}$ es $\mathscr{L}$, una vez que hemos identificado $\mathscr{L}$ con un subhaz de $\widetilde{\Sigma}$, es decir, una vez que prefijamos un isomorfismo $\mathscr{L}_g \simeq \Sigma$. Recíprocamente, el divisor asociado a $\mathscr{L}_D$ es D. □

15. Proposición: *El grupo de Picard de la recta proyectiva es isomorfo a $\mathbb{Z}$, es decir*

$$\mathrm{Pic}(\mathbb{P}^1) \simeq \mathbb{Z}$$

Demostración. El grado define un morfismo de grupos $\mathrm{gr} : \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}$, claramente epiyectivo. Por el teorema 12.2.6, si dos divisores son linealmente equivalentes, entonces tienen el mismo grado. Por tanto, se tiene un morfismo epiyectivo

$$\mathrm{gr} : \mathrm{Div}(\mathbb{P}^1)/\sim = \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$$

Construyamos el inverso. $\mathbb{P}^1$ es la variedad de Riemann de $k(x)$ y $\mathbb{P}^1 = \mathrm{Spec}\, k[x] \cup \mathrm{Spec}\, k[\frac{1}{x}] = \mathrm{Spec}\, k[x] \cup \infty$. Definimos $\mathbb{Z} \to \mathrm{Pic}(\mathbb{P}^1)$ como $n \mapsto n \cdot \infty$. Para concluir, basta ver que todo divisor D es equivalente a $(\mathrm{gr}\, D) \cdot \infty$.

Sea $p(x) = a_0 x^n + \cdots + a_n \in k[x]$ un polinomio irreducible de grado n. Denotemos por p el punto de $\mathrm{Spec}\, k[x]$ definido por el ideal maximal $(p(x))$ de $k[x]$. Obsérvese que

$$v_\infty(p(x)) = v_\infty\left(\frac{p(x)}{x^n} \cdot x^n\right) = v_\infty\left((a_0 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n}) \cdot (\frac{1}{x})^{-n}\right) = 0 + (-n) = -n$$

Por tanto, $D(p(x)) = 1 \cdot p - n \cdot \infty$, es decir $1 \cdot p \sim \mathrm{gr}\, p \cdot \infty$ y en general $D \sim (grD) \cdot \infty$. □

16. Proposición: *Sea C una curva completa y no singular sobre un cuerpo k algebraicamente cerrado. Si $\mathrm{Pic}(C) = \mathbb{Z}$, entonces $C = \mathbb{P}^1_k$.*

Demostración. El grado define un morfismo $\mathrm{Pic}(C) \to \mathbb{Z}$, claramente epiyectivo, y por hipótesis ($\mathrm{Pic}(C) = \mathbb{Z}$) isomorfismo. Por tanto, $\mathrm{Pic}(C) = \mathbb{Z} \cdot p$, siendo p cualquier punto cerrado de C. En consecuencia, si q es otro punto cerrado, entonces $p - q$ es linealmente equivalente al divisor de ceros y polos de una función $f \in \Sigma_C$. Por tanto, el morfismo $\widetilde{f} : C \to \mathbb{P}^1, \alpha \mapsto f(\alpha)$, es un morfismo de grado 1, es decir, un isomorfismo. □

17. Ejercicio: Prueba que si $\operatorname{gr} D < 0$, entonces $\Gamma(C, \mathscr{L}_D) = 0$.

18. Proposición: *Sea C una curva completa y no singular de cuerpo de fracciones Σ y $\mathscr{L}$ un haz de línea en C. Sea g el punto genérico de C y $s \in \mathscr{L}_g \simeq \Sigma$. Definamos $v_x(s) = n$ si $s \in \mathfrak{m}_x^n \mathscr{L}_x$ y $s \notin \mathfrak{m}_x^{n+1}\mathscr{L}_x$. Entonces, el haz de línea asociado al "divisor de ceros y polos de s", $D(s) := \sum_x v_x(s) \cdot x$, es $\mathscr{L}$.*

Demostración. El isomorfismo es $\mathscr{L}_{D(s)} \xrightarrow{\cdot s} \mathscr{L}$, $f \mapsto f \cdot s$. □

Si $D' = D(s) + D(f)$, $f \in \Sigma_C$, entonces $D' = D(f \cdot s)$. Por tanto, módulo k (supongamos $\bar{k} \cap \mathscr{O}_C(C) = k$), las secciones de $\mathscr{L}_g$ se corresponden biyectivamente con el conjunto de divisores equivalentes a $D(s)$. Obsérvese que $D(s)$ es un divisor efectivo si y solo si $s \in \Gamma(C, \mathscr{L})$. Por tanto, $\mathbb{P}(\Gamma(C, \mathscr{L})) = \{\text{Divisores efectivos equivalentes a } D(s)\}$.

Dado un divisor efectivo $D = \sum_i n_i x_i$ podemos considerarlo como un subesquema cerrado de C definiendo $D = \operatorname{Spec} \mathscr{O}_C/\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$. Observemos que $\mathscr{O}_D(D) = \oplus_i \mathscr{O}_{C,x_i}/\mathfrak{m}_{x_i}^{n_i}$, luego $\dim_k \mathscr{O}_D(D) = \operatorname{gr} D$. Recíprocamente, dado un subesquema cerrado $D \subset C$ (distinto de C), el haz de ideales $\mathfrak{p}_D \subset \mathscr{O}_C$ de funciones que se anulan en D, es $\mathfrak{p}_D = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, $x_i \in D$ y ciertos $n_i \in \mathbb{N}$, y podemos asociarle el divisor efectivo $\sum_i n_i x_i$.

Observemos que $\operatorname{Hom}_{\mathscr{O}_C}(\mathscr{L}^{-1}, \mathscr{O}_C) = \operatorname{Hom}_{\mathscr{O}_C}(\mathscr{O}_C, \mathscr{L}) = \Gamma(C, \mathscr{L})$ y dada $s \in \Gamma(C, \mathscr{L})$ tenemos la sucesión exacta

$$0 \to \mathscr{L}^{-1} \xrightarrow{s} \mathscr{O}_C \to i_* \mathscr{O}_{D(s)} \to 0$$

donde $i : D(s) \hookrightarrow C$ es el morfismo natural de inclusión.

Hemos hablado de divisores en curvas, los cuales se obtienen localmente como ceros y polos de funciones. El grupo de Picard de una curva es un invariante importante en el estudio de la geometría intrínseca de la curva. En variedades algebraicas de dimensión mayor, los ceros y polos de funciones son hipersuperficies y los divisores serán sumas formales de hipersuperficies. Como en curvas, veremos la correspondencia entre los divisores y los haces de línea.

Decimos que un punto x de un esquema X es de codimensión r si $\dim \mathscr{O}_{X,x} = r$. Si X es una variedad algebraica irreducible de dimensión n, un punto $x \in X$ es de codimensión 1, si y solo si $\dim \bar{x} = n - 1$.

19. Definición: Diremos que un esquema X es regular en codimensión 1, si $\mathscr{O}_{X,x}$ es un anillo regular para todo punto $x \in X$, tal que $\dim \mathscr{O}_{X,x} = 1$.

Por ejemplo, si X es normal (es decir, para todo abierto afín U de X, el anillo $\mathscr{O}_X(U)$ es un anillo íntegro e íntegramente cerrado en su cuerpo de fracciones), entonces X es regular en codimensión 1. Por tanto, los esquemas no singulares (ver 7.5.9), los espacios proyectivos $\mathbb{P}_k^n$ o las curvas no singulares son regulares en codimensión 1.

20. Definición: Sea X un esquema íntegro y regular en codimensión 1. Llamaremos divisor de Weil de X a una suma formal finita, $\sum_i n_i \cdot x_i$, con $n_i \in \mathbb{Z}$ y $x_i \in X$ de codimensión 1.

El conjunto de divisores de Weil es un grupo abeliano, con la suma obvia.

21. Definición: Sea X un esquema noetheriano, íntegro y regular en codimensión 1. Sea g el punto genérico de X y $\Sigma = \mathcal{O}_{X,g}$ el cuerpo de funciones de X. Para cada $f \in \Sigma$, llamaremos divisor de Weil asociado a f a

$$D(f) = \sum_{\operatorname{codim} x = 1} v_x(f) \cdot x$$

($\mathcal{O}_{X,x}$ es un anillo regular de dimensión 1, luego de valoración discreta y podemos hablar de $v_x(f)$). Los divisores de Weil de la forma $D(f)$ se denominan principales.

Para que esta definición sea correcta tenemos que ver que la suma $\sum_{\operatorname{codim} x = 1} v_x(f) \cdot x$ es finita. Como X se recubre por un número finito de abiertos afines, podemos suponer que $X = \operatorname{Spec} A$ es afín. Entonces $f = \frac{a}{b}$, con $a, b \in A$, y $v_x(f) = v_x(a) - v_x(b)$. Por tanto, basta ver que si $c \in A$, entonces $v_x(c) \neq 0$ para un número finito de puntos x de codimensión 1. Los puntos $x \in X$ de codimensión 1 tales que $v_x(c) > 0$ son los puntos x de codimensión 1 tales que $c \in \mathfrak{p}_x$, es decir, son los ideales primos minimales de $A/(c)$, que son un número finito por noetherianidad.

22. Definición: Dos divisores de Weil se dicen equivalentes si su diferencia es un divisor principal. Denotaremos $Cl(X) = \{\text{Div. Weil de } X\}/\sim$.

23. Ejemplo: Veamos que $Cl(\mathbb{P}^n_k) \simeq \mathbb{Z}$.

Sean $U_0, \ldots, U_n$ los abiertos afines estándar de $\mathbb{P}^n_k$. Sea $x \in \mathbb{P}^n_k = \operatorname{Proj} k[x_0, \ldots, x_n]$ un punto de codimensión 1. Supongamos que $x \in U_0 = \operatorname{Spec} k[y_1, \ldots, y_n]$, con $y_i = x_i/x_0$. Sea $p(y_1, \ldots, y_n) \in \mathfrak{p}_x$ un polinomio irreducible. Como $(p(y_1, \ldots, y_n))$ es un ideal primo, ha de coincidir con $\mathfrak{p}_x$, por codimensiones. Si $p(y_1, \ldots, y_n) = \frac{p_r(x_0, \ldots, x_n)}{x_0^r}$, (con $p_r(x_0, \ldots, x_n)$ irreducible), entonces x es el punto genérico de la hipersuperficie definida por los ceros de $p_r(x_0, \ldots, x_n)$.

Sea H_0 el punto genérico del hiperplano complementario de U_0. Para todo y de codimensión 1 distinto de x y de H_0 se cumple que $v_y(p(y_1, \ldots, y_n)) = 0$. Por otra parte, $v_x(p(y_1, \ldots, y_n)) = 1$ y $v_{H_0}(p(y_1, \ldots, y_n)) = v_{H_0}((\frac{x_0}{x_1})^{-r} \cdot \frac{p_r}{x_1^r}) = v_{H_0}((\frac{x_0}{x_1})^{-r}) = -r$. En conclusión, $D(p(y_1, \ldots, y_n)) = x - rH_0$. Si x es el punto genérico de una hipersuperficie de grado r, diremos que $\operatorname{gr} x = r$. Tenemos por tanto que $\sum_i n_i \cdot x_i \sim (\sum_i n_i \operatorname{gr} x_i) \cdot H_0$. Así pues, el morfismo $\mathbb{Z} \to Cl(\mathbb{P}^n)$, $n \mapsto nH_0$, es epiyectivo. Dejamos al lector que pruebe la inyectividad.

Sea X un esquema. Denotemos K el prehaz de anillos sobre X definido por $K(U) = \mathcal{O}_X(U)_S$, donde $S := \{s \in \mathcal{O}_X(U) : \ s_x \in \mathcal{O}_{X,x}$ es un no divisor de cero, para todo $x \in U\}$. Sea $\mathcal{O}_X^*$ el haz de elementos invertibles de $\mathcal{O}_X$ y de K^* el prehaz de los elementos invertibles de K. Si X es íntegro de cuerpo de funciones Σ, entonces el haz asociado a K^* es el haz constante $\Sigma^* = \Sigma\backslash\{0\}$. Denotaremos $\mathfrak{C}$ el haz asociado al prehaz $K^*/\mathcal{O}_X^*$.

24. Ejercicio: Prueba que $K^*(U) = \{\frac{s}{s'} \in \mathcal{O}_X(U)_S : s, s' \in S\}$, donde seguimos las notaciones que preceden.

25. Definición: Un divisor de Cartier de un esquema X es una sección global de $\mathfrak{C}$. El conjunto de divisores de Cartier es un grupo abeliano (multiplicativo). Diremos que un divisor de Cartier es principal si pertenece a la imagen del morfismo natural $K^*(X) \to \mathfrak{C}(X)$. Diremos que dos divisores de Cartier son linealmente equivalentes si difieren en un divisor de Cartier principal.[1]

Veamos que un divisor de Cartier D define un subhaz de línea $\mathcal{L}_D$ de K. Para dar D hay que dar un recubrimiento abierto $\{U_i\}$ de X y secciones $f_i \in K^*(U_i)$ tales que $\frac{f_i}{f_j} \in \mathcal{O}_X^*(U_i \cap U_j)$. Sea $(\mathcal{L}_D)_{|U_i} = f_i \cdot \mathcal{O}_{U_i} \subset K_{|U_i}$. Esto define un haz de línea $\mathcal{L}_D$ en X, porque f_i y f_j difieren, en $U_i \cap U_j$, en un invertible de $\mathcal{O}_X(U_i \cap U_j)$, luego $f_i \cdot \mathcal{O}_{U_i \cap U_j} = f_j \cdot \mathcal{O}_{U_i \cap U_j}$. El haz de línea $\mathcal{L}_D$, que es un subhaz de K, no depende del recubrimiento $\{U_i\}$ escogido, porque dado $x \in X$, el germen de D en x es, salvo invertibles de $\mathcal{O}_{X,x}$, una función $f_x \in K_x^*$ y $(\mathcal{L}_D)_x = f_x \cdot \mathcal{O}_{X,x}$.

26. Teorema: *Sea X un esquema. La correspondencia $D \mapsto \mathcal{L}_D$ establece un isomorfismo de grupos entre el grupo de los divisores de Cartier de X y los subhaces de línea de K. Además, $D \sim D'$ si y solo si $\mathcal{L}_D \simeq \mathcal{L}_{D'}$.*

Demostración. Sea $\mathcal{L} \subset K$ un subhaz de línea. Consideremos un recubrimiento de X por abiertos U_i tales que $\mathcal{L}_{|U_i} \simeq \mathcal{O}_{U_i}$. Entonces $\mathcal{L}_{|U_i} = f_i \cdot \mathcal{O}_{U_i}$, para una $f_i \in K(U_i)$ no divisora de cero (única salvo invertibles de $\mathcal{O}_X(U_i)$), luego $f_i \in K^*(U_i)$. Estas f_i definen una sección global $D_{\mathcal{L}}$ de $\mathfrak{C}$.

Las asignaciones $D \mapsto \mathcal{L}_D$, $\mathcal{L} \mapsto D_{\mathcal{L}}$ son inversas entre sí. Dejamos que el lector termine con la demostración del teorema. □

27. Corolario: *Si X es un esquema íntegro, entonces el grupo de los divisores de Cartier módulo la equivalencia lineal es isomorfo al grupo de Picard de X.*

Demostración. Solo tenemos que probar que todo haz de línea $\mathcal{L}$ de X es isomorfo a un subhaz de línea de K. Sea $g \in X$ el punto genérico y Σ el cuerpo de fracciones de X.

[1] Sea X un esquema íntegro y consideremos la sucesión exacta $1 \to \mathcal{O}_X^* \to \Sigma^* \to \Sigma^*/\mathcal{O}_X^* \to 1$. Es trivial, una vez definidos los grupos de cohomología, que los divisores de Cartier módulo la equivalencia lineal se identifican con $H^1(X, \mathcal{O}_X^*)$.

K es el prehaz constante Σ. Como $\mathscr{L}_g \simeq \mathscr{O}_{X,g} = \Sigma$, tenemos inclusiones $\mathscr{L}(U) \hookrightarrow \mathscr{L}_g \simeq \Sigma = K(U)$. Hemos concluido. □

28. Definición: Diremos que un esquema X es localmente factorial si $\mathscr{O}_{X,x}$ es un dominio de factorización única para todo $x \in X$.

Si X es un esquema íntegro noetheriano localmente factorial, entonces es un esquema normal, porque lo es localmente. Los esquemas íntegros y no singulares son localmente factoriales (por 7.5.15).

29. Proposición: *Sea X un esquema noetheriano, íntegro y localmente factorial. El grupo de los divisores de Weil de X es canónicamente isomorfo al grupo de los divisores de Cartier.*

Demostración. Sea Σ el cuerpo de funciones de X. Dado un divisor de Cartier, definido por un recubrimiento de X por abiertos U_i y secciones $f_i \in K^*(U_i) = \Sigma$, tales que $\frac{f_i}{f_j} \in \mathscr{O}_X^*(U_i \cap U_j)$, le asociamos el divisor de Weil D definido localmente por $D_{|U_i} = -D(f_i)_{|U_i}$.

Recíprocamente, sea $D = \sum_{i=1}^{s} n_i \cdot x_i$ un divisor de Weil. Para cada $y \in X$ existe un entorno abierto afín $U_y = \operatorname{Spec} A$ de y tal que $(\mathfrak{p}_{x_i})_{|U_y} = (f_{iy}) \subset A$, para todo $i = 1, \ldots, s$. Un número finito de ellos, $\{U_{y_1}, \ldots, U_{y_r}\}$, recubren X. Denotemos $f_j = \prod_{i=1}^{s} f_{iy_j}^{-n_i} \in K^*(U_{y_j}) = \Sigma$. Se cumple que $\frac{f_i}{f_j} \in \mathscr{O}_X^*(U_{y_i} \cap U_{y_j})$, luego definen un divisor de Cartier.

□

12.3. Módulos quasi-coherentes en esquemas proyectivos

1. Definición: Sea $R = \bigoplus_{n \in \mathbb{Z}} R_n$ un anillo graduado, $X = \operatorname{Proj} R$, $\mathscr{O} = \widetilde{R}$ el haz estructural. Para cada R-módulo graduado $M = \bigoplus_{n \in \mathbb{Z}} M_n$, llamaremos haz de localizaciones homogéneas de M, y lo denotaremos $\widetilde{M}$, al haz sobre X asociado al prehaz (denominado prehaz de localizaciones homogéneas de M)

$$U \rightsquigarrow [M_U]_0 = \left\{ \begin{array}{ll} \frac{m}{f} \in M_U, & \text{con } m \in M,\ f \in R \text{ homogéneos del mismo grado} \\ & \text{y } f \text{ no nula en ningún punto de } U \end{array} \right\}$$

Supondremos para simplificar que $R = R_0[\xi_1,\dots,\xi_n]$ con ξ_i de grado 1, y denotaremos U_i el abierto de X complementario de los ceros de ξ_i. Igual que veíamos para el haz estructural de X, se cumple que

$$\widetilde{M}_{|U_i} = \widetilde{[M_{\xi_i}]_0}$$

Por tanto, $\widetilde{M}$ es un $\mathcal{O}$-módulo quasi-coherente.

2. Proposición : *Sea R_0 un anillo noetheriano, $R = R_0[\xi_1,\dots,\xi_n]$ y $f : M \to M'$ un morfismo de R-módulos graduados finito generados. Entonces, el morfismo inducido $\widetilde{f} : \widetilde{M} \to \widetilde{M'}$ es un isomorfismo si y solo si $M_n = M'_n$, para todo $n >> 0$.*

Demostración. El morfismo $\widetilde{f}$ es isomorfismo si y solo si $0 = \operatorname{Ker}\widetilde{f} = \widetilde{\operatorname{Ker} f}$ y $0 = \operatorname{Coker}\widetilde{f} = \widetilde{\operatorname{Coker} f}$. Por tanto, basta probar que un R-módulo graduado finito generado M cumple que $\widetilde{M} = 0$ si y solo si $M_n = 0$, para todo $n >> 0$. Veamos solo la implicación directa. Si $\widetilde{M} = 0$ entonces $[M_{\xi_i}]_0 = 0$, para todo i, luego $M_{\xi_i} = 0$, para todo i. Escribamos $M = \langle m_1,\dots,m_r\rangle$, con m_i homogéneos. Entonces, existen n_i, tales que $\xi_i^{n_i}\cdot m_j = 0$, para todo j. Sea $n_1 = \sum_i n_i$ y n_2 el máximo de los grados de los m_j. Ahora es fácil ver que $M_n = 0$, para todo $n > n_1 + n_2$. □

Notación: Sea M un R-módulo graduado. Para cada $n \in \mathbb{Z}$, denotaremos $M(n)$ al R-módulo graduado cuya componente de grado r es la componente de grado $n+r$ de M. Denotaremos por $\mathcal{O}(n)$ al haz $\widetilde{R(n)}$.

Se tiene un isomorfismo $\widetilde{M} \otimes_{\mathcal{O}} \mathcal{O}(n) \simeq \widetilde{M(n)}$, inducido por el isomorfismo de R-módulos graduados $M \otimes_R R(n) \simeq M(n)$. En particular, $\mathcal{O}(n)\otimes\mathcal{O}(m) = \mathcal{O}(n+m)$.

Para cada número natural n, se tiene un morfismo graduado $R \to R(n)$ consistente en multiplicar por ξ_i^n, que induce un morfismo de haces

$$\mathcal{O} \xrightarrow{\cdot\xi_i^n} \mathcal{O}(n)$$

que es isomorfismo al restringir a U_i. Por tanto, $\mathcal{O}(n)$ es un haz de línea y su inverso es $\mathcal{O}(-n)$.

Para cada $\mathcal{O}$-módulo quasi-coherente $\mathcal{M}$ denotaremos $\mathcal{M}(n) = \mathcal{M}\otimes_{\mathcal{O}}\mathcal{O}(n)$. El morfismo $\mathcal{O} \xrightarrow{\cdot\xi_i} \mathcal{O}(1)$, induce, tensando por $\mathcal{M}(n)$, un morfismo

$$\mathcal{M}(n) \xrightarrow{\cdot\xi_i} \mathcal{M}(n+1).$$

Por otra parte, el morfismo

$$\mathcal{M} \xrightarrow{\cdot\xi_i^n} \mathcal{M}(n)$$

inducido por $\mathcal{O} \xrightarrow{\cdot\xi_i^n} \mathcal{O}(n)$, es isomorfismo al restringir a U_i

$$\mathcal{M}_{|U_i} \simeq \mathcal{M}(n)_{|U_i}.$$

Por tanto se tienen morfismos $\mathcal{M}(n) \to i_*(\mathcal{M}_{|U_i})$ consistentes en restringir a U_i y multiplicar por ξ_i^{-n}. Además se tiene un diagrama conmutativo

$$\begin{array}{ccc} \mathcal{M}(n+1) & \longrightarrow & i_*(\mathcal{M}_{|U_i}) \\ {\scriptstyle \cdot\xi_i}\uparrow & \nearrow & \\ \mathcal{M}(n) & & \end{array}$$

y por tanto se tiene un morfismo

$$\varinjlim_n \mathcal{M}(n) \to i_*(\mathcal{M}_{|U_i})$$

3. Proposición: *El morfismo anterior* $\varinjlim_n \mathcal{M}(n) \to i_*(\mathcal{M}_{|U_i})$ *es un isomorfismo.*

Demostración. Restringiendo a un abierto afín se reduce a probar que si M es un A-módulo y consideramos el sistema inductivo $M_n = M$ cuyos morfismos $M_n \to M_{n+1}$ consisten en multiplicar por $a \in A$, entonces

$$\varinjlim_n M_n = M_a$$

lo cual es sencillo. □

La igualdad $\varinjlim_n \mathcal{M}(n) = i_*(\mathcal{M}_{|U_i})$ se puede leer: "las secciones de $\mathcal{M}$ regulares en U_i son las secciones globales meromorfas de $\mathcal{M}$ que tienen polo (de orden finito) solo en $X \setminus U_i$".

Los morfismos naturales $R_n \to \Gamma(X, \mathcal{O}(n))$ definen un morfismo $R \to \oplus_n \Gamma(X, \mathcal{O}(n))$ de R_0-álgebras graduadas. Por tanto, para cada $\mathcal{O}$-módulo $\mathcal{M}$, la suma $\oplus_n \Gamma(X, \mathcal{M}(n))$ tiene una estructura natural de R-módulo graduado.

4. Teorema: *Todo módulo quasi-coherente* $\mathcal{M}$ *sobre* $X = \operatorname{Proj} R$ *es la localización homogénea del módulo graduado* $\bigoplus_{n \in \mathbb{N}} \Gamma(X, \mathcal{M}(n))$.

Demostración. Sea $M = \bigoplus_{n\in\mathbb{N}} \Gamma(X, \mathscr{M}(n))$. Entonces

$$\Gamma(U_i, \widetilde{M}) = \bigcup_n \frac{\Gamma(X, \mathscr{M}(n))}{\xi_i^n} = \varinjlim_n \Gamma(X, \mathscr{M}(n)) = \Gamma(X, \varinjlim_n \mathscr{M}(n)) = \Gamma(X, i_* \mathscr{M}_{|U_i}) = \mathscr{M}(U_i)$$

donde hemos utilizado que el límite inductivo conmuta con la toma de secciones. □

5. Ejercicio: Demuéstrese que todo haz finito generado sobre $(\mathrm{Proj}R, \widetilde{R})$ es la localización homogénea de un R-módulo graduado finito generado.

6. Proposición: *Para todo módulo $\mathscr{M}$ quasi-coherente sobre $X = \mathrm{Proj}R$ existe una resolución*

$$\bigoplus_I \mathscr{O}(n_i) \to \bigoplus_J \mathscr{O}(n_j) \to \mathscr{M} \to 0$$

Si $\mathscr{M}$ es de presentación finita pueden tomarse I, J finitos.

Demostración. Por la proposición anterior, $\mathscr{M}$ es la localización homogénea de un R-módulo graduado. Ahora bien, todo R-módulo graduado es el cociente graduado de una suma directa $\bigoplus_J R(n_j)$. Luego $\mathscr{M}$ es un cociente de $\bigoplus_J \mathscr{O}(n_j)$ (con J finito si $\mathscr{M}$ es finito generado) y argumentando igual con el núcleo (que vuelve a ser finito generado si $\mathscr{M}$ es de presentación finita), concluimos. □

12.4. Morfismos en espacios proyectivos

Sea X una variedad algebraica íntegra sobre un cuerpo algebraicamente cerrado k y $\mathscr{L}$ un haz de línea en X. Dado un punto cerrado $x \in X$ y un isomorfismo $\mathscr{L}/\mathfrak{m}_x\mathscr{L} \simeq k$, para cada $s \in \Gamma(X, \mathscr{L})$ podemos definir el valor de s en x, "$s(x)$":

$$\Gamma(X, \mathscr{L}) \to \mathscr{L}/\mathfrak{m}_x\mathscr{L} \simeq k$$
$$s \mapsto \overline{s_x} \overset{\mathrm{Not}}{=} s(x)$$

El valor $s(x)$ depende del isomorfismo $\mathscr{L}/\mathfrak{m}_x\mathscr{L} \simeq k$, luego está definido salvo un factor $\lambda \in k$. Ahora bien, sí tiene sentido decir si $s(x) = 0$ o no. Además, los puntos donde $s(x) = 0$, que denotaremos $(s)_0$, es un cerrado de X. Recordemos que el divisor de ceros de Cartier (no hay polos) de $s \in \Gamma(X, \mathscr{L})$ es un divisor efectivo cuyo haz de línea asociado es $\mathscr{L}$. Por tanto, $(s)_0$ es el soporte del divisor $D(s)$ asociado a s.

Sean $s_0, \ldots, s_n \Gamma(X, \mathscr{L})$ y supongamos que no tienen puntos base, es decir, $\bigcap_i (s_i)_0 = \emptyset$. Definen "puntualmente" el morfismo

$$X \to \mathbb{P}^n,\ x \overset{\mathrm{def}}{\mapsto} (s_0(x), \ldots, s_n(x)).$$

Definámoslo ahora esquemáticamente (no necesitaremos que k sea algebraicamente cerrado): Dada $s \in \Gamma(X, \mathscr{L})$ y $U_s = X \setminus (s)_0$, tenemos que $\mathscr{L}_{|U_s} = \mathscr{O}_{U_s} \cdot s$. Dada $s' \in \Gamma(X, \mathscr{L})$, entonces $s' = f \cdot s$, con $f \in \mathscr{O}_X(U_s)$. Escribiremos $f = \frac{s'}{s}$.

Los morfismos

$$\begin{array}{rcl} U_{s_i} & \longrightarrow & \mathbb{P}^n - (x_i)_0^h = \operatorname{Spec} k[\dfrac{x_0}{x_i}, \ldots, \dfrac{x_n}{x_i}] \\ \mathscr{O}_X(U_{s_i}) & \longleftarrow & k[\dfrac{x_0}{x_i}, \ldots, \dfrac{x_n}{x_i}] \\ \dfrac{x_j}{x_i} & \longleftarrow\!\shortmid & \dfrac{s_j}{s_i} \end{array}$$

nos definen el morfismo $X \to \mathbb{P}^n$, antes definido "puntualmente".

Recíprocamente, dado un morfismo $\pi\colon X \to \mathbb{P}^n$, entonces π es el morfismo definido por $\mathscr{L} := \pi^* \mathscr{O}_{\mathbb{P}(E^*)}(1)$ y $s_i := \pi^*(x_i)$, donde $\pi^*\colon \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) \to \Gamma(X, \mathscr{L})$ es el morfismo inducido por π.

Si H es un hiperplano de $\mathbb{P}^n$ y $s = \pi^* H \in \Gamma(X, \mathscr{L})$, entonces $H \cap X := \pi^{-1}(H) = D(s)$. Es decir, los hiperplanos de $\mathbb{P}^n$ cortan a X en los divisores efectivos de Cartier asociados a $\mathscr{L}$. En particular, si π es una inmersión cerrada y X es una curva completa no singular, el grado de X es igual al grado de los divisores asociados a $\mathscr{L}$.

Procedamos ahora con toda generalidad.

1. Proposición: *Sea M un A-módulo localmente libre de rango n. Sea $\pi\colon X \to \operatorname{Spec} A$ un morfismo de esquemas. Entonces,*

$$\operatorname{Hom}_{\operatorname{Spec} A}(X, \operatorname{Proj} S^{\cdot} M) = \{\textit{Cocientes de línea de } \pi^* \tilde{M} = \mathscr{O}_X \otimes_A M\}.$$

Demostración. Consideremos el morfismo de $S^{\cdot}M$-módulos graduados natural

$$S^{\cdot} M \otimes_A M \to S^{\cdot} M[1],\ 1 \otimes m \mapsto m.$$

Tomando localizaciones homogéneas, obtenemos un morfismo de $\mathscr{O}_{\operatorname{Proj} S^{\cdot} M}$-módulos

$$\mathscr{O}_{\operatorname{Proj} S^{\cdot} M} \otimes_A M \to \mathscr{O}_{\operatorname{Proj} S^{\cdot} M}[1].$$

Que es un epimorfismo, porque para cada $m' \in M$, la restricción de este morfismo al abierto $\operatorname{Spec} B = U_{m'}^h$ es el epimorfismo $M_B \to B \cdot m'$, $m \mapsto \frac{m}{m'} \cdot m'$.

Sea $f\colon X \to \operatorname{Proj} S^{\cdot} M$ un morfismo de A-esquemas. Entonces, tenemos el epimorfismo en un haz de línea

$$\pi^* \tilde{M} = \mathscr{O}_X \otimes_A M = f^*(\mathscr{O}_{\operatorname{Proj} S^{\cdot} M} \otimes_A M) \to f^*(\mathscr{O}_{\operatorname{Proj} S^{\cdot} M}[1]).$$

Veamos el recíproco. Sea $\pi^*\tilde{M} = \mathscr{O}_X \otimes_A M \xrightarrow{\phi} \mathscr{L}$ un cociente de línea.. Dado $m \in M$, sea $U_{\phi(m)} := X - (\phi(m)_0)$. Entonces, $\mathscr{L}_{|U_{\phi(m)}} = \mathscr{O}_{U_{\phi(m)}} \cdot \phi(m)$ y tenemos el morfismo de X-esquemas: $U_{\phi(m)} \to U_m^h$ definido por $[(S^\cdot M)_m]_0 \to \mathscr{O}_{U_{\phi(m)}}$, $\frac{m'}{m} \mapsto \frac{\phi(m')}{\phi(m)}$. Variando m, obtenemos un morfismo $X \to \operatorname{Proj} S^\cdot M$.

Ambas asignaciones son inversas entre sí. □

Sea $X \to \operatorname{Spec} A$ un morfismo de esquemas y $\mathscr{L}$ un haz de línea en X. Dar una sección global $s \in \Gamma(X, \mathscr{L})$ es equivalente a definir un morfismo $\mathscr{O}_X \to \mathscr{L}$, $a \mapsto a \cdot s$ y diremos que los ceros de s, $(s)_0$, es el soporte del conúcleo de este morfismo. Diremos que $s_0, \ldots, s_n \in \Gamma(X, \mathscr{L})$ no tienen puntos base si $\bigcap_i (s_i)_0 = \emptyset$, que equivale a decir, que el morfismo $\mathscr{O}_X^{n+1} \to \mathscr{L}$, $(a_i) \mapsto \sum_i a_i s_i$ es un epimorfismo. Entonces,

$$\left\{ \begin{array}{l} s_0, \ldots, s_n \in \Gamma(X, \mathscr{L}) \\ \text{sin puntos base} \end{array} \right\} = \{\text{Epimorfismos } f : \mathscr{O}_X^{n+1} \to \mathscr{L}\}$$

y módulo automorfismos de $\mathscr{L}$, que son homotecias por $a \in \mathscr{O}_X(X)^*$, obtenemos

$$\left\{ \begin{array}{l} s_0, \ldots, s_n \in \Gamma(X, \mathscr{L}) \\ \text{sin puntos base.} \end{array} \right\} / \sim = \{\text{Coc. } \mathscr{O}_X^{n+1} \to \mathscr{L}\} = \{f \in \operatorname{Hom}_{\operatorname{Spec} A}(X, \mathbb{P}_A^n) \colon f^* \mathscr{O}_{\mathbb{P}_A^n}(1) \simeq \mathscr{L}\}.$$

Si denotamos $U_j = X \setminus (s_j)_0$, entonces $\mathscr{L}_{|U_j} \overset{\cdot s_j^{-1}}{\simeq} \mathscr{O}_{U_j}$ y $\frac{s_i}{s_j} = f_{ij} \in \mathscr{O}_X(U_j)$. El morfismo inducido por $s_0, \ldots, s_n$ aplica U_j en $\mathbb{P}_A^n \setminus (x_j)_0^h$ y su expresión en anillos es:

$$A[x_0/x_j, \ldots, x_n/x_j] \to \mathscr{O}_X(U_j),\ x_i/x_j \mapsto f_{ij}.$$

2. Definición: Sea X una k-variedad. Diremos que un haz de línea $\mathscr{L}$ sobre X es muy amplio (sobre k) si existe una inmersión cerrada $i : X \hookrightarrow \mathbb{P}_k^n$, de modo que $i^* \mathscr{O}_{\mathbb{P}_k^n}(1) = \mathscr{L}$.

Si la serie lineal completa $\Gamma(X, \mathscr{L})$ es un espacio vectorial de dimensión finita, $\mathscr{L}$ es muy amplio si y sólo si el morfismo definido por la serie lineal completa es una inmersión cerrada.

Supongamos que X es una variedad algebraica sobre un cuerpo algebraicamente cerrado y $\Gamma(X, \mathscr{L})$ no tiene puntos base. Dados dos puntos cerrados $x \neq x' \in X$ que el morfismo $\Gamma(X, \mathscr{L}) \to \mathscr{L}/\mathfrak{m}_x \mathfrak{m}_{x'} \mathscr{L}$ sea epiyectivo equivale a que exista una sección global $s \in \Gamma(X, \mathscr{L})$ tal que $s(x) = 0$ y $s(x') \neq 0$ (se dice que las secciones globales del haz de línea $\mathscr{L}$ separan puntos). Que el morfismo $\Gamma(X, \mathscr{L}) \to \mathscr{L}/\mathfrak{m}_x^2 \mathscr{L}$ sea epiyectivo equivale a que las secciones globales de $\mathscr{L}$ que se anulan en x generan $\mathfrak{m}_x \mathscr{L}/\mathfrak{m}_x^2 \mathscr{L}$ (se dice que las secciones globales de $\mathscr{L}$ separan puntos infinitesimalmente próximos).

Siguiendo las notaciones anteriores, sobre U_j tenemos el isomorfismo $\mathscr{L}_{U_j} \overset{s_j^{-1}}{\simeq} \mathscr{O}_{U_j}$. Dados $x, y \in U_j$, decir que las secciones globales de $\mathscr{L}$ separan x de y, equivale a decir que existe una sección $s \in \Gamma(X, \mathscr{O}_X)$ de modo que la función $f = s/s_j$ satisface $f(x) = 0$ y $f(y) \neq 0$. Decir que las secciones globales separan puntos infinitesimalmente próximos a x equivale a decir que las funciones $f = s/s_j$ que se anulan en x generan $\mathfrak{m}_x$.

3. Teorema: [2] *Sea C una curva completa y $\mathscr{L}$ un haz de línea en C. Entonces, $\mathscr{L}$ es muy amplio si y sólo si para cada par de puntos cerrados $x, x' \in C$ (distintos o no) el morfismo natural $\Gamma(C, \mathscr{L}) \to \mathscr{L}/\mathfrak{m}_x \mathfrak{m}_{x'} \mathscr{L}$ es epiyectivo, es decir, "la serie lineal completa no tiene puntos base, separa puntos y separa puntos infinitesimalmente próximos".*

Demostración. Sea $\langle s_0, \ldots, s_n \rangle = \Gamma(C, \mathscr{L})$ la "serie lineal completa" y supongamos que no tiene puntos base. El morfismo

$$i : C \to \mathbb{P}^n,\ x \mapsto (s_0(x), \ldots, s_n(x))$$

inducido es una inmersión cerrada si y sólo si $\mathscr{L}$ es un haz de línea muy amplio.

Localmente el morfismo i viene dado por

$$\begin{array}{ccccc} k[x_0/x_i, \ldots, x_n/x_i] & \longrightarrow & k[s_0/s_i, \ldots, s_n/s_i] & \overset{i^*}{\hookrightarrow} & \mathscr{O}_C(U_i) \\ x_j/x_i & \longmapsto & s_j/s_i & \longmapsto & s_j/s_i. \end{array}$$

Tenemos que probar que las inclusiones $i^* : B = k[s_0/s_i, \ldots, s_n/s_i] \hookrightarrow \mathscr{O}_C(U_i)$ son isomorfismos si y sólo si $\mathscr{L}$ no tiene puntos base, separa puntos y separa puntos infinitesimalmente próximos.

El morfismo finito $B \overset{i^*}{\hookrightarrow} \mathscr{O}_C(U_i)$ es un isomorfismo si y sólo si para todo ideal maximal $\mathfrak{m}_y$ de B, el morfismo $B/\mathfrak{m}_y \to \mathscr{O}_C(U_i)/\mathfrak{m}_y \mathscr{O}_C(U_i)$ es un epimorfismo. Es decir, si y sólo si $\mathfrak{m}_y \mathscr{O}_C(U_i)$ está contenido en un único ideal maximal, digamos $\mathfrak{m}_x$ (donde $\mathfrak{m}_x \cap B = \mathfrak{m}_y$) y $B \to \mathscr{O}_C/\mathfrak{m}_x^2$ es epiyectivo. Es decir, las secciones globales de $\mathscr{L}$ que se anulan en x no se anulan, todas a la vez, en otro punto y separan los puntos infinitesimalmente próximos a x. □

12.4.1. Teorema de Bézout

Sea X una k-variedad algebraica de dimensión cero, es decir, $X = \{x_1, \ldots, x_r\}$ es un conjunto finito de puntos (cerrados). Llamaremos número de puntos de X contando multiplicidades y grados, que denotaremos (X), a

$$(X) := \dim_k \mathscr{O}_X(X).$$

[2] Este teorema se demuestra con mayor generalidad en 13.12.1.

Observemos que $\mathscr{O}_X(X) = \oplus_i \mathscr{O}_{X,x_i}$. Dado $x \in X$, llamaremos multiplicidad con la que aparece x en X, que denotaremos $(X)_x$ a

$$(X)_x = l_{\mathscr{O}_{X,x}} \mathscr{O}_{X,x}$$

Sea $\operatorname{gr} x := \dim_k \mathscr{O}_{X,x}/\mathfrak{m}_x$ el grado de x. Como $\dim_k \mathscr{O}_{X,x} = l_{\mathscr{O}_{X,x}} \mathscr{O}_{X,x} \cdot \operatorname{gr} x$, tenemos que

$$(X) = \dim_k \mathscr{O}_X(X) = \sum_{x \in X} \dim_k \mathscr{O}_{X,x} = \sum_{x \in X} (X)_x \cdot \operatorname{gr} x.$$

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo y $k[\xi_0, \ldots, \xi_n] = k[x_0, \ldots, x_n]/I$. Se tiene una inmersión cerrada

$$i \colon X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n] \hookrightarrow \operatorname{Proj} k[x_0, \ldots, x_n] = \mathbb{P}^n_k.$$

El núcleo del morfismo

$$\mathscr{O}_{\mathbb{P}^n} \to i_* \mathscr{O}_X$$

es el haz de localizaciones homogéneas de I y lo denotaremos $\mathfrak{p}_X$. Diremos que $\mathfrak{p}_X$ es el haz de ideales de funciones de $\mathbb{P}^n$ que se anulan en X.

Si C_1, C_2 son dos subesquemas cerrados de $\mathbb{P}^n$ definidos por los ideales I_1, I_2, denotaremos $C_1 \cap C_2$ al subesquema cerrado de $\mathbb{P}^n$ definido por $I_1 + I_2$, que topológicamente es la intersección de C_1 y C_2.

Si $C_1 \cap C_2 = \{x_1, \ldots, x_n\}$ es un número finito de puntos cerrados de $\mathbb{P}^n$, llamaremos número de puntos de corte de C_1 con C_2 en $\mathbb{P}^n$ (contando multiplicidades y grados) a $(C_1 \cap C_2)$. Diremos que $(C_1 \cap C_2)_{x_i}$ es la multiplicidad de intersección de C_1 con C_2 en x_i.

4. Ejercicio: Sea $C = \operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 - x_2^2)$ y $f = \frac{x_1}{x_0} \in \Sigma_C$. Calcular el divisor de ceros y polos de f e interpretarlo geométricamente.

5. Lema: *Sea A una k-álgebra de tipo finito íntegra de dimensión de Krull 1 y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. Dada $f \in A$ no nula se cumple que* $\dim_k(A/fA) = \dim_k(\bar{A}/f\bar{A})$.

Si C es una curva íntegra, $\pi \colon \bar{C} \to C$ es el morfismo de desingularización, $D \subset C$ un divisor efectivo de Cartier y $\pi^{-1}(D) = \bar{C} \times_C D$, entonces

$$(D) = (\pi^{-1}(D)) = \operatorname{gr} \pi^{-1}(D)$$

Demostración. Del isomorfismo $\bar{A}/A \simeq f\bar{A}/fA$ y el diagrama conmutativo

$$\begin{array}{ccc} fA & \longrightarrow & f\bar{A} \\ \downarrow & & \downarrow \\ A & \longrightarrow & \bar{A} \end{array}$$

se deduce que $\dim_k(A/fA) = \dim_k(\bar{A}/f\bar{A})$.

Dada una variedad algebraica de dimensión cero, X, como $(X) = \sum_{x\in X}(X)_x \cdot \mathrm{gr}\, x$, para probar que $(D) = (\pi^{-1}(D))$ basta verlo localmente en C, luego podemos suponer que $C = \mathrm{Spec} A$ es afín y que $D = \mathrm{Spec} A/fA$ (luego $\bar{C} = \mathrm{Spec}\bar{A}$ y $\pi^{-1}(D) = \mathrm{Spec}\bar{A}/f\bar{A}$). Se concluye por el párrafo anterior. □

6. Teorema de Bézout: *Sea C una curva proyectiva íntegra.*

1) Para cada hiperplano H que no contenga a C, el número de puntos de corte de H con C (contando multipicidades y grados) es un número natural que no depende del hiperplano H y que se llama grado de la curva C.

2) Sea C de grado n y H una hipersuperficie de grado m (es decir, definida por los ceros de un polinomio homogéneo de grado m). Si H no contiene a C, entonces el número de puntos de corte de H con C es $n \cdot m$.

Demostración. Sean $H \equiv p_m(x_0,\dots,x_n) = 0$ y $H' \equiv q_m(x_0,x_1,x_2) = 0$ dos hipersuperficies de $\mathbb{P}^n$ de grado m (que no contengan a C). Sea $\pi\colon \tilde{C} \to C$ el morfismo de desingularización. Obviamente

$$\pi^{-1}(H\cap C) + D(q_m/p_m) = \pi^{-1}(H'\cap C)$$

Por el lema anterior,

$$(H\cap C) = (\pi^{-1}(H\cap C)) = \mathrm{gr}(\pi^{-1}(H\cap C)) = \mathrm{gr}(\pi^{-1}(H'\cap C)) = (H'\cap C)$$

Por tanto, $(C\cap H)$ no depende de la hipersuperficie de grado m considerada. Algún hiperplano coordenado, digamos $x_0 = 0$, no contiene a C. Entonces,

$$(H\cap C) = (\{x_0^m = 0\}\cap C) = (\pi^{-1}(\{x_0^m = 0\}\cap C)) = (m\cdot\pi^{-1}(\{x_0 = 0\}\cap C)) = m\cdot n$$

□

7. Ejercicio: Sean $p_1, p_2 \in k[x,y]$ polinomios primos con $p \in k[x,y]$. Demuestra que la sucesión

$$0 \to k[x,y]/(p,p_2) \xrightarrow{\cdot p_1} k[x,y]/(p,p_1\cdot p_2) \to k[x,y]/(p,p_1) \to 0$$

es exacta. Si denotamos C, C', C_1 y C_2 las curvas planas definidas por los ceros de $p, p_1\cdot p_2, p_1$ y p_2 respectivamente, demostrar que $(C\cap C')_x = (C\cap C_1)_x + (C\cap C_2)_x$.

8. Corolario: *Sean C, C' dos curvas planas definidas por los ceros homogéneos de $p_r(x_0,x_1,x_2)$ y $p_{r'}(x_0,x_1,x_2)$ respectivamente. Si no tienen componentes comunes, el número de puntos de corte de las dos curvas es $r\cdot r'$.*

Demostración. Podemos suponer las curvas son íntegras, por el ejercicio 12.4.7. Por el teorema anterior, solo tenemos que probar que si C es una curva proyectiva plana definida por los ceros de un polinomio homogéneo $p_r(x_0,x_1,x_2)$ de grado r, entonces C tiene grado r. Si C es una recta es claro que su grado es uno. Ahora ya,

$$(C \cap R) = (R \cap C) = r \cdot \text{grado de } R = r$$

□

Generalizaremos estos resultados de curvas planas para variedades proyectivas de dimensión superior en el siguiente capítulo, mediante las técnicas cohomológicas.

12.5. Apéndice: Fibrados. Grassmannianas

12.5.1. Morfismos afines y haces de álgebras quasi-coherentes

1. Definición: Sea X un esquema y $\mathscr{O}_X \to \mathscr{B}$ un morfismo de haces de álgebras sobre X. Diremos que $\mathscr{B}$ es un haz de $\mathscr{O}_X$-álgebras quasi-coherente (resp. coherente) si $\mathscr{B}$ es un $\mathscr{O}_X$-módulo quasi-coherente (resp. coherente).

Sea $\mathscr{B}$ un haz de $\mathscr{O}_X$-álgebras quasi-coherente. Consideremos el funtor F sobre la categoría de X-esquemas que asigna a cada X-esquema $\pi\colon X' \to X$,

$$X' \rightsquigarrow F(X') := \mathrm{Hom}_{\mathscr{O}_X-alg}(\mathscr{B}, \pi_*\mathscr{O}_{X'}).$$

Si $X = \mathrm{Spec}\, A$ es afín, entonces $\mathscr{B} = \tilde{B}$, con $B = \mathscr{B}(X)$ y

$$\mathrm{Hom}_{\mathscr{O}_X-alg}(\mathscr{B}, \pi_*\mathscr{O}_{X'}) = \mathrm{Hom}_{A-alg}(B, \mathscr{O}_{X'}(X')) = \mathrm{Hom}_X(X', \mathrm{Spec}\, B).$$

Es decir, F es representable. Ahora, en general: Como F es un haz para la topología de Zariski, se cumple que F es representable por un X-esquema que denotaremos $\mathrm{Spec}\,\mathscr{B}$. Denotemos $\pi\colon \mathrm{Spec}\,\mathscr{B} \to X$ el morfismo estructural. Dado un abierto afín $U \subset X$, $\pi^{-1}(U) = \mathrm{Spec}\,\mathscr{B}(U)$, por tanto π es un morfismo afín.

2. Teorema: *La categoría de esquemas afines sobre X es anti-equivalente a la categoría de haces de $\mathscr{O}_X$-álgebras quasi-coherentes.*

Demostración. Sea F el funtor que asigna a cada haz de $\mathscr{O}_X$-álgebras quasi-coherente $\mathscr{B}$ el X-esquema $\mathrm{Spec}\,\mathscr{B}$, y G el funtor que asigna a cada esquema afín sobre X, $\pi\colon X' \to X$, el haz de $\mathscr{O}_X$-álgebras quasi-coherente $\pi_*\mathscr{O}_{X'}$. Se cumple que F y G son inversos entre sí. □

3. Corolario: *Sea X un esquema localmente noetheriano. La categoría de esquemas finitos sobre X es anti-equivalente a la categoría de haces de $\mathscr{O}_X$-álgebras coherentes.*

12.5.2. Módulos y fibrados

En Geometría Diferencial, es conocida la correspondencia entre fibrados vectoriales sobre una variedad diferenciable X y los C^∞_X-módulos localmente libres. Al fibrado vectorial $\pi\colon E \to X$ se le asigna el C^∞_X-módulo localmente libre de sus secciones, y todo C^∞_X-módulo localmente libre son las secciones de un único fibrado vectorial, salvo isomorfismos. Por ejemplo, si $M = (\mathscr{C}^\infty_X)^n$ es un C^∞_X-módulo libre, entonces M son las secciones del fibrado vectorial trivial $X \times \mathbb{R}^n \to X$.

Sea $\mathscr{M}$ un módulo quasi-coherente sobre un esquema X. Sea $S^\cdot_{\mathscr{O}_X}\mathscr{M}$, el $\mathscr{O}_X$-álgebra quasi-coherente definida por $S^\cdot_{\mathscr{O}_X}\mathscr{M}(U) = S^\cdot_{\mathscr{O}_X(U)}\mathscr{M}(U)$, para cada abierto afín $U \subseteq X$. Consideremos el funtor $\mathscr{M}^*$ sobre la categoría de X-esquemas, definido sobre cada esquema $\pi\colon X' \to X$ por $\mathscr{M}^*(X') := \mathrm{Hom}_{\mathscr{O}_{X'}}(\pi^*\mathscr{M}, \mathscr{O}_{X'})$. Entonces,

$$\begin{aligned}\mathscr{M}^*(X') &= \mathrm{Hom}_{\mathscr{O}_{X'}}(\pi^*\mathscr{M}, \mathscr{O}_{X'}) = \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M}, \pi_*\mathscr{O}_{X'}) \\ &= \mathrm{Hom}_{\mathscr{O}_X - alg}(S^\cdot_{\mathscr{O}_X}\mathscr{M}, \pi_*\mathscr{O}_{X'}) = \mathrm{Hom}_X(X', \mathrm{Spec}\, S^\cdot_{\mathscr{O}_X}\mathscr{M}).\end{aligned}$$

En conclusión, $\mathscr{M}^*$ es representable por el X-esquema $\mathrm{Spec}\, S^\cdot_{\mathscr{O}_X}\mathscr{M}$. Denotemos por π el morfismo estructural $\pi\colon \mathrm{Spec}\, S^\cdot_{\mathscr{O}_X}\mathscr{M} \to X$. Para cada abierto afín U de X tenemos que $\pi^{-1}(U) = \mathrm{Spec}\, S^\cdot_{\mathscr{O}_X(U)}\mathscr{M}(U)$. Por tanto, si $\{U_i\}$ es un recubrimiento por abiertos afines de X, entonces $\mathrm{Spec}\, S^\cdot_{\mathscr{O}_X}\mathscr{M}$ está recubierto por los abiertos afines $\mathrm{Spec}\, S^\cdot_{\mathscr{O}_X(U_i)}\mathscr{M}(U_i)$.

4. Notación: Denotaremos $\mathbf{M}^* = \mathrm{Spec}\, S^\cdot_{\mathscr{O}_X}\mathscr{M}$.

Por tanto, para cada X-esquema X', se cumple que

$$\mathrm{Hom}_X(X', \mathbf{M}^*) = \mathscr{M}^*(X').$$

Si $\mathscr{M} = \mathscr{O}^n_X$, es fácil probar que $\mathbf{M}^* = \mathbb{A}^n \times X$.

5. Definición: Un morfismo de esquemas $P \to X$ se dice un fibrado de módulos si su funtor de puntos $P^\cdot = \mathrm{Hom}_X(-, P)$ cumple que $P^\cdot(X')$ es un $\Gamma(X', \mathscr{O}_{X'})$-módulo (funtorialmente), para todo X-esquema X'. Es decir, se tienen morfismos de funtores

$$P^\cdot \times P^\cdot \xrightarrow{+} P^\cdot, \quad (\mathbb{A}^1)^\cdot \times P^\cdot \xrightarrow{\cdot} P^\cdot$$

satisfaciendo los axiomas de módulo. Por el teorema 11.5.3, esto equivale a tener morfismos de X-esquemas

$$P \times_X P \xrightarrow{+} P, \quad \mathbb{A}^1 \times P \xrightarrow{\cdot} P$$

satisfaciendo los axiomas de módulo.

6. Definición: Sean $P \to X$ y $P' \to X$ fibrados de módulos. Diremos que un morfismo $f\colon P \to P'$ de X-esquemas es un morfismo de fibrados de módulos si $f(p + p') = f(p) + f(p')$ y $f(\lambda p) = \lambda f(p)$ para cualesquiera puntos (del funtor de puntos) p, p' de P y λ de $\mathbb{A}^1$.

7. Definición: Diremos que un fibrado de módulos $\pi: P \to X$ es un fibrado localmente trivial si existe un recubrimiento $\{U_i\}$ de X de modo que $\pi^{-1}(U_i) \simeq \mathbb{A}^n \times U_i$, como fibrados de módulos.

8. Teorema: *La categoría de módulos finito generados localmente libres sobre X es equivalente a la categoría de los fibrados localmente triviales sobre X.*

Demostración. Sea F el funtor que asigna a cada módulo finito generado localmente libre $\mathscr{M}$, el fibrado $\mathbf{M}^*$. Sea G el funtor que asigna a cada fibrado localmente libre $P \to X$ el módulo finito generado $\mathscr{N}$ de sus secciones: $\mathscr{N}(U) = \mathrm{Hom}_X(U,P)$. Se cumple que $\mathscr{N}$ es un módulo localmente libre y F y G son asignaciones inversas entre sí. □

12.5.3. Grassmannianas

La Grassmanniana de orden r de un espacio vectorial E es el conjunto, $\mathrm{Grass}_r E$, de los subespacios vectoriales de dimensión r de E. En particular, $\mathrm{Grass}_1 E = \mathbb{P}(E)$. $\mathrm{Grass}^s E$ es el conjunto de los cocientes de E de dimensión s. Si $\dim E = n$, entonces $\mathrm{Grass}_r E = \mathrm{Grass}^{n-r} E$, $V \mapsto E/V$.

Veamos que $\mathrm{Grass}^s E$ es el conjunto de puntos racionales de una k-variedad algebraica. Consideremos una base de $\{e_i\}_{i\in I}$ y sea $E \to V$ un cociente de dimensión s. Entonces, la clase de r vectores de la base forman una base de V. Sea J el conjunto de los subconjuntos de orden s de I y dado $l \in J$, sea G_l el conjunto de cocientes $E \to V$ de dimensión s, tales que $\{\bar{e}_i\}_{i\in l}$ sean una base de V. Obviamente, $\mathrm{Grass}^s E = \cup_{l\in J} G_l$. Escribamos por sencillez $l = \{1,\dots,s\}$. La base $\{\bar{e}_i\}_{i\in l}$ del cociente V, determina un isomorfismo $\phi_V: \mathbb{R}^s \simeq V$, $(\lambda_i) \mapsto \sum_{i\in l} \lambda_i \bar{e}_i$. Luego, $G_l = \{f \in \mathrm{Hom}_{k-lin}(E,k^r):$ $f(e_i) = (0,\dots,\overset{i}{1},\dots,0),\ \forall i \in j\}$, $V \mapsto \phi_V^{-1} \circ \pi_V$. Por tanto,

$$G_l = \{(w_1,\dots,w_s) \in E^* \times \overset{s}{\cdots} \times E^* : w_i(e_j) = \delta_{ij},\ \forall i,j\}$$

que es una subvariedad afín de $E^* \times \overset{s}{\cdots} \times E^*$.

Procedamos ahora en general, sustituyendo la base k por un esquema X y E por un $\mathscr{O}_X$-módulo quasi-coherente $\mathscr{M}$. Dado un X-esquema $f: T \to X$, denotamos $\mathscr{M}_T := f^*\mathscr{M}$. Denotaremos por $\mathrm{Grass}^s(\mathscr{M})$ al funtor sobre la categoría de X-esquemas

$$\mathrm{Grass}^s(\mathscr{M})(T) := \left\{ \begin{array}{l} \text{Cocientes quasi-coeherentes de } \mathscr{M}_T \\ \text{localmente libres de rango } s. \end{array} \right\}$$

Evidentemente, $\mathrm{Grass}^s(\mathscr{M})$ es un haz para la topología de Zariski. Demostremos que es representable. Consideremos un recubrimiento de X por abiertos afines U_i. $\{\mathrm{Grass}^s(\mathscr{M})_{|U_i} = \mathrm{Grass}^s(\mathscr{M}_{|U_i})\}$ es un recubrimiento de $\mathrm{Grass}^s(\mathscr{M})$, por tanto, solo tenemos que probar la representabilidad de $\mathrm{Grass}^s(\mathscr{M})$, cuando $X = \mathrm{Spec}A$ y $\mathscr{M} = \tilde{M}$.

Sea $\{m_i\}_{i\in I}$ un sistema generador del A-módulo M y J el conjunto de los subconjuntos de orden s de I. Dado $l \in J$, sea G_l es subfuntor de $\mathrm{Grass}^s(\mathscr{M})$, definido por

$$G_l(T) := \left\{ \begin{array}{l} \text{Cocientes quasi-coherentes } \mathscr{M}_T \to \mathscr{V} \\ \text{tales que } \{\bar{m}_i\}_{i\in l} \text{ es una base de } \mathscr{V}. \end{array} \right\}$$

Sea $T^{\cdot} \to \mathrm{Grass}^s(\mathscr{M})$ un morfismo de funtores, que equivale a tomar un cociente $\mathscr{V}$ de $\mathscr{M}_T$ localmente libre de rango s. Se cumple que (comprobación al lector)

1. $G_l \times_{\mathrm{Grass}^s(\mathscr{M})} T^{\cdot}$ es representable por el abierto U de T formado por los puntos $y \in T$ tales que $\{\bar{m}_i\}_{i\in l}$ es una base de $\mathscr{V}_y$.

2. $\{G_l\}_{l\in J}$ es un recubrimiento de $\mathrm{Grass}_r(\mathscr{M})$.

Para concluir, solo nos falta probar que G_l es representable. Para simplificar notaciones escribamos $l = \{1,\dots,s\}$. Dado $\mathscr{V} \in G_l(T)$, es decir, dado un cociente $\pi_{\mathscr{V}} : \mathscr{M}_T \to \mathscr{V}$ tal que $\{\pi_{\mathscr{V}}(m_i)\}_{i\in l}$ sea una base de $\mathscr{V}$, tenemos el isomorfismo $\phi_{\mathscr{V}} : \mathscr{O}_T^s \to \mathscr{V}$, $\phi_{\mathscr{V}}(t_i) := \sum_i t_i \cdot \pi_{\mathscr{V}}(m_i)$ y la biyección

$$G_l(T) = \{f \in \mathrm{Hom}_{\mathscr{O}_T}(\mathscr{M}_T, \mathscr{O}_T^s) \colon f(m_i) = (0,\dots,\overset{i}{1},\dots,0),\ \forall i \in l\},\ \mathscr{V} \mapsto \phi_{\mathscr{V}}^{-1} \circ \pi_{\mathscr{V}}.$$

Luego, $G_l(T) = \{(w_1,\dots,w_s) \in \mathrm{Hom}_{\mathscr{O}_T}(\mathscr{M}_T, \mathscr{O}_T)^s \colon w_j(m_i) = \delta_{ij},\ \forall i,j \in l\}$ y G_l es representable por el subesquema cerrado de $\mathbf{M}^* \times \overset{s}{\cdots} \times \mathbf{M}^* = \mathrm{Spec}(S^{\cdot}M \otimes \cdots \otimes S^{\cdot}M)$ definido por los ceros de las funciones $\{1 \otimes \cdots \otimes \overset{i}{m}_j \otimes \cdots \otimes 1 - \delta_{ij}\}_{1\le i,j\le s}$.

9. Ejercicio : Sea $\mathscr{M}$ un $\mathscr{O}_X$-módulo localmente libre de rango n. Prueba que

$$\mathrm{Grass}_r(\mathscr{M}) = \mathrm{Grass}^{n-r}(\mathscr{M}) = \mathrm{Grass}_{n-r}(\mathscr{M}^*).$$

10. Teorema : *Sea X un esquema y $\mathscr{M}$ un $\mathscr{O}_X$-módulo quasi-coherente. Para cada abierto afín $U \subset X$, se cumple que*

$$\mathrm{Grass}^1(\mathscr{M}_{|U}) = \mathrm{Proj}\, S^{\cdot}\mathscr{M}(U).$$

Demostración. Es consecuencia inmediata de 12.4.1.

De otro modo: dado $m \in \mathscr{M}(U) = M$, si seguimos las notaciones anteriores, tenemos los isomorfismos locales

$$G_{\{m\}} = \mathrm{Spec}(S^{\cdot}M)/(m-1) = \mathrm{Proj}(S^{\cdot}M)_m = U_m^h.$$

□

Suele denotarse $\mathrm{Grass}^1 \mathscr{M} = \mathbb{P}(\mathscr{M}^*)$.

12.6. Problemas

1. Demuestra que la sucesión de $\mathcal{O}_X$-módulos quasi-coherentes $0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}''$ es exacta si y solo si para todo módulo quasi-coherente $\mathcal{N}$, la sucesión siguiente es exacta

$$0 \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{M}') \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{M}) \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{M}'')$$

2. Demuestra que la sucesión de $\mathcal{O}_X$-módulos quasi-coherentes $\mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$ es exacta si y solo si para todo módulo quasi-coherente $\mathcal{N}$, la sucesión siguiente es exacta

$$0 \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}'', \mathcal{N}) \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}', \mathcal{N})$$

3. Sea $\mathcal{L}$ un haz de línea sobre una variedad algebraica X, $s_0, \ldots, s_n \in \Gamma(X, \mathcal{L})$ y $C = \cap (s_i)_0$. Prueba que el morfismo $X \backslash C \to \mathbb{P}^n$ definido por las secciones s_i extiende a un morfismo de la explosión de X en C, $\tilde{X}$, en $\mathbb{P}^n$. (Pista: las secciones s_i definen un morfismo $\mathcal{O}_X^{n+1} \to \mathcal{L}$, y tensando por $\mathcal{L}^*$, un morfismo $\mathcal{L}^{*n+1} \to \mathcal{O}_X$ de imagen un haz de ideales I (tal que $(I)_0 = C$). Podemos definir un epimorfismo $S^{\cdot}_{\mathcal{O}_X} \mathcal{L}^{*n+1} \to D_I \mathcal{O}_X$ y tomando espectros proyectivos un morfismo $\tilde{X} \to \mathbb{P}^n_X$).

Capítulo 13

Cohomología en esquemas

13.1. Introducción

Este capítulo está dedicado principalmente a la introducción de la cohomología en esquemas y a los teoremas relativos a su finitud. Ya hemos visto que los esquemas, como las variedades diferenciales, son espacios anillados. Podremos ahora asociar a los esquemas sus grupos de cohomología, que son invariantes fundamentales para su clasificación.

13.2. Cohomología Cech

En Geometría Algebraica la cohomología Cech es especialmente operativa para los cómputos.

Sea X un espacio topológico, F un haz sobre X y $\mathscr{U} = \{U_i\}_{i\in I}$ un recubrimiento de X por abiertos, donde I es un conjunto totalmente ordenado. Vamos a definir un complejo de haces $\check{C}^{\cdot}_{\mathscr{U}}F$ y un cuasi-isomorfismo

$$F \to \check{C}^{\cdot}_{\mathscr{U}}F$$

funtorial en F (en el sentido obvio). Dado un abierto $i\colon V \hookrightarrow X$, denotamos $F_V = i_* i^{-1}F$.

1. Definición: Sea $\check{C}^0F := \prod_i F_{U_i}$ y más en general

$$\check{C}^m F := \prod_{i_0<\cdots<i_m} F_{U_{i_0}\cap\cdots\cap U_{i_m}}$$

y por tanto $\Gamma(V, C^m F) = \prod_{i_0<\cdots<i_m} F(V \cap U_{i_0} \cap \cdots \cap U_{i_m})$. Definamos $d\colon \check{C}^m F \to \check{C}^{m+1} F$, que en cada abierto V y cada $s = (s_{i_0,\ldots,i_m}) \in \prod_{i_0<\cdots<i_m} F(V \cap U_{i_0} \cap \cdots \cap U_{i_m})$ es

$$(ds)_{i_0,\ldots,i_{m+1}} = \sum_{k=0}^{m+1} (-1)^k s_{i_0,\ldots,\widehat{i_k},\ldots,i_{m+1}|V\cap U_{i_0}\cap\cdots\cap U_{i_{m+1}}}$$

Es fácil comprobar que $d^2 = 0$. El complejo $\check{C}^{\cdot} F$ se denomina *complejo de haces de Cech de F asociado a $\mathscr{U}$*. También se denota $\check{C}^{\cdot}_{\mathscr{U}} F$, cuando se necesite indicar el recubrimiento $\mathscr{U}$. Tomando secciones globales se obtiene un complejo $\Gamma(X, \check{C}^{\cdot} F)$ que se denomina *complejo de cocadenas de Cech de F asociado al recubrimiento $\mathscr{U}$*. Es fácil comprobar que $H^0(\Gamma(X, \check{C}^{\cdot} F)) = F(X)$ y que $H^0 \check{C}^{\cdot} F = F$.

2. Teorema: *$\check{C}^{\cdot}_{\mathscr{U}} F$ es una resolución por haces de F.*

Demostración. Denotemos $F_{U_{i_0}\cap\cdots\cap U_{i_n}} = F_{i_0\cdots i_n}$.

1. Supongamos que alguno de los abiertos U_i es igual a X. Podemos suponer por sencillez (de notación) que $i = i_0$ es ínfimo. Sea $\mathscr{U}' = \{U_i\}_{i\neq i_0}$ y aunque $\mathscr{U}'$ no recubra a X, podemos definir igualmente el complejo $\check{C}^{\cdot}_{\mathscr{U}'} F$ y su diferencial d'. Observemos que

$$\check{C}^m_{\mathscr{U}} F = \prod_{i_0<\cdots<i_m} F_{i_0\cdots i_m} \times \prod_{i_0<\cdots<i_{m+1}} F_{i_1\cdots i_{m+1}} = \prod_{i_0<\cdots<i_m} F_{i_1\cdots i_m} \times \prod_{i_0<\cdots<i_{m+1}} F_{i_1\cdots i_{m+1}} = \check{C}^{m-1}_{\mathscr{U}'} F \times \check{C}^m_{\mathscr{U}'} F.$$

Además, dado $(a, b) \in \check{C}^{m-1}_{\mathscr{U}'} F \times \check{C}^m_{\mathscr{U}'} F = \check{C}^m_{\mathscr{U}} F$, se cumple que

$$d(a, b) = (b - d'a, d'b).$$

Por tanto, si $d(a, b) = 0$ entonces $b = d'a$, luego $(a, b) = d(0, a)$. En conclusión, $\check{C}^{\cdot}_{\mathscr{U}} F$ es acíclico.

2. Para ver que $\check{C}^{\cdot}_{\mathscr{U}} F$ es acíclico basta verlo al restringir este complejo a los abiertos U_j del recubrimiento $\mathscr{U}$. Consideremos el recubrimiento $\mathscr{U}_j = \{U_i \cap U_j\}_{i\in I}$ de U_i. Entonces, $(\check{C}^{\cdot}_{\mathscr{U}} F)_{|U_j} = \check{C}^{\cdot}_{\mathscr{U}_j} F_{|U_j}$ es acíclico por 1.

□

3. Observaciones: 1. Si F es flasco, entonces el complejo de haces $\check{C}^{\cdot} F$ es un complejo de haces flascos, luego el complejo de cocadenas de Cech de F es acíclico.

2. Si $\#I = n$, entonces $\check{C}^m_{\mathscr{U}} F = 0$, para $m \geq n$.

4. Teorema: *Si los $F_{|U_{i_0}\cap\cdots\cap U_{i_n}}$ son acíclicos, para un recubrimiento $\mathscr{U}$ de U, entonces*

$$H^i(U,F) = H^i\Gamma(U,\check{C}^{\cdot}_{\mathscr{U}}F),$$

para todo i.

Demostración. 1. Si T es flasco entonces T_V es flasco para todo abierto V, luego $\check{C}^{\cdot}_{\mathscr{U}}T$ es una resolución por haces flascos de T_U y $H^i\Gamma(U,\check{C}^{\cdot}_{\mathscr{U}}T) = 0$ para $i > 0$ (y $H^0\Gamma(U,\check{C}^{\cdot}_{\mathscr{U}}T) = T(U)$).

2. Sea $C^{\cdot}F$ la resolución de Godement de F, entonces $H^i\Gamma(U_{i_0}\cap\cdots\cap U_{i_n},C^{\cdot}F) = 0$, para $i > 0$ (y $H^0\Gamma(U_{i_0}\cap\cdots\cap U_{i_n},C^{\cdot}F) = F(U_{i_0}\cap\cdots\cap U_{i_n})$).

3. Por tanto,

$$H^i(U,F) = H^i\Gamma(U,C^{\cdot}F) \overset{1.}{=} H^i\Gamma(U,\check{C}^{\cdot}_{\mathscr{U}}C^{\cdot}F) \overset{2.}{=} H^i\Gamma(U,\check{C}^{\cdot}_{\mathscr{U}}F).$$

□

13.2.1. Cech generalizado

Sea $\mathscr{U} = \{U_i\}_{i\in I}$ un recubrimiento finito por abiertos de U. Supongamos que I es un conjunto con un orden $\leq$, de modo que si $i \leq j$ entonces $U_i \subseteq U_j$ y además

$$U_i \cap U_j = \bigcup_{k\leq i,j} U_k$$

para todo $i,j \in I$. Diremos que $\mathscr{U}$ es un recubrimiento saturado de U.

5. Ejemplo: Si X es un esquema compacto quasi-separado, existe un recubrimiento saturado por abiertos afines de X.

6. Notación: Sea F un haz en X y $V \subseteq X$ un abierto, F_V denota el haz en X definido por $F_V(U) := F(V\cap U)$. Denotaremos $F_i := F_{U_i}$. Si $i_0 > i_1 > \cdots > i_n$, diremos que $F_{i_0\cdots i_n} := F_{i_n}$. Sea $a_{i_0\cdots i_n} \in F_{i_0\cdots i_n}$. Dado $j < i_n$, definimos $a_{i_0\cdots i_n j} \in F_{i_0\cdots i_n j}$ como la restricción de $a_{i_0\cdots i_n}$ a U_j. Si $j > i_n$, definimos $a_{i_0\cdots j\cdots i_n} \in F_{i_0\cdots j\cdots i_n}$ como $a_{i_0\cdots i_n}$.

Definimos $\check{C}^n_{\mathscr{U}}F := \prod_{i_0>\cdots>i_n} F_{i_0\cdots i_n}$ y la diferencial

$$d : \check{C}^n_{\mathscr{U}}F \to \check{C}^{n+1}_{\mathscr{U}}F,\ d(a_{i_0\cdots i_n}) = \sum_j (-1)^r a_{i_0\cdots i_{r-1}ji_r\cdots i_n} \in \check{C}^{n+1}_{\mathscr{U}}F.$$

Es fácil comprobar que $d^2 = 0$ y que $\mathrm{Ker}[\check{C}^0_{\mathscr{U}}F \to \check{C}^1_{\mathscr{U}}F] = F_U$.

7. Teorema: *Si F es flasco, entonces $\check{C}^{\cdot}_{\mathscr{U}}F$ es una resolución de F_U.*

Demostración. 1. Supongamos que existe $i \in I$ máximo. Denotemos $\mathscr{U}' = \{U_j : j \neq i\}$, $U' = \bigcup_{j \neq i} U_j$ y d' la diferencial del complejo $\check{C}^{\cdot}_{\mathscr{U}'}F$ asociado. Entonces,

$$\check{C}^n_{\mathscr{U}}F = \prod_{i=i_0>\cdots>i_n} F_{i_0\cdots i_n} \times \prod_{i\neq i_0>\cdots>i_n} F_{i_0\cdots i_n} = \check{C}^{n-1}_{\mathscr{U}'}F \times \check{C}^n_{\mathscr{U}'}F.$$

Es fácil ver que dado $(a,b) \in \check{C}^{n-1}_{\mathscr{U}'}F \times \check{C}^n_{\mathscr{U}'}F = \check{C}^n_{\mathscr{U}}F$ se tiene que $d(a,b) = (b - d'a, d'b)$. Por tanto, si $d(a,b) = 0$ entonces $b = d'a$ y $d(0,a) = (a,b)$. Por lo tanto, $\check{C}^{\cdot}_{\mathscr{U}}F(V)$ es acíclico (en todo abierto V).

2, Sea $i_1 \in I$ maximal, $\mathscr{U}_1 = \{U_i : i \leq i_1\}$, $\mathscr{U}_2 = \{U_i : i \neq i_1\}$ y $U_2 = \bigcup_{i\neq i_1} U_i$. Definamos $\mathscr{U}_1 \cap \mathscr{U}_2 := \{U_i : i < i_1\}$. Consideremos las proyecciones obvias $\check{C}^n_{\mathscr{U}}F \to \check{C}^n_{\mathscr{U}_1}F$, $\check{C}^n_{\mathscr{U}}F \to \check{C}^n_{\mathscr{U}_2}F$, $\check{C}^n_{\mathscr{U}_1}F \to \check{C}^n_{\mathscr{U}_1\cap\mathscr{U}_2}F$, etc y los morfismos obvios de complejos

$$0 \longrightarrow \check{C}^{\cdot}_{\mathscr{U}}F \longrightarrow \check{C}^{\cdot}_{\mathscr{U}_1}F \oplus \check{C}^{\cdot}_{\mathscr{U}_2}F \longrightarrow \check{C}^{\cdot}_{\mathscr{U}_1\cap\mathscr{U}_2}F \longrightarrow 0$$

Por inducción sobre el número de abiertos del recubrimiento $\mathscr{U}$ y por 1., los complejos de haces $\check{C}^{\cdot}_{\mathscr{U}_1}F \oplus \check{C}^{\cdot}_{\mathscr{U}_2}F$ y $\check{C}^{\cdot}_{\mathscr{U}_1\cap\mathscr{U}_2}F$ son resoluciones de $F_{U_1} \oplus F_{U_2}$ y $F_{U_1\cap U_2}$ y la sucesión $0 \to F_U \to F_{U_1} \oplus F_{U_2} \to F_{U_1\cap U_2} \to 0$ es exacta, porque F es flasco. Por tanto, $\check{C}^{\cdot}_{\mathscr{U}}F$ es una resolución de F_U.

□

8. Teorema : *Si F es acíclico sobre los abiertos del recubrimiento $\mathscr{U}$ saturado de U, entonces*

$$H^i(U,F) = H^i\Gamma(U, \check{C}^{\cdot}_{\mathscr{U}}F),$$

para todo i.

Demostración. 1. Si T es flasco entonces T_V es flasco para todo abierto V, luego $\check{C}^{\cdot}_{\mathscr{U}}T$ es una resolución por haces flascos de T_U y $H^i\Gamma(U, \check{C}^{\cdot}_{\mathscr{U}}T) = 0$ para $i > 0$ (y $H^0\Gamma(U, \check{C}^{\cdot}_{\mathscr{U}}T) = T(U)$).

2. Por otra parte, sea $C^{\cdot}F$ la resolución de Godement de F, como F es acíclico en los abiertos U_i, entonces $H^i\Gamma(U_i, C^{\cdot}F) = 0$, para $i > 0$ (y $H^0\Gamma(U_i, C^{\cdot}F) = F(U_i)$).

3. Por tanto,

$$H^i(U,F) = H^i\Gamma(U, C^{\cdot}F) \overset{1.}{=} H^i\Gamma(U, \check{C}^{\cdot}_{\mathscr{U}}C^{\cdot}F) \overset{2.}{=} H^i\Gamma(U, \check{C}^{\cdot}_{\mathscr{U}}F).$$

□

13.3. Aciclicidad en esquemas afines

Sea X un esquema.

1. Definición: Diremos que un haz F de grupos abelianos en X es Cech afín acíclico (abreviadamente Caa) si $H^i(\check{C}^{\cdot}_{\mathscr{U}}F(U)) = 0$, para todo $i > 0$, todo abierto afín U y todo recubrimiento finito $\mathscr{U}$ por abiertos afines de U.

2. Ejemplos: Si $\mathscr{M}$ es un módulo quasi-coherente entonces es Caa, pues el complejo de Cech de todo recubrimiento por abiertos afines de un abierto afín es acíclico y un complejo de módulos quasi-coherentes en un esquema afín es acíclico si y sólo si lo es el complejo de sus secciones.

Si F es un haz flasco entonces es Caa, por la observación 13.2.3.

3. Teorema: *Los módulos quasi-coherentes en esquemas afines son acíclicos.*

Demostración. Basta probar que en esquemas afines $X = \operatorname{Spec} A$, todo haz Caa es acíclico.

1. Sea $0 \to F \xrightarrow{i} F' \xrightarrow{j} F'' \to 0$ una sucesión exacta de haces y supongamos que F es Caa. Sea U un abierto afín de X, probemos que el morfismo $F'(U) \to F''(U)$ es epiyectivo. Sea $s'' \in F''(U)$. Por ser $j\colon F' \to F''$ un epimorfismo existe un recubrimiento $\{U_1,\dots,U_n\}$ por abiertos afines de U y secciones $s'_i \in F'(U_i)$ de modo que $j(s'_i) = s''_{|U_i}$. Observemos que $\check{j}(d((s'_i)) = d(\check{j}((s'_i))) = d((s''_{|U_i})) = 0$, por tanto existe $s \in \Gamma(U, \check{C}^1(F))$ tal que $\check{\imath}(s) = d((s'_i))$. Además, $d(s) = 0$ porque $\check{\imath}(d(s)) = d(\check{\imath}(s)) = d^2((s'_i)) = 0$. Luego, existe $s_0 \in \Gamma(U, \check{C}^0(F))$ tal que $d(s_0) = s$. Sea $s' = (s'_i) - \check{\imath}(s_0)$, entonces $d(s') = d((s'_i)) - \check{\imath}(s) = 0$ y $\check{j}(s') = \check{j}((s'_i)) = (s''_{|U_i})$. Luego, existe $s'_0 \in \Gamma(U, F')$ tal que $d(s'_0) = s'$ y cumple que $d(\check{j}(s'_0)) = \check{j}(s') = (s''_{|U_i})$, luego $j(s'_0) = s''$.

2. Si F y F' son Caa entonces F'' es Caa. Efectivamente, sea V un abierto afín y $\mathscr{W}$ un recubrimiento por abiertos afines de V, la sucesión

$$0 \to \Gamma(V, \check{C}^{\cdot}_{\mathscr{W}}(F)) \to \Gamma(V, \check{C}^{\cdot}_{\mathscr{W}}(F')) \to \Gamma(V, \check{C}^{\cdot}_{\mathscr{W}}(F'')) \to 0$$

es exacta y los dos primeros complejos son acíclicos, luego el tercero también.

3. Consideremos la sucesión exacta $0 \to F \to C^0F \to F_1 \to 0$ ($F_1 = C^0F/F$). Por 1., $0 \to F(X) \to C^0F(X) \to F_1(X) \to 0$ es exacta. Por 2., F_1 es Caa. Consideremos la sucesión exacta $0 \to F_1 \to C^1F \to F_2 \to 0$. Por 1., $0 \to F_1(X) \to C^1F(X) \to F_2(X) \to 0$ es exacta. Por 2., F_2 es Caa. Así sucesivamente, obtenemos que $F(X) \to C^{\cdot}(X)$ es una resolución, luego F es acíclico en X.

□

4. Observación : El teorema, anterior, para esquemas afines notherianos, podríamos haberlo demostrado usando la aciclicidad de los haces quasi-coherentes inyectivos. Véase para ello el problema 1.

5. Corolario : *Sea $\pi\colon X \to Y$ un morfismo de esquemas afín y $\mathscr{M}$ un haz quasi-coherente en X. Se cumple que*

$$H^i(X,\mathscr{M}) = H^i(Y,\pi_*\mathscr{M}).$$

Demostración. Sea $\mathscr{M} \to C^0\mathscr{M} \to C^1\mathscr{M} \to \dots$ una resolución de $\mathscr{M}$ por haces flascos. Se cumple que $\pi_*\mathscr{M} \to \pi_*C^0\mathscr{M} \to \pi_*C^1\mathscr{M} \to \dots$ es una sucesión exacta, porque para cada abierto afín $U \subset Y$,

$$H^i(\Gamma(U,\pi_*C^\cdot\mathscr{M}) = H^i(\Gamma(\pi^{-1}(U),C^\cdot\mathscr{M})) = H^i(\pi^{-1}(U),\mathscr{M}) \underset{13.3.3}{=} 0.$$

Además, la imagen directa de un haz flasco es flasco. Por tanto,

$$H^i(Y,\pi_*\mathscr{M}) = H^i(\Gamma(Y,\pi_*C^\cdot\mathscr{M})) = H^i(\Gamma(X,C^\cdot\mathscr{M})) = H^i(X,\mathscr{M}).$$

□

Si X es un esquema compacto semiseparado (i.e., la intersección de dos abiertos afines es afín), $\mathscr{M}$ es un haz quasi-coherente y los abiertos U_i forman un recubrimiento afín de X, entonces $U_{i_1} \cap \dots \cap U_{i_r}$ son afines y las inclusiones $U_{i_1} \cap \dots \cap U_{i_r} \hookrightarrow X$ son afines. Por tanto, los haces $\mathscr{M}_{U_{i_1}\cap\dots\cap U_{i_r}}$ son acíclicos y obtenemos el siguiente teorema.

6. Teorema : *Sea X un esquema compacto semiseparado y $X = U_1 \cup \dots \cup U_n$ un recubrimiento finito por abiertos afines. Para todo módulo quasi-coherente $\mathscr{M}$ el complejo de haces de Cech de $\mathscr{M}$ asociado al recubrimiento $\{U_i\}$ es una resolución finita*

$$0 \to \mathscr{M} \to \check{C}^0\mathscr{M} \to \dots \to \check{C}^n\mathscr{M} \to 0$$

por haces quasi-coherentes y acíclicos que depende de manera funtorial y exacta de $\mathscr{M}$.

En consecuencia los grupos de cohomología $H^i(X,\mathscr{M})$ son funtorialmente isomorfos a los grupos de cohomología del complejo $\Gamma(X,\check{C}^\cdot\mathscr{M})$ de cocadenas de Cech asociado al recubrimiento $\{U_i\}$:

$$H^i(X,\mathscr{M}) = H^i(\Gamma(X,\check{C}^\cdot\mathscr{M})).$$

Demostración. Si $U \subset X$ es un abierto afín $\mathscr{M}_U$ es quasi-coherente porque el morfismo $i\colon U \hookrightarrow X$ es cuasicompacto y $\mathscr{M}_U = i_*(\mathscr{M}_{|U})$. Sólo queda ver que $\check{C}^\cdot\mathscr{M}$ depende de modo exacto de $\mathscr{M}$: Esto es consecuencia de que para todo abierto afín U de X el funtor $\mathscr{M} \rightsquigarrow \mathscr{M}_U$ es exacto, porque el el funtor $\mathscr{M} \rightsquigarrow \mathscr{M}(V)$ (o equivalentemente $\mathscr{M} \rightsquigarrow \mathscr{M}_{|V}$) es exacto para todo abierto afín V. □

7. Teorema: *Sea X un esquema compacto. Las siguientes condiciones son equivalentes:*

1. *X es afín.*
2. *$H^i(X,\mathscr{M})=0$, para todo módulo quasi-coherente $\mathscr{M}$ y todo $i>0$.*
3. *$H^1(X,I)=0$, para todo haz de ideales quasi-coherente $I\subseteq\mathscr{O}_X$.*

Demostración. Sólo nos falta probar que 3. $\Rightarrow$ 1. Por el lema 11.2.14, basta probar que X es recubrible por abiertos afines X_{f_i}, con $f_i\in\Gamma(X,\mathscr{O}_X)$ y $(f_i)_i=\Gamma(X,\mathscr{O}_X)$.

Sea $x\in X$ un punto cerrado. Sea U un entorno abierto afín de x y $C=X\setminus U$. Sean $I_{C\cup x}$ y I_C los haces de ideales de $\mathscr{O}_X$ que se anulan en $C\cup x$ y C respectivamente. Tenemos la sucesión exacta

$$0\to I_{C\cup x}\to I_C\to k(x)\to 0$$

donde $k(x)$ es un haz quasi-coherente cuyo soporte es x y $k(x)_x=\mathscr{O}_{X,x}/\mathfrak{m}_x$. Tomando cohomología tenemos la sucesión exacta

$$\Gamma(X,I_C)\to\Gamma(X,k(x))=\mathscr{O}_{X,x}/\mathfrak{m}_x\to 0$$

Por tanto, existe $f\in\Gamma(X,I_C)\subseteq\Gamma(X,\mathscr{O}_X)$ cuyo valor en x es 1. En conclusión, $X_f=U_f$ es un entorno abierto afín de x.

Por noetherianidad de X existe un número finito $X_{f_1},\dots,X_{f_r}$ de abiertos afines que recubren X. Nos falta probar que $(f_i)_i=\Gamma(X,\mathscr{O}_X)$. Consideremos el epimorfismo $\pi\colon\mathscr{O}_X^r\to\mathscr{O}_X$, $(a_i)_i\mapsto\sum_i a_i f_i$. Tenemos la sucesión exacta

$$0\to\operatorname{Ker}\pi\to\mathscr{O}_X^r\xrightarrow{\pi}\mathscr{O}_X\to 0$$

Consideremos la filtración de $\operatorname{Ker}\pi$

$$\operatorname{Ker}\pi\supseteq\operatorname{Ker}\pi\cap\mathscr{O}_X^{r-1}\supseteq\cdots\supseteq\operatorname{Ker}\pi\cap\mathscr{O}_X$$

para una ordenación cualquiera de los sumandos de $\mathscr{O}_X^r$. Cada uno de los cocientes de esta filtración es un haz de ideales quasi-coherente de $\mathscr{O}_X$. Usando la hipótesis y las sucesiones exactas largas de cohomología obtenemos que $H^1(X,\operatorname{Ker}\pi)=0$. Por tanto, $\Gamma(X,\mathscr{O}_X^r)\to\Gamma(X,\mathscr{O}_X)$ es epiyectivo, luego $(f_i)_i=\Gamma(X,\mathscr{O}_X)$.

□

13.4. Estabilidad de la cohomología por cambios de base planos

1. Definición: Sea $f: X \to Y$ una aplicación continua entre espacios topológicos y F un haz de grupos abelianos en X. Llamaremos imagen directa superior i-ésima de F por f, y lo denotaremos $R^i f_*(F)$, al haz sobre Y asociado al prehaz

$$V \rightsquigarrow H^i(\pi^{-1}(V), F).$$

Dado que el haz cociente es el haz asociado al prehaz cociente, se concluye que $R^i f_*(F)$ es el i-ésimo haz de cohomología del complejo de haces $f_* C^{\cdot} F$; es decir,

$$R^i f_*(F) := H^i(f_* C^{\cdot} F).$$

Observe el lector que conoce la teoría de funtores derivados, que como los haces flascos son f_*-acíclicos y por el teorema 10.6.8 3., $R^i f_*(F)$ es el i-ésimo funtor derivado de f_* aplicado a F.

Dada una sucesión exacta de haces de grupos abelianos en X,

$$0 \to F_1 \to F_2 \to F_3 \to 0,$$

induce una sucesión exacta de complejos de haces,

$$0 \to f_* C^{\cdot} F_1 \to f_* C^{\cdot} F_2 \to f_* C^{\cdot} F_3 \to 0,$$

y por tanto una sucesión exacta larga

$$0 \to f_*(F_1) \to f_*(F_2) \to f_*(F_3) \to R^1 f_*(F_1) \to R^1 f_*(F_2) \to R^1 f_*(F_3) \to R^2 f_*(F_1) \to \cdots.$$

Además, si $F \to K^0 \to K^1 \to \cdots$ es una resolución de F por haces f_*-acíclicos (es decir, $R^i f_* K^n = 0$, para todo $i > 0$ y todo n), entonces $R^i f_* F = H^i(K^{\cdot})$, para todo i, por 7.2.17, ya que $f_* C^{\cdot} F \to f_* C^{\cdot} K^{\cdot}$ es un cuasi-isomorfismo (o por el teorema 10.6.8).

2. Teorema: *Sea $f: X \to Y$ un morfismo quasi-separado cuasicompacto y $\mathscr{M}$ un haz quasi-coherente en X. Se cumple que:*

1. *Si $Y = \operatorname{Spec} A$ es afín, entonces $R^i f_*(\mathscr{M}) = \widetilde{H^i(X, \mathscr{M})}$.*
2. *$R^i f_*(\mathscr{M})$ es un haz quasi-coherente.*

Demostración. 1. Sea $\mathscr{U} = \{U_i\}$ un recubrimiento finito saturado de X por abiertos afines y $\check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}$ el complejo de haces de Cech generalizado asociado al recubrimiento $\mathscr{U}$. Veamos que $R^i f_*\mathscr{M} = H^i f_* \check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}$. Sea $V \subset Y = \operatorname{Spec} A$ un abierto afín. $U_i \cap f^{-1}(V)$ es afín, porque la composición $U_i \hookrightarrow X \to \operatorname{Spec} A$ es un morfismo afín. Sea $\mathscr{U} \cap f^{-1}(V) = \{U_i \cap f^{-1}(V)\}$. Entonces,

$$H^i(f^{-1}(V), \mathscr{M}) = H^i\Gamma(f^{-1}(V), \check{C}^{\cdot}_{\mathscr{U}\cap f^{-1}(V)}\mathscr{M}) = H^i\Gamma(V, f_*\check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}).$$

Por tanto, $R^i f_*\mathscr{M} = H^i f_* \check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}$. Observemos que $f_*\check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}$ es un complejo de haces quasi-coherentes por 12.1.25. Por tanto, $R^i f_*\mathscr{M}$ es quasi-coherente y como Y es afín,

$$R^i f_*\mathscr{M}(Y) = (H^i f_* \check{C}^{\cdot}_{\mathscr{U}}\mathscr{M})(Y) = H^i\Gamma(Y, f_*\check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}) = H^i\Gamma(X, \check{C}^{\cdot}_{\mathscr{U}}\mathscr{M}) = H^i(X, \mathscr{M}).$$

□

3. Proposición: *Sea un diagrama conmutativo*

$$\begin{array}{ccc} \overline{X} & \xrightarrow{\bar{f}} & X \\ {\scriptstyle \bar{g}}\downarrow & & \downarrow{\scriptstyle g} \\ \overline{Y} & \xrightarrow{f} & Y \end{array}$$

y F un haz en X. Se tienen morfismos $f^{-1}R^i g_*(F) \to R^i \bar{g}_*(\bar{f}^{-1}F)$, funtoriales en F.

Si los espacios considerados son esquemas, los morfismos son morfismos de esquemas y F es un $\mathscr{O}_X$-módulo, entonces se tienen morfismos naturales $f^*R^i g_*(F) \to R^i \bar{g}_*(\bar{f}^*F)$ que se denominan morfismos de cambio de base.

Demostración. Existen morfismos naturales $R^i g_*(F) \to f_*R^i \bar{g}_*(\bar{f}^{-1}F)$, por la proposición 10.4.5. Por adjunción, obtenemos $f^{-1}R^i g_*(F) \to R^i \bar{g}_*(\bar{f}^{-1}F)$.

Para la segunda parte se argumenta igual, teniendo en cuenta el morfismo natural de composición $H^i(X,F) \to H^i(\bar{X}, \bar{f}^{-1}F) \to H^i(\bar{X}, \bar{f}^*F)$.

□

4. Definición: Un morfismo de esquemas $f : X \to Y$ se dice que es plano si para todo punto $x \in X$, el morfismo $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ es plano. Diremos que un $\mathscr{O}_X$-módulo quasi-coherente $\mathscr{M}$ es plano sobre Y, si para todo punto $x \in X$, $\mathscr{M}_x$ es un $\mathscr{O}_{Y,f(x)}$-módulo plano.

5. Ejercicio: Probar que un $\mathscr{O}_X$-módulo quasi-coherente $\mathscr{M}$ es plano sobre Y, si para todo punto $x \in X$ existen entornos abiertos afines U de x y V de $f(x)$, tal que $f(U) \subset V$, de modo que $\mathscr{M}(U)$ es un $\mathscr{O}_Y(V)$-módulo plano.

6. Teorema: *Sea $g: X \to Y$ un morfismo de esquemas quasi-separado quasi-compacto y $f: \overline{Y} \to Y$ un morfismo de esquemas plano. Consideremos el diagrama conmutativo*

$$\begin{array}{ccc} X \times_Y \overline{Y} & \xrightarrow{\bar{f}} & X \\ \downarrow{\scriptstyle \bar{g}} & & \downarrow{\scriptstyle g} \\ \overline{Y} & \xrightarrow{f} & Y \end{array}$$

con $\bar{g}$ y $\bar{f}$ las proyecciones obvias. Para todo módulo quasi-coherente $\mathscr{M}$ sobre X, los morfismos de cambios de base

$$f^* R^i g_*(\mathscr{M}) \to R^i \bar{g}_*(\bar{f}^* \mathscr{M})$$

son isomorfismos, para todo $i \geq 0$.

Demostración. El problema es local en Y y en $\overline{Y}$, luego podemos suponer que $Y = \operatorname{Spec} A$ e $\overline{Y} = \operatorname{Spec} B$ son afines. Denotemos $\overline{X} = X \times_Y \overline{Y}$. Por 13.4.2, tenemos que probar que

$$H^i(X, \mathscr{M}) \otimes_A B \simeq H^i(\overline{X}, \bar{f}^* \mathscr{M})$$

Sea $\{U_i\}$ un recubrimiento finito saturado por abiertos afines de X y sea $\Gamma(X, \check{C}^\cdot \mathscr{M})$ el complejo de cocadenas de Cech de $\mathscr{M}$ asociado a dicho recubrimiento. Entonces $\{\overline{U}_i = \bar{f}^{-1}(U_i)\}$ es un recubrimiento finito saturado de $\overline{X}$ por abiertos afines y el complejo $\Gamma(\overline{X}, \check{C}^\cdot \bar{f}^* \mathscr{M})$ de cocadenas de Cech del haz $\bar{f}^* \mathscr{M}$ asociado al recubrimiento finito $\{\bar{U}_i\}$ coincide con $\Gamma(X, \check{C}^\cdot \mathscr{M}) \otimes_A B$. Es decir,

$$\Gamma(X, \check{C}^\cdot \mathscr{M}) \otimes_A B = \Gamma(\overline{X}, \check{C}^\cdot \bar{f}^* \mathscr{M})$$

Tomando cohomología y por ser B plano sobre A, se concluye.

□

13.5. Acotación de la cohomología por la dimensión.

El objetivo de esta sección es demostrar que los grupos de cohomología de un haz (de grupos abelianos) sobre un esquema noetheriano están acotados por la dimensión.

1. Definición: Dado un haz F sobre un espacio topológico X, llamaremos soporte de F y lo denotaremos $\operatorname{Sop} F$, a

$$\operatorname{Sop} F = \{x \in X : F_x \neq 0\}$$

Si X es un esquema, denotaremos $\dim F = \max\{\dim \bar{x} \mid x \in \operatorname{Sop} F\}$.

2. Teorema: *Sea X un esquema noetheriano de dimensión finita y $\mathscr{M}$ un haz en X. Se cumple que*

$$H^i(X,\mathscr{M}) = 0, \text{ para } i > \dim \mathscr{M}.$$

Demostración. Demostremos el teorema por inducción sobre $\dim \mathscr{M}$.

Si $\dim \mathscr{M} = -1$ entonces $\mathscr{M} = 0$ y el teorema es obvio. Sean $\{x_i\}$ los puntos minimales de $\operatorname{Sop}\mathscr{M}$. Sea $i: x_i \hookrightarrow X$ la inclusión obvia y $\mathscr{M}_{x_i} := i_* i^{-1}\mathscr{M}$. $i^{-1}\mathscr{M}$ es flasco, luego $\mathscr{M}_{x_i}$ también. Por tanto, $\oplus_{x_i} \mathscr{M}_{x_i}$ es un haz flasco. Sea $\phi: \mathscr{M} \to \oplus_{x_i} \mathscr{M}_{x_i}$ el morfismo natural (obsérvese que la fibra de una sección de $\mathscr{M}$ es no nula en un número finito de x_i). El morfismo ϕ es un isomorfismo en los x_i y la dimensión de $\operatorname{Ker}\phi$ y $\operatorname{Coker}\phi$ es menor estrictamente que la de $\mathscr{M}$, porque $(\mathscr{M}_{x_i})_y = 0$ si $y \notin \bar{x}_i$. Por hipótesis de inducción, $H^i(X, \operatorname{Ker}\phi) = H^i(X, \operatorname{Coker}\phi) = 0$, para $i \geq \dim \mathscr{M}$. De la sucesión

$$0 \to \operatorname{Im}\phi \to \oplus_{x_i} \mathscr{M}_{x_i} \to \operatorname{Coker}\phi \to 0$$

y la sucesión exacta larga de cohomología obtenemos que $H^i(X, \operatorname{Im}\phi) = 0$, para $i > \dim \mathscr{M}$. De la sucesión

$$0 \to \operatorname{Ker}\phi \to \mathscr{M} \to \operatorname{Im}\phi \to 0$$

y la sucesión exacta de cohomología obtenemos que $H^i(X,\mathscr{M}) = 0$, para $i > \dim \mathscr{M}$. □

3. Observaciones: a) Sea X un esquema noetheriano y $\mathscr{M}$ un haz de dimensión cero. En la demostración del teorema anterior hemos probado que $\mathscr{M} = \oplus_{x \in X} \mathscr{M}_x$. Por tanto, $\mathscr{M}(U) = \oplus_{x \in U} \mathscr{M}_x$ y $\mathscr{M}$ es un haz flasco.

b) Si $\mathscr{L}$ es un haz de línea y $\mathscr{M}$ un haz de $\mathscr{O}_X$-módulos de dimensión cero, entonces $\mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{L} \simeq \mathscr{M}$. En efecto, $\mathscr{L}_x \simeq \mathscr{O}_{X,x}$ luego $(\mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{L})_x = \mathscr{M}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{L}_x \simeq \mathscr{M}_x$. Por tanto, $\dim(\mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{L}) = \dim \mathscr{M} = 0$. Si fijamos para cada $x \in X$ un isomorfismo $(\mathscr{M} \otimes_{\mathscr{O}_C} \mathscr{L})_x \simeq \mathscr{M}_x$, podemos definir los isomorfismos

$$\mathscr{M}(U) = \oplus_{x \in U} \mathscr{M}_x \simeq \oplus_{x \in U} (\mathscr{M} \otimes_{\mathscr{O}_C} \mathscr{L})_x = (\mathscr{M} \otimes_{\mathscr{O}_C} \mathscr{L})(U)$$

y $\mathscr{M} \simeq (\mathscr{M} \otimes_{\mathscr{O}_C} \mathscr{L})$.

13.6. Teoremas de finitud

La dimensión de los grupos de cohomología de los haces de localizaciones de las variedades proyectivas son invariantes importantes en su clasificación. Para su uso efectivo necesitamos probar que dichas dimensiones son finitas.

Probaremos que la cohomología de los haces coherentes de las variedades proyectivas es finita calculando primero la cohomología de los $\mathscr{O}_{\mathbb{P}^n}(m)$ y resolviendo todo módulo por haces de línea, $\mathscr{O}_{\mathbb{P}^n}(m)$. Calcularemos la cohomología de los haces coherentes de una curva, desingularizándola y proyectándola sobre la recta proyectiva.

13.6.1. Caracterización cohomológica de la recta proyectiva

Sea C una curva completa no singular de cuerpo de fracciones Σ y haz estructural $\mathscr{O}$. Consideremos la sucesión exacta

$$0 \to \mathscr{O} \to \Sigma \xrightarrow{\pi} \Sigma/\mathscr{O} \to 0$$

donde Σ es el haz constante Σ. La fibra de $\Sigma/\mathscr{O}$ en el punto genérico es cero, luego la dimensión del soporte de $\Sigma/\mathscr{O}$ es cero y $\Gamma(U, \Sigma/\mathscr{O}) = \bigoplus_{x \in U} \Sigma/\mathscr{O}_x$. Dado un punto cerrado $x \in C$, denotemos por $\mathfrak{m}_x \subseteq \mathscr{O}_x$ el ideal de las funciones que se anulan en x. Sea $t \in \mathscr{O}_x$ un parámetro en x, es decir, $\mathfrak{m}_x = t \cdot \mathscr{O}_x$. Se verifica que $(\mathscr{O}_x)_t = \Sigma_C$, luego dada $f \in \Sigma$, se tiene que $f = \frac{a}{t^n}$ para un $n \in \mathbb{N}$ y un $a \in \mathscr{O}_x$. Si x es un punto racional, sabemos que $a = \sum_{i=1}^{n} a_i t^i + bt^n$, con $a_i \in k$ y $b \in \mathscr{O}_x$. En conclusión, $f = \sum_{i=1}^{n} \frac{a_i}{t^{n-i}} \mod \mathscr{O}_x$, luego

$$\Sigma/\mathscr{O}_x = \left\{ \sum_{i=1}^{n} \frac{a_i}{t^i},\ n \text{ variable}, a_i \in k \right\}$$
$$= \{\text{partes princ. del desarrollo de Laurent en el punto } x \text{ de } f \in \Sigma\}$$

El morfismo π asigna a cada $f \in \Sigma = \Sigma(U)$ las partes principales de sus desarrollos de Laurent en los puntos $x \in U$.

1. Ejercicio: Si el punto cerrado $x \in C$ no es racional, entonces

$$\Sigma/\mathscr{O}_x = \left\{ \sum_{i=1}^{n} \frac{a_i}{t^i},\ n \text{ variable}, a_i \in \mathscr{O}_x/\mathfrak{m}_x \right\}$$

(Pista: Recordar que, por el teorema de Cohen, el morfismo de paso al cociente $\widehat{\mathscr{O}}_x \to \widehat{\mathscr{O}}_x/\mathfrak{m}_x\widehat{\mathscr{O}}_x = \mathscr{O}_x/\mathfrak{m}_x$ tiene sección).

2. Teorema: *Una curva C completa y no singular es isomorfa a la recta proyectiva $\Leftrightarrow$ existe un punto racional $x \in C$ y $H^1(C, \mathscr{O}) = 0$.*

Demostración. $\Rightarrow$) Como la cohomología es estable por cambio de base planos, podemos suponer que k es algebraicamente cerrado. Consideremos la sucesión exacta larga de cohomología asociada a la sucesión exacta $0 \to \mathscr{O} \to \Sigma \xrightarrow{\pi} \Sigma/\mathscr{O} \to 0$, con $C = \mathbb{P}^1$ (luego $\Sigma = k(x)$)

$$\Sigma \xrightarrow{\pi} \Gamma(\mathbb{P}^1, \Sigma/\mathscr{O}) = \bigoplus_{y\in\mathbb{P}^1} \Sigma/\mathscr{O}_y \to H^1(\mathbb{P}^1, \mathscr{O}) \to H^1(\mathbb{P}^1, \Sigma) = 0$$

Dada $s \in \Gamma(\mathbb{P}^1, \Sigma/\mathscr{O})$, se escribe $s = (\sum_{j=1}^{n_i} \frac{a_{ij}}{(x-\alpha_i)^j})$. [1] Las funciones $\frac{1}{x-\alpha}$ tienen polo sólo en el punto $\alpha \in \mathbb{P}^1$, por tanto, la imagen por π de $f(x) = \sum_i \sum_{j=1}^{n_i} \frac{a_{ij}}{(x-\alpha_i)^j}$ es s. En conclusión, π es epiyectiva y $H^1(\mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}) = 0$.

$\Leftarrow$) Consideremos la sucesión exacta larga asociada a $0 \to \mathscr{O} \to \Sigma \xrightarrow{\pi} \Sigma/\mathscr{O} \to 0$, de nuevo, y los morfismos inducidos en cohomología

$$\Sigma \to \Gamma(C, \Sigma/\mathscr{O}) = \bigoplus_{x\in C} \Sigma/\mathscr{O}_x \to H^1(C, \mathscr{O}) = 0 \qquad (**).$$

Sea t un parámetro en el punto x (es decir, $(\mathfrak{m}_x)_x = t\cdot\mathscr{O}_x$) y sea $s \in \Gamma(C, \Sigma/\mathscr{O})$ el elemento que vale $1/t$ en la componente de x y cero en las demás. Por la sucesión exacta $(**)$ existe $f \in \Sigma$ que se aplica en s. Por tanto, f no tiene polos en C, salvo en x donde tiene un polo de orden 1. Por tanto, el morfismo $\widetilde{f}\colon C \to \mathbb{P}^1$ inducido por la inclusión $k(f) \hookrightarrow \Sigma$ es de grado 1, es decir, es un isomorfismo. □

3. Ejemplo: Consideremos en el plano proyectivo real la elipse imaginaria

$$C \equiv x_0^2 + x_1^2 + x_2^2 = 0.$$

La elipse imaginaria C no tiene puntos racionales, luego no puede ser isomorfa a la recta proyectiva. Por otra parte, si hacemos el cambio de base $\mathbb{R} \to \mathbb{C}$, la elipse imaginaria ya es isomorfa a la recta proyectiva, pues es isomorfa al haz de rectas que pasa por cualquiera de sus puntos. Entonces, $H^1(C \times_{\mathbb{R}} \mathbb{C}, \mathscr{O}_{C\times_{\mathbb{R}}\mathbb{C}}) = H^1(\mathbb{P}^1_{\mathbb{C}}, \mathscr{O}_{\mathbb{P}^1_{\mathbb{C}}}) = 0$ y por el teorema de cambio de base $H^1(C, \mathscr{O}_C) = 0$.

4. Ejercicio: Calcular mediante la cohomología Cech la cohomología de $\mathbb{P}^1$.

13.6.2. Cohomología de los morfismos proyectivos

Sea A un anillo, $R = A[x_0, \dots, x_r]$ y $\mathbb{P}^r_A = \operatorname{Proj} R$ el espacio proyectivo r-dimensional sobre A.

Sea $R' = R/(x_0) = A[x_1, \dots, x_r]$. Entonces $\mathbb{P}^{r-1}_A = \operatorname{Proj} R' \xrightarrow{j} \operatorname{Proj} R = \mathbb{P}^r_A$ es un hiperplano.

[1] El desarrollo de Laurent en el punto del infinito es un polinomio en x sin coeficiente constante.

Consideremos la sucesión exacta de R-módulos graduados

$$0 \to R(-1) \xrightarrow{\cdot x_0} R \to R' \to 0$$

Corriendo los grados

$$0 \to R(n-1) \to R(n) \to R'(n) \to 0$$

y tomando los haces asociados, obtenemos la sucesión exacta

$$0 \to \mathscr{O}_{\mathbb{P}^r_A}(n-1) \to \mathscr{O}_{\mathbb{P}^r_A}(n) \to j_*\mathscr{O}_{\mathbb{P}^{r-1}_A}(n) \to 0$$

.

5. Lema: *Para cada entero n el morfismo natural $R_n \to \Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n))$ es un isomorfismo.*

Demostración. Si $n < 0$, $\Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)) = 0$ En efecto, $\bigcap_{i=0}^{r} \mathscr{O}_{\mathbb{P}^r_A}(n)(U^h_{x_i}) = 0$, porque si $\frac{p_{m+n}}{x_i^m} = \frac{q_{m'+n}}{x_j^{m'}}$, entonces $x_j^{m'} \cdot p_{m+n} = x_i^m \cdot q_{m'+n}$, luego x_i^m divide a p_{m+n} lo cual es imposible. Por tanto, $\Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)) = 0 = R_n$. Supongamos $n \geq 0$. Procedemos por inducción sobre r. Para $r = 0$ no hay nada que decir. Tenemos que probarlo para $r > 0$. Hipótesis de inducción: el lema es cierto para $0, \ldots, r-1$. Si $n \geq 0$, procedemos ahora por inducción sobre n. Consideramos el diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R_{n-1} & \longrightarrow & R_n & \longrightarrow & R'_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n-1)) & \longrightarrow & \Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)) & \longrightarrow & \Gamma(\mathbb{P}^{r-1}_A, \mathscr{O}_{\mathbb{P}^{r-1}_A}(n)) & &
\end{array}$$

Los morfismos verticales de los extremos son isomorfismos por inducción. Luego, el morfismo $\Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)) \to \Gamma(\mathbb{P}^{r-1}_A, \mathscr{O}_{\mathbb{P}^{r-1}_A}(n))$ es epiyectivo, luego $R_n \to \Gamma(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n))$ es un isomorfismo.

□

6. Cohomología de los $\mathscr{O}_{\mathbb{P}^r_A}(n)$: *Se cumple que:*

1. *Si $n \geq 0$, $\mathscr{O}_{\mathbb{P}^r_A}(n)$ es acíclico y $H^0(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n))$ es un A-módulo libre de rango $\binom{n+r}{r}$.*
2. *Si $n > 0$, $H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(-n)) = 0$ para $i \neq r$ y $H^r(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(-n))$ es nulo para $0 < n \leq r$ y un A-módulo libre de rango $\binom{n-1}{r}$ para $n > r$.*

Demostración. 1. Las secciones globales de $\mathscr{O}_{\mathbb{P}^r_A}(n)$ son, por el lema anterior, los polinomios homogéneos de grado n, que es un A-módulo libre de rango $\binom{n+r}{r}$. La aciclicidad de $\mathscr{O}_{\mathbb{P}^r_A}(n)$ $(n \geq 0)$ la probamos por inducción sobre r, siendo el caso $r = 0$ trivial. Consideremos la sucesión exacta

$$0 \to \mathscr{O}_{\mathbb{P}^r_A}(n-1) \to \mathscr{O}_{\mathbb{P}^r_A}(n) \to j_*\mathscr{O}_{\mathbb{P}^{r-1}_A}(n) \to 0.$$

Como la sucesión de secciones globales es exacta por el lema anterior, y como $j_*\mathscr{O}_{\mathbb{P}^{r-1}_A}(n)$ es acíclico por inducción, se tienen los isomorfismos

$$H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n-1)) \xrightarrow{\sim} H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)), \qquad \text{para todo } i > 0 \text{ y } n \geq 0.$$

Como $\varinjlim \mathscr{O}_{\mathbb{P}^r_A}(n) i_* \mathscr{O}_{\mathbb{P}^r_A U}$, siendo $U = \mathbb{P}^r_A \setminus \mathbb{P}^{r-1}_A \xhookrightarrow{i} \mathbb{P}^r_A$ (proposición 12.3.3), y la cohomología conmuta con el límite inductivo, se tiene

$$H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n)) = H^i(\mathbb{P}^r_A, i_*\mathscr{O}_{\mathbb{P}^r_A U}) = 0$$

ya que i es un morfismo afín.

2. Se demuestra por inducción sobre n (se utiliza el caso $n = 0$ que ha sido resuelto en el apartado anterior) a partir de la sucesión

$$\cdots \to H^{i-1}(\mathbb{P}^{r-1}_A, \mathscr{O}_{\mathbb{P}^{r-1}_A}(-n)) \to H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(-n-1)) \to H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(-n)) \to \cdots,$$

asociada a la sucesión

$$0 \to \mathscr{O}_{\mathbb{P}^r_A}(-n-1) \to \mathscr{O}_{\mathbb{P}^r_A}(-n) \to j_*\mathscr{O}_{\mathbb{P}^{r-1}_A}(-n) \to 0$$

y por inducción sobre r.

□

7. Observación: Si denotamos $\binom{n+r}{r} = \left|\frac{(n+r)\cdot\ldots\cdot(n+1)}{r!}\right|$, entonces $H^i(\mathbb{P}^r_A, \mathscr{O}_{\mathbb{P}^r_A}(n))$ es un A-módulo libre de rango

$$\begin{cases} \binom{n+r}{r} \text{ para } \begin{cases} i = 0 \text{ y } n \geq 0 \\ i = r \text{ y } n < 0 \end{cases} \\ 0 \text{ en los demás casos.} \end{cases}$$

13.6.3. Cohomología de los haces coherentes en variedades proyectivas

8. Teorema de finitud de Serre: *Sea X un esquema proyectivo sobre un anillo noetheriano A y $\mathscr{M}$ un haz coherente en X. Se verifica*

1. Los grupos de cohomología $H^i(X,\mathscr{M})$ son A-módulos finito generados para todo i.

2. Existe un entero n_0, que depende de $\mathscr{M}$, tal que $\mathscr{M}(n)$ es acíclico para $n \geq n_0$.

3. Existe un entero n_0, que depende de $\mathscr{M}$, tal que $\mathscr{M}(n)$ está generado por sus secciones globales para todo $n \geq n_0$, esto es, el morfismo natural

$$\Gamma(X,\mathscr{M}(n)) \otimes_A \mathscr{O}_X \to \mathscr{M}(n)$$

es epiyectivo.

Demostración. 1. Sea $X = \operatorname{Proj} A[\xi_0,\dots,\xi_r]$. El epimorfismo $A[x_0,\dots,x_r] \to A[\xi_0,\dots,\xi_r]$ obvio induce una inmersión cerrada $i : X \hookrightarrow \mathbb{P}^r_A$. Por ser i un morfismo afín, $H^i(X,\mathscr{M}) = H^i(\mathbb{P}^r, i_*\mathscr{M})$ y $i_*\mathscr{M}$ es un haz coherente en $\mathbb{P}^r$. Basta demostrar el teorema para $X = \mathbb{P}^r$. Por 12.3.6, existe una sucesión exacta

$$(*) \qquad 0 \to \operatorname{Ker} \to \bigoplus_{i=1}^{m} \mathscr{O}(n_i) \to \mathscr{M} \to 0$$

Por acotación cohomológica, $H^{r+1}(\mathbb{P}^r,\mathscr{M}) = 0$ para todo $\mathscr{M}$. Por la sucesión exacta larga de cohomología se obtiene que $H^r(\mathbb{P}^r,\mathscr{M})$ es finito para todo $\mathscr{M}$. En particular $H^r(\mathbb{P}^r,\operatorname{Ker})$ es finito. De nuevo por la sucesión exacta larga de cohomología $H^{r-1}(\mathbb{P}^r,\mathscr{M})$ es finito. En particular, $H^{r-1}(\mathbb{P}^r,\operatorname{Ker})$ es finito. Por inducción descendente concluimos.

2. Igual que antes, basta demostrar el teorema para $X = \mathbb{P}^r_A$. Tensamos la sucesión exacta $(*)$ por un $\mathscr{O}_{\mathbb{P}^r}(k)$ tal que $n_i + k > 0$ para todo i. Tomando la sucesión exacta larga de cohomología obtenemos que $H^r(\mathbb{P}^r,\mathscr{M}(n)) = 0$, para $n \geq k$. Descendiendo como en 1. se acaba.

3. Basta probarlo para el espacio proyectivo. Tensamos la sucesión exacta $(*)$ por un $\mathscr{O}_{\mathbb{P}^r}(k)$ tal que $n_i + k \geq 0$ para todo i. Basta ver entonces que para $n \geq 0$ el haz $\mathscr{O}(n)$ está generado por sus secciones globales, es decir, que $R_n \otimes_A \mathscr{O} \to \mathscr{O}(n)$ es epiyectivo. $\mathscr{O}(n)$ es la localización homogénea de $\bigoplus_{r\geq 0} R_{n+r}$. El morfismo graduado

$$R_n \otimes_A R \to \bigoplus_{r\geq 0} R_{n+r},\ f \otimes g \mapsto f \cdot g,$$

es epiyectivo y se concluye. □

El Teorema de finitud de Serre puede relativizarse dando el siguiente teorema.

9. Teorema de finitud de Serre: *Sea Y un esquema noetheriano, $f: X \to Y$ un morfismo localmente proyectivo y $\mathscr{M}$ un haz coherente en X. Se verifica:*

1. *Las imágenes directas superiores $R^i f_*(\mathscr{M})$ son coherentes para todo i.*
2. *Para n suficientemente grande, $R^i f_*(\mathscr{M}(n)) = 0$ para todo $i > 0$.*
3. *Para n suficientemente grande, el morfismo natural*

$$f^* f_* \mathscr{M}(n) \to \mathscr{M}(n)$$

es epiyectivo.

Demostración. Como Y es compacto, los problemas son locales en Y, luego puede suponerse que Y es el espectro de un anillo noetheriano y que X es un esquema proyectivo sobre él, con lo que estamos en las hipótesis teorema anterior. □

10. Observación: La parte 1. del teorema anterior es cierta en hipótesis más generales, basta que $f: X \to Y$ sea un morfismo propio e Y localmente noetheriano. Para ello véase el teorema 13.13.4

11. Ejercicio: Sea $R = R_0[\xi_1, \ldots, \xi_r]$ un anillo graduado, con R_0 anillo noetheriano, $\operatorname{gr} \xi_i = 1$, $X = \operatorname{Proj} R$ y $\mathscr{M}$ un $\mathscr{O}_X$-módulo coherente. Prueba que $M = \oplus_{n \in \mathbb{N}} \Gamma(X, \mathscr{M}(n))$ es un R-módulo finito generado.

Resolución: Sea $i: X \hookrightarrow \mathbb{P}^{r-1}$ la inmersión cerrada inducida por el epimorfismo obvio $R_0[x_1, \ldots, x_r] \to R_0[\xi_1, \ldots, \xi_r]$. Como $\Gamma(X, \mathscr{M}(n)) = \Gamma(\mathbb{P}^{r-1}, (i_* \mathscr{M})(n))$, podemos suponer que $X = \mathbb{P}^r$. Por 12.3.6, existe una sucesión exacta

$$(*) \qquad 0 \to \operatorname{Ker} \to \bigoplus_{i=1}^{m} \mathscr{O}_{\mathbb{P}^{r-1}}(n_i) \to \mathscr{M} \to 0$$

y por el teorema de finitud de Serre, $\operatorname{Ker}(n)$ es acíclico para todo $n >> 0$. Para $s \geq 0$, $\Gamma(\mathbb{P}^{r-1}, \mathscr{O}(s)) = R_s$ y $\oplus_{t \geq s} \Gamma(\mathbb{P}^{r-1}, \mathscr{O}(t)) = (x_1, \ldots, x_r)^s$. Luego, si $\mathscr{N} = \bigoplus_{i=1}^{m} \mathscr{O}(n_i)$, entonces $\oplus_{n' \geq n} \Gamma(\mathbb{P}^{r-1}, \mathscr{N}(n'))$ es un R-módulo finito generado para $n >> 0$. Por tanto, el cociente $\oplus_{n' \geq n} \Gamma(\mathbb{P}^{r-1}, \mathscr{M}(n'))$ es un R-módulo finito generado para $n >> 0$. Luego, el R-módulo $\oplus_{n' \in \mathbb{N}} \Gamma(\mathbb{P}^{r-1}, \mathscr{M}(n'))$ es finito generado.

12. Definición: Sea X una variedad proyectiva de dimensión r sobre un cuerpo k y $\mathscr{M}$ un módulo coherente sobre X. Llamaremos característica (de Euler-Poincaré) de $\mathscr{M}$, y lo denotaremos $\chi(X, \mathscr{M})$ ó $\chi(\mathscr{M})$, a la suma alternada de las dimensiones de sus grupos de cohomología:

$$\chi(X, \mathscr{M}) := \sum_{i=0}^{r} h^i(X, \mathscr{M})$$

donde denotamos $h^i(X, \mathscr{M}) := \dim_k H^i(X, \mathscr{M})$.

Calculemos la característica de las intersecciones completas en los espacios proyectivos.

13. Teorema : *Sea $X \hookrightarrow \mathbb{P}^r_k$ una variedad proyectiva definida por el ideal homogéneo $(p_1,\dots,p_s) \subset k[x_0,\dots,x_r]$. Supongamos que $\{p_1,\dots,p_s\}$ es una sucesión regular de $k[x_0,\dots,x_r]$ y que p_i es homogéneo de grado d_i. Para todo $n \in \mathbb{Z}$, se verifica*

$$\chi(X,\mathcal{O}_X(n)) = (-1)^s \sum_{i=0}^{r-s} \binom{n+i}{i} \cdot \sum_{h_1+\dots+h_s=n-s-i} \prod_{j=1}^{s} (-1)^{h_j-1} \binom{d_j}{h_j+1}.$$

En particular, si X es una curva completa su género aritmético $\pi := h^1(X,\mathcal{O}_X)$ es igual a

$$\pi = 1 - (\prod_{j=1}^{r-1} d_j)(1 - \sum_{j=1}^{r-1} \frac{d_j - 1}{2}).$$

Si X es de dimensión cero, entonces $h^0(X,\mathcal{O}_X) = \prod_{j=1}^{r} d_j$, que es el teorema de Bézout.

Demostración. El cálculo de la característica de Euler de los $\mathcal{O}_X(n)$, en un caso concreto, se obtiene de modo sencillo por recurrencia. El cálculo de la fórmula general, se obtiene también por recurrencia, pero es algo más delicado.

Por el teorema 13.6.6 (y por 13.6.7), $\chi(\mathbb{P}^r,\mathcal{O}_{\mathbb{P}^r}(n))$ es igual al coeficiente de t^r de la serie $\frac{1}{(1-t)^{n+1}}$. Denotemos $X_l = (p_1,\dots,p_l)^h_0$. De la sucesión exacta

$$0 \to \mathcal{O}_{\mathbb{P}^r}(n-d_1) \xrightarrow{p_1\cdot} \mathcal{O}_{\mathbb{P}^r}(n) \to \mathcal{O}_{X_1}(n) \to 0$$

se obtiene

$$\chi(X_1,\mathcal{O}_{X_1}(n)) = \text{ Coef. de } t^r \text{ de } (\frac{1}{(1-t)^{n+1}} - \frac{1}{(1-t)^{n-d_1+1}}) = \text{ Coef. de } t^r \text{ en } \frac{1-(1-t)^{d_1}}{(1-t)^{n+1}}.$$

De $0 \to \mathcal{O}_{X_1}(n-d_2) \xrightarrow{p_2\cdot} \mathcal{O}_{X_1}(n) \to \mathcal{O}_{X_2}(n) \to 0$ se sigue

$$\chi(X_2,\mathcal{O}_{X_2}(n)) = \text{ Coef. de } t^r \text{ de } (\frac{1-(1-t)^{d_1}}{(1-t)^{n+1}} - \frac{1-(1-t)^{d_1}}{(1-t)^{n-d_2+1}})$$

$$= \text{ Coef. de } t^r \text{ de } \frac{1 - \sum_{j=1}^{2}(1-t)^{d_j} + (1-t)^{d_1+d_2}}{(1-t)^{n+1}} = \text{ Coef. de } t^r \text{ de } \frac{\prod_{j=1,2} 1-(1-t)^{d_j}}{(1-t)^{n+1}}$$

y por recurrencia

$$\begin{aligned}\chi(X,\mathcal{O}_X(n)) &= \text{ Coef. de } t^r \text{ de } \frac{\prod_{j=1}^{s} 1-(1-t)^{d_j}}{(1-t)^{n+1}}\\ &= \text{ Coef. de } t^r \text{ de } (-1)^s t^s \sum_{k\geq 0}\Big(\sum_{i=0}^{k}\binom{n+i}{i}\sum_{h_1+\ldots+h_s=k-i}\prod_{j=1}^{s}(-1)^{h_j-1}\binom{d_j}{h_j+1}\Big)t^k\\ &= (-1)^s\sum_{i=0}^{r-s}\binom{n+i}{i}\sum_{h_1+\ldots+h_s=n-s-i}\prod_{j=1}^{s}(-1)^{h_j-1}\binom{d_j}{h_j+1}.\end{aligned}$$

Lo demás al lector. □

Polinomio de Hilbert.

Sea $X \hookrightarrow \mathbb{P}^r_k$ una variedad proyectiva sobre un cuerpo k y $\mathcal{M}$ un haz coherente sobre X. Como sabemos la descomposición primaria de un A-módulo localiza, por tanto, tiene sentido hablar de los ideales primos asociados a $\mathcal{M}$. Los ceros de estos ideales primos diremos que son las componentes (sumergidas o no) del soporte de $\mathcal{M}$.

14. Teorema : *Existe un polinomio $P(t)$ con coeficientes racionales, cuyo grado es la dimensión del soporte de $\mathcal{M}$ y tal que*

$$P(n) = \chi(X,\mathcal{M}(n)) \quad \textit{para todo } n \geq 0.$$

Dicho polinomio se conoce como polinomio de Hilbert de $\mathcal{M}$.

Demostración. Por cambio de cuerpo base podemos suponer que k es algebraicamente cerrado.

Procedamos para la demostración del teorema por inducción sobre la dimensión del soporte de $\mathcal{M}$. Si la dimensión es cero es trivial. Sea pues $\dim \mathrm{Sop}\,\mathcal{M} \geq 1$. Sea $H \hookrightarrow \mathbb{P}^r_k$ un hiperplano que no pase por (es decir, no contenga) ninguna de las componentes sumergidas o no del soporte de $\mathcal{M}$. H está definida por un polinomio irreducible homogéneo de grado 1, $Q(x_0,\ldots,x_r)$. Sea $i\colon H\cap X \hookrightarrow X$ el morfismo obvio. Al tensar por $\mathcal{M}$ la sucesión exacta

$$0 \to \mathcal{O}_X(-1) \xrightarrow{\cdot Q} \mathcal{O}_X \to i_*\mathcal{O}_{H\cap X} \to 0$$

se obtiene

$$0 \to \mathcal{M}(-1) \to \mathcal{M} \to \mathcal{M}_H \to 0$$

siendo $\mathcal{M}_H = (i_*\mathcal{O}_{H\cap X})\otimes_{\mathcal{O}_X}\mathcal{M} = i_*\mathcal{M}_{|H\cap X}$. El soporte de $\mathcal{M}_H$ es de dimensión estrictamente menor que el soporte de $\mathcal{M}$. Por inducción, existe un polinomio $R(t)$ de grado $\dim \mathrm{Sop}\,\mathcal{M} - 1$ tal que

$$R(n) = \chi(X,\mathcal{M}_H(n)), \qquad \text{para todo } n \geq 0.$$

Así, $\chi(X,\mathscr{M}(n+1))-\chi(X,\mathscr{M}(n))=R(n+1)$ es un polinomio en n de grado $\dim \operatorname{Sop}\mathscr{M}-1$ (para $n+1\geq 0$), luego $\chi(X,\mathscr{M}(n))$ es un polinomio en n de grado la dimensión del soporte de $\mathscr{M}$ (para $n\geq 0$). □

15. Observación: Por el teorema de finitud de Serre 13.6.8, sabemos que $\mathscr{M}(n)$ es acíclico para $n>>0$. Por tanto, $\chi(X,\mathscr{M}(n))=\dim_k \Gamma(X,\mathscr{M}(n))$, para $n>>0$. $\mathscr{M}$ es igual al haz de localizaciones homogéneas del módulo graduado $M=\oplus_{n\in\mathbb{N}}\Gamma(X,\mathscr{M}(n))$. Escribamos $X=\operatorname{Proj} k[\xi_1,\ldots,\xi_n]$. M es un $k[\xi_1,\ldots,\xi_n]$-módulo graduado finito generado, por 13.6.11, y como sabemos la función de Hilbert H_M de M es, por definición, $H_M(n)=\dim_k M_n=\dim_k \Gamma(X,\mathscr{M}(n))$.

16. Teorema: *Sea L una subvariedad lineal de codimensión d de $\mathbb{P}^r$ que no pasa por ninguna componente (sumergida o no) de una variedad proyectiva de dimensión d, $X\subseteq\mathbb{P}^r$ y tal que $L\cap X$ sea un número finito de puntos cerrados. Sea $P(n)$ el polinomio de Hilbert de $\mathscr{O}_X$. Entonces,*

$$\Delta^d P(n)=d!\cdot \textit{ Coeficiente de grado } d \textit{ de } P(n)=(X\cap L),$$

donde $(X\cap L)=h^0(X\cap L,\mathscr{O}_{X\cap L})$ es el número de puntos, contando grados y multiplicidades, de $X\cap L$ (si $d=0$ tomaremos $L=\mathbb{P}^r$). Por tanto, el número de puntos de intersección de X con una variedad lineal de dimensión complementaria (y sin componentes comunes) no depende de la variedad lineal y se conoce como grado de X.

Demostración. Podemos suponer que k es algebraicamente cerrado. Sea H un hiperplano que pase por L y que no pase por ninguna componente (sumergida o no) de X. Se tiene la sucesión exacta

$$0\to\mathscr{O}_X(-1)\to\mathscr{O}_X\to\mathscr{O}_{X\cap H}\to 0$$

luego el polinomio de Hilbert de $\mathscr{O}_{X\cap H}$ es la diferencia del de $\mathscr{O}_X$. Repitiendo el proceso, $\Delta^d P(n)=\chi(\mathscr{O}_{X\cap L}(n))=h^0(\mathscr{O}_{X\cap L})=(X\cap L)$. □

13.6.4. Cohomología de los haces coherentes en curvas

Vamos a demostrar la finitud de los grupos de cohomología de una curva completa sobre un cuerpo k. Esto lo haremos reduciendo el problema a una curva lisa (por desingularización) y después por proyección a la recta proyectiva.

17. Teorema: *Sea C una curva completa sobre un cuerpo k y $\mathscr{M}$ un haz coherente en C. Se cumple que:*

1. *$H^0(C,\mathscr{M})$ y $H^1(C,\mathscr{M})$ son k-espacios vectoriales de dimensión finita.*

2. $H^i(C,\mathscr{M}) = 0$ *para* $i > 1$.

Demostración. La segunda parte es por acotación cohomológica. Para la primera, sea $\pi\colon \tilde{C} \to C$ el morfismo de desingularización de C. Consideremos el morfismo natural $i\colon \mathscr{M} \to \pi_*\pi^*\mathscr{M}$ y la sucesión exacta

$$0 \to \operatorname{Ker} i \to \mathscr{M} \to \pi_*\pi^*\mathscr{M} \to \operatorname{Coker} i \to 0$$

$\operatorname{Coker} i$ y $\operatorname{Ker} i$ tienen el soporte concentrado en los puntos singulares de C, luego son flascos y sus secciones son k-espacios vectoriales de dimensión finita. En efecto, sean $x_1,\dots,x_n$ los puntos singulares de C. Si un módulo $\mathscr{M}$ está concentrado en ellos, entonces para cada abierto afín U, $\mathscr{M}(U)$ es un $\mathscr{O}(U)/\operatorname{Anul}(\mathscr{M}(U))$-módulo finito generado. Ahora bien, $\mathscr{O}(U)/\operatorname{Anul}(\mathscr{M}(U))$ es un k-espacio vectorial de dimensión finita porque $\operatorname{Anul}(\mathscr{M}(U)) \neq 0$, luego $\mathscr{M}(U)$ es un k-espacio de dimensión finita y por tanto $\Gamma(C,\mathscr{M})$ también.

Así pues, basta demostrar el teorema para $\pi_*\pi^*\mathscr{M}$. Ahora bien, $H^\cdot(C,\pi_*\pi^*\mathscr{M}) = H^\cdot(\tilde{C},\pi^*\mathscr{M})$ porque π es un morfismo afín, y éstos conservan la cohomología por 13.3.5. En conclusión, como $\pi^*\mathscr{M}$ es coherente por 12.1.23, podemos suponer que C es no singular.

Sea $\phi\colon C \to \mathbb{P}^1$ un morfismo finito en la recta proyectiva. Se verifica que $H^\cdot(C,\mathscr{M}) = H^\cdot(\mathbb{P}^1,\phi_*\mathscr{M})$. Luego basta demostrar el teorema en la recta proyectiva y hemos concluido. □

18. Proposición: *Sea* $i\colon C \hookrightarrow \mathbb{P}^2$ *la curva proyectiva plana definida por los ceros de un polinomio homogéneo* $p_n(x_0,x_1,x_2)$. *Entonces* $\dim_k H^1(C,\mathscr{O}_C) = \frac{(n-1)\cdot(n-2)}{2}$.

Demostración. Tómese la sucesión exacta larga de cohomología asociada a la sucesión

$$0 \to \mathfrak{p}_C = \mathscr{O}_{\mathbb{P}^2}(-n) \xrightarrow{p_n\cdot} \mathscr{O}_{\mathbb{P}^2} \longrightarrow i_*\mathscr{O}_C \to 0$$

donde $\mathfrak{p}_C$ es el haz de ideales de funciones que se anulan en C. □

19. Definición: Se llama género aritmético de una curva completa C a la dimensión de $H^1(C,\mathscr{O}_C)$. Se llama género geométrico al género aritmético de su desingularización $\bar{C}$. Para todo módulo coherente $\mathscr{M}$ denotaremos $h^i(C,\mathscr{M}) = \dim_k H^i(C,\mathscr{M})$. Entonces el género geométrico de C es $g = h^1(\bar{C},\mathscr{O}_{\bar{C}})$. .

20. Corolario: *Sea C una curva proyectiva plana, íntegra, de grado n, sobre un cuerpo algebraicamente cerrado. Entonces el género geométrico es*

$$g = \frac{(n-1)\cdot(n-2)}{2} - \sum_{x\in \operatorname{Sing} C} \sum_{y\in A_x} \frac{m_y\cdot(m_y-1)}{2}$$

donde A_x es el árbol de explosión asociado a la desingularización de x y m_y es la multiplicidad en el punto y.

Demostración. Sea $\pi\colon \bar{C} \to C$ el morfismo de desingularización. Consideremos la sucesión exacta

$$0 \to \mathscr{O}_C \to \pi_*\mathscr{O}_{\bar{C}} \to \bigoplus_{x\in \operatorname{Sing} C} \bar{\mathscr{O}}_{C,x}/\mathscr{O}_{C,x} \to 0$$

Como k es algebraicamente cerrado, tenemos que $\Gamma(C,\mathscr{O}_C) = \Gamma(C,\pi_*\mathscr{O}_{\bar{C}}) = \Gamma(\bar{C},\mathscr{O}_{\bar{C}}) = k$, luego

$$g = h^1(\bar{C},\mathscr{O}_{\bar{C}}) = h^1(C,\mathscr{O}_C) - \dim_k \bigoplus_{x\in \operatorname{Sing} C} \bar{\mathscr{O}}_{C,x}/\mathscr{O}_{C,x}.$$

Por 5.6.10, sabemos que $\dim_k \bigoplus_{x\in \operatorname{Sing} C} \bar{\mathscr{O}}_{C,x}/\mathscr{O}_{C,x} = \sum_{x\in \operatorname{Sing} C} \sum_{y\in a_x} \frac{m_y\cdot(m_y-1)}{2}$. Por la proposición anterior, $h^1(C,\mathscr{O}_C) = \frac{(n-1)\cdot(n-2)}{2}$ y concluimos. □

13.7. Cohomología local y extens

Si X es quasi-compacto quasi-separado, los módulos finito generados son una familia de generadores de la categoría de los módulos quasi-coherentes.

1. Proposición : *Sea X un esquema compacto quasi-separado. La categoría de $\mathscr{O}_X$-módulos quasi-coherentes tiene suficientes inyectivos.*

Demostración. Sea F un $\mathscr{O}_X$-módulo. El funtor $\operatorname{Hom}_{\mathscr{O}_X}(-,F)$ sobre la categoría de $\mathscr{O}_X$-módulos quasi-coherentes es exacto por la izquierda, luego es representable por un haz quasi-coherente, que denotamos qF, por tanto,

$$\operatorname{Hom}_{\mathscr{O}_X}(\mathscr{M},qF) = \operatorname{Hom}_{\mathscr{O}_X}(\mathscr{M},F)$$

Si F es inyectivo entonces qF es un módulo inyectivo en la categoría de módulos quasi-coherentes. Ahora ya, dado un módulo quasi-coherente $\mathscr{M}$, existe un $\mathscr{O}_X$-módulo inyectivo, I, y un morfismo inyectivo $\mathscr{M} \to I$, que factoriza a través de qI. Tenemos pues un morfismo inyectivo $\mathscr{M} \to qI$. Ahora ya es fácil concluir que la categoría de $\mathscr{O}_X$-módulos quasi-coherentes tiene suficientes inyectivos.

□

2. Proposición: *Sea X un esquema noetheriano o compacto semiseparado, $\mathscr{C}_{\mathscr{O}_X-mod}$ la categoría de $\mathscr{O}_X$-módulos y $\mathscr{C}_{\mathscr{O}_X-qcoh}$ la categoría de los $\mathscr{O}_X$-módulos quasi-coherentes. Consideremos el funtor*

$$q : \mathscr{C}_{\mathscr{O}_X-mod} \rightsquigarrow \mathscr{C}_{\mathscr{O}_X-qcoh},\ F \mapsto qF.$$

Se cumple que los $\mathscr{O}_X$-módulos quasi-coherentes son q-acíclicos. Por tanto,

$$\mathrm{Ext}^i_{\mathscr{O}_X-mod}(\mathscr{M},\mathscr{N}) = \mathrm{Ext}^i_{\mathscr{O}_X-qcoh}(\mathscr{M},\mathscr{N}),$$

para todo i y todo módulo quasi-coherente $\mathscr{M}$ y $\mathscr{N}$.

Demostración. 1. Sea $i : U \hookrightarrow X$ un abierto afín y F un $\mathscr{O}_U$-módulo. Veamos que $qi_*F = i_*\widetilde{F(U)}$:

$$\begin{aligned}\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M}, qi_*F) &= \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M}, i_*F) = \mathrm{Hom}_{\mathscr{O}_U}(\mathscr{M}_{|U}, F) = \mathrm{Hom}_{\mathscr{O}_U}(\mathscr{M}_{|U}, \widetilde{F(U)})\\ &= \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{M}, i_*\widetilde{F(U)}).\end{aligned}$$

2. Sea $\mathscr{U} = \{U_i\}$ un recubrimiento por abiertos afines (saturado en el caso noetheriano). Sea $\mathscr{N} \to I^{\cdot}$ una resolución de $\mathscr{N}$ por $\mathscr{O}_X$-módulos inyectivos, entonces $\check{C}_{\mathscr{U}}I^{\cdot}$ también es una resolución por inyectivos de $\mathscr{N}$. Veamos que $q\check{C}_{\mathscr{U}}I^{\cdot} \to \check{C}_{\mathscr{U}}I^{\cdot}$ es un quasi-isomorfismo. Basta ver que $qI^{\cdot}_{U_i} \to I^{\cdot}_{U_i}$ es quasi-isomorfismo, para todo i. En efecto,

$$H^n\Gamma(V, qI^{\cdot}_{U_i}) \overset{1.}{=} H^n\Gamma(V \cap U_i, \widetilde{I^{\cdot}(U_i)}) \overset{*}{=} H^n(V \cap U_i, \mathscr{N}) = H^n\Gamma(V, I^{\cdot}_{U_i}),$$

para todo abierto afín V (* si X es semiseparado entonces $V \cap U_i$ es afín, si X es noetheriano $\widetilde{I^{\cdot}(U_i)}$ es una resolución flasca de $\mathscr{N}_{|U_i}$).

3. $R^n q_*\mathscr{N} = H^n q\check{C}_{\mathscr{U}}I^{\cdot} = H^n\check{C}_{\mathscr{U}}I^{\cdot} = 0$, para $n > 0$.

□

3. Teorema: *Sea X un esquema noetheriano, $Y \hookrightarrow X$ un subesquema cerrado y $\mathscr{M}$ un $\mathscr{O}_X$-módulo quasi-coherente. Se cumple que*

$$\varinjlim_n \mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}_Y^n, \mathscr{M}) = H^i_Y(X, \mathscr{M})$$

Demostración. Sea $I^{\cdot}$ una resolución de $\mathscr{M}$ por haces quasi-coherentes inyectivos, entonces

$$\begin{aligned}\varinjlim_n \mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}_Y^n, \mathscr{M}) &= \varinjlim_n H^i[\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}_Y^n, I^{\cdot})] = H^i[\varinjlim_n \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}_Y^n, I^{\cdot})]\\ &= H^i[\Gamma_Y(X, I^{\cdot})] = H^i_Y(X, \mathscr{M}).\end{aligned}$$

□

13.8. Teorema de las funciones formales. Teoremas de Stein y Zariski

El objetivo de esta sección es probar que la cohomología de los haces coherentes conmuta con compleciones. Para ello probaremos que la compleción de la resolución de Godement de un haz coherente es una resolución por haces flascos del completado del haz coherente, y que la toma de secciones del complejo de Godement conmuta con la compleción.

1. Definición: Dado un esquema X, un haz de ideales quasi-coherente $\mathfrak{p} \subset \mathscr{O}_X$ y un $\mathscr{O}_X$-módulo $\mathscr{M}$ definimos la compleción $\mathfrak{p}$-ádica de $\mathscr{M}$, que denotaremos por $\widehat{\mathscr{M}}$, por

$$\widehat{\mathscr{M}} := \varprojlim_n \mathscr{M}/\mathfrak{p}^n\mathscr{M}$$

Si $U = \operatorname{Spec} A$ es un abierto afín e $I = \mathfrak{p}(U)$, se tiene un morfismo natural

$$\Gamma(U,\mathscr{M}) \otimes_A A/I^n \to \Gamma(U,\mathscr{M}/\mathfrak{p}^n\mathscr{M}),$$

y por tanto un morfismo

$$\Gamma(U,\mathscr{M})^\wedge \to \Gamma(U,\widehat{\mathscr{M}}),$$

siendo $\Gamma(U,\mathscr{M})^\wedge$ la compleción I-ádica de $\Gamma(U,\mathscr{M})$.

2. Definición: Diremos que $\mathscr{M}$ es $\mathfrak{p}$-afínmente acíclico si para todo abierto afín U y todo número natural $n \geq 0$, $\mathfrak{p}^n\mathscr{M}$ es acíclico en U y $(\mathfrak{p}^n\mathscr{M})(U) = \mathfrak{p}^n(U)\cdot\mathscr{M}(U)$.

Si $\mathscr{M}$ es $\mathfrak{p}$-afínmente acíclico y U afín, $\mathscr{M}/\mathfrak{p}^n\mathscr{M}$ es acíclico en U, $(\mathscr{M}/\mathfrak{p}^n\mathscr{M})(U) = \mathscr{M}(U)/\mathfrak{p}^n(U)\cdot\mathscr{M}(U)$ y

$$\Gamma(U,\mathscr{M})^\wedge \to \Gamma(U,\widehat{\mathscr{M}})$$

es isomorfismo.

Es claro que todo módulo quasi-coherente es $\mathfrak{p}$-afínmente acíclico.

3. Lema: *Sea X un esquema y $\mathfrak{p} \subseteq \mathscr{O}_X$ un ideal finito generado. Para todo $\mathscr{O}_X$-módulo $\mathscr{M}$ se cumple que:*

1. *$\mathfrak{p}\cdot C^0\mathscr{M} = C^0(\mathfrak{p}\mathscr{M})$ y $\mathscr{M} \cap (\mathfrak{p}C^0\mathscr{M}) = \mathfrak{p}\mathscr{M}$. Si denotamos $\mathscr{M}_1 := (C^0\mathscr{M})/\mathscr{M}$ entonces $\mathfrak{p}\mathscr{M}_1 = (\mathfrak{p}\mathscr{M})_1$.*
2. *$C^0\mathscr{M}$ es $\mathfrak{p}$-afínmente acíclico.*
3. *$\widehat{C^0(\mathscr{M})}$ es un haz flasco.*

Supongamos que existen $f_1,\dots,f_r \in \mathfrak{p}(X)$ *que generen en fibras* $\mathfrak{p}$ *y sea* $I=(f_1,\dots,f_r)$. *Entonces*

4 $\widehat{C^0(\mathscr{M})}(X) = C^0\widehat{(\mathscr{M})(X)}$ *(que denota el completado de* $C^0(\mathscr{M})(X)$ *por la topología* I*-ádica).*

Demostración. 1. Podemos suponer que X es afín. Si I es un ideal finito generado de un anillo A y M_i es una familia de A-módulos, entonces $I\cdot\prod M_i = \prod(I\cdot M_i)$. Por tanto, $\mathfrak{p}\cdot C^0\mathscr{M} = C^0(\mathfrak{p}\mathscr{M})$. Además, $\mathscr{M}\cap C^0(\mathfrak{p}\mathscr{M}) = \mathfrak{p}\mathscr{M}$, porque $m\in\mathscr{M}(U)$ cumple que $m\in(\mathfrak{p}\mathscr{M})(U)$ si y sólo si $m_x\in(\mathfrak{p}\mathscr{M})_x = \mathfrak{p}_x\mathscr{M}_x$ para todo $x\in U$. Por tanto, $\mathscr{M}\cap(\mathfrak{p}C^0\mathscr{M}) = \mathfrak{p}\mathscr{M}$. Ahora es fácil concluir.

2. $\mathfrak{p}^nC^0\mathscr{M} = C^0(\mathfrak{p}^n\mathscr{M})$ es acíclico en todo abierto. Para todo abierto U afín,

$$(\mathfrak{p}^nC^0\mathscr{M})(U) = C^0(\mathfrak{p}^n\mathscr{M})(U) = \mathfrak{p}^n(U)C^0\mathscr{M}(U).$$

4. Observemos que $\mathfrak{p}^nC^0(\mathscr{M})(X) = C^0(\mathfrak{p}^n\mathscr{M})(X) = I^nC^0(\mathscr{M})(X)$. Ahora ya,

$$\begin{aligned}\Gamma(X,C^0\mathscr{M})^\wedge &= \varprojlim_n C^0\mathscr{M}(X)/I^nC^0\mathscr{M}(X) = \varprojlim_n C^0\mathscr{M}(X)/\mathfrak{p}^nC^0\mathscr{M}(X)\\ &= \varprojlim_n (C^0\mathscr{M}/\mathfrak{p}^nC^0\mathscr{M})(X) = \Gamma(X,\widehat{C^0\mathscr{M}}).\end{aligned}$$

3. La propiedad de ser flasco es local. Podemos suponer que X es afín. Por el punto 4., se concluye porque $C^0(\mathscr{M})$ es flasco y la compleción I-ádica conserva epiyecciones.

□

4. Proposición: *Sea* X *un esquema y* $\mathfrak{p}\subseteq\mathscr{O}_X$ *un ideal finito generado. Si* $\mathscr{M}$ *es* $\mathscr{O}_X$*-módulo* $\mathfrak{p}$*-afínmente acíclico entonces* $\widehat{\mathscr{M}}$ *es acíclico en todo abierto afín y* $\widehat{C^\cdot\mathscr{M}}$ *es una resolución por haces flascos de* $\widehat{\mathscr{M}}$.

Demostración. $\mathscr{M}_1 = C^0\mathscr{M}/\mathscr{M}$ es $\mathfrak{p}$-afínmente acíclico porque $\mathscr{M}$ y $\mathscr{C}^0\mathscr{M}$ son afínmente acíclicos y las sucesiones $0\to\mathfrak{p}^n\mathscr{M}\to C^0(\mathfrak{p}^n\mathscr{M}) = \mathfrak{p}^nC^0(\mathscr{M})\to\mathfrak{p}^n\mathscr{M}_1\to 0$ son exactas. La sucesión

$$0\to\mathscr{M}/\mathfrak{p}^n\mathscr{M}\to C^0(\mathscr{M}/\mathfrak{p}^n\mathscr{M}) = C^0(\mathscr{M})/\mathfrak{p}^nC^0\mathscr{M}\to\mathscr{M}_1/\mathfrak{p}^n\mathscr{M}_1\to 0$$

es exacta. Además, tomando secciones en un abierto afín $U=\operatorname{Spec}A$, si denotamos $I=\mathfrak{p}(U)$, se obtiene la sucesión exacta

$$0\to\Gamma(U,\mathscr{M})\otimes_A A/I^n\to\Gamma(U,C^0\mathscr{M})\otimes_A A/I^n\to\Gamma(U,\mathscr{M}_1)\otimes_A A/I^n\to 0$$

Tomando límite proyectivo en la sucesión exacta anterior (téngase en cuenta que la compleción I-ádica conserva epiyecciones) se obtiene la sucesión exacta

$$0 \to \Gamma(U, \widehat{\mathscr{M}}) \to \Gamma(U, \widehat{C^0\mathscr{M}}) \to \Gamma(U, \widehat{\mathscr{M}_1}) \to 0$$

Por tanto, $H^1(U, \widehat{\mathscr{M}}) = 0$, luego $H^2(U, \mathscr{M}) = H^1(U, \mathscr{M}_1) = 0$ y vamos obteniendo recurrentemente que $\widehat{\mathscr{M}}$ es acíclico en abiertos afines.

Además, la sucesión $0 \to \widehat{\mathscr{M}} \to \widehat{C^0\mathscr{M}} \to \widehat{\mathscr{M}_1} \to 0$ es exacta. Ahora ya es fácil probar inductivamente que $\widehat{C^\cdot\mathscr{M}}$ es una resolución por haces flascos de $\widehat{\mathscr{M}}$.

□

5. Definición: Sea $\mathfrak{p} \subseteq \mathscr{O}_X$ un ideal quasi-coherente tal que existen $f_1, \dots, f_r \in \mathfrak{p}(X)$ que generen $\mathfrak{p}$ en fibras y sea $I = (f_1, \dots, f_r)$. Diremos que un $\mathscr{O}_X$-módulo $\mathscr{M}$ cumple la propiedad H si para cada p, los morfismos

$$I^n \otimes_A H^p(X, \mathfrak{p}^m\mathscr{M}) \to H^p(X, \mathfrak{p}^{m+n}\mathscr{M})$$

son epiyectivos para todo n y $m >> 0$.

6. Proposición: *Sea $X \to \operatorname{Spec} A$ un morfismo propio entre esquemas localmente noetherianos. Sea $I \subset A$ un ideal y $\mathfrak{p} = I \cdot \mathscr{O}_X$. Si $\mathscr{M}$ es un $\mathscr{O}_X$-módulo coherente entonces cumple H.*

Demostración. Sea $D_I A = \bigoplus_{n=0}^{\infty} I^n$, $X' = X \times_A D_I A$ y $\pi\colon X' \to X$ la proyección natural. Sea $\mathscr{M}' = \bigoplus_{n=0}^{\infty} \mathfrak{p}^n\mathscr{M}$ el $\mathscr{O}_{X'}$-módulo coherente obvio. Entonces, $\pi_*\mathscr{M}' = \bigoplus_{n=0}^{\infty} \mathfrak{p}^n\mathscr{M}$ y

$$H^p(X', \mathscr{M}') = H^p(X, \pi_*\mathscr{M}') = \bigoplus_{n=0}^{\infty} H^p(X, \mathfrak{p}^n\mathscr{M})$$

es un $D_I A$-módulo finito generado. Luego, $\mathscr{M}$ cumple la propiedad H.

□

7. Lema: *Sea $f\colon X \to \operatorname{Spec} A$ un morfismo propio entre esquemas localmente noetherianos. Si $\mathscr{M}$ es un $\mathscr{O}_X$-módulo que cumple la propiedad H, entonces $\mathscr{M}_1 = C^0\mathscr{M}/\mathscr{M}$ cumple la propiedad H.*

Demostración. De las sucesiones exactas $0 \to \mathfrak{p}^n\mathscr{M} \to \mathfrak{p}^n C^0\mathscr{M} \to \mathfrak{p}^n\mathscr{M}_1 \to 0$ se obtiene la sucesión exacta

$$H^0(X, \mathfrak{p}^n C^0\mathscr{M}) \to H^0(X, \mathfrak{p}^n\mathscr{M}) \to H^1(X, \mathfrak{p}^n\mathscr{M}) \to 0$$

e isomorfismos $H^p(X, \mathfrak{p}^n\mathscr{M}_1) = H^{p+1}(X, \mathfrak{p}^n\mathscr{M})$, para $p > 0$. Se concluye por la hipótesis y porque $H^0(X, \mathfrak{p}^n C^0\mathscr{M}) = I^n H^0(X, C^0\mathscr{M})$. □

8. Lema : *Sea A un anillo noetheriano e $I \subseteq A$ un ideal. Si $0 \to M' \to M \to N \to 0$ es una sucesión exacta de A-módulos y N es finito generado, entonces la compleción I-ádica $0 \to \widehat{M'} \to \widehat{M} \to \widehat{N} \to 0$ es una sucesión exacta.*

Demostración. Sólo tenemos que probar que la topología inducida en M', por la topología I-ádica de M, es justamente la topología I-ádica de M'. Sea $N' \subseteq M$ un submódulo finito generado que se epiyecte en N. Obviamente $M = M' + N'$. Por un lado $I^n \cdot M' \subseteq (I^n M) \cap M'$ y por otro

$$\begin{aligned}(I^n M) \cap M' &= (I^n M' + I^n N') \cap M' = I^n M' + (I^n N' \cap M') \\ &= I^n M' + (I^n N' \cap (N' \cap M')) = I^n M' + I^{n-r}(I^r N' \cap (N' \cap M')) \subseteq I^{n-r} M'\end{aligned}$$

donde la última igualdad, se verifica para un cierto r y todo $n \geq r$, por el lema de Artin-Rees. □

9. Teorema de las funciones formales : *Sea $f : X \to Y$ un morfismo propio de esquemas localmente noetherianos y $\mathfrak{p}$ un haz de ideales coherente en Y por el que vamos a completar. Para cada módulo coherente $\mathscr{M}$ sobre X, los morfismos naturales*

$$\widehat{R^i f_* \mathscr{M}} \to R^i f_* (\widehat{\mathscr{M}})$$

son isomorfismos. Si $Y = \operatorname{Spec} A$ se cumple que

$$H^i(X, \mathscr{M})^\wedge = H^i(X, \widehat{\mathscr{M}})$$

Demostración. El teorema es local en Y, luego podemos suponer que $Y = \operatorname{Spec} A$ es afín. Tenemos que probar que $H^i(X, \mathscr{M})^\wedge = H^i(X, \widehat{\mathscr{M}})$. Por 13.8.6, basta probarlo para los $\mathscr{O}_X$-módulos $\mathscr{M}$ $\mathfrak{p}$-afínmente acíclicos que cumplen la propiedad H.

Sea $C^\cdot \mathscr{M}$ la resolución de Godement de $\mathscr{M}$. Tenemos que probar que el morfismo natural

$$H^i(X, \mathscr{M})^\wedge = H^i(\Gamma(X, C^\cdot \mathscr{M}))^\wedge \to H^i(\Gamma(X, C^\cdot \mathscr{M})^\wedge) \underset{13.8.3\ 3.}{=} H^i(\Gamma(X, \widehat{C^\cdot \mathscr{M}})) \underset{13.8.4}{=} H^i(X, \widehat{\mathscr{M}})$$

$$\sum_n a_n \cdot \bar{c}_n \mapsto \overline{\sum_n a_n c_n}$$

(con $a_n \in I^n$ y $\bar{c}_n \in H^i(\Gamma(X, C^\cdot \mathscr{M}))$) es un isomorfismo.

Consideremos la sucesión exacta $0 \to \mathscr{M} \to C^0(\mathscr{M}) \xrightarrow{d} \mathscr{M}_1 \to 0$. Tenemos las sucesiones exactas

$$0 \longrightarrow \mathscr{M}(X) \longrightarrow C^0 \mathscr{M}(X) \longrightarrow \operatorname{Im} d_X \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Im} d_X \longrightarrow \mathscr{M}_1(X) \longrightarrow H^1(X, \mathscr{M}) \longrightarrow 0$$

1. Por el lema 13.8.3 1., la topología I-ádica de $C^0\mathscr{M}(X)$ induce en $\mathscr{M}(X)$ la topología inducida por la filtración $\{H^0(X,\mathfrak{p}^n\mathscr{M})\}$, que coincide con la topología I-ádica porque $\mathscr{M}$ cumple la propiedad H. Luego tenemos la inyección $\widehat{\mathscr{M}(X)} \hookrightarrow \widehat{C^0\mathscr{M}(X)}$, e igualmente $\widehat{\mathscr{M}_1(X)} \hookrightarrow \widehat{C^0\mathscr{M}_1(X)}$. 2. La topología I-ádica de $\mathscr{M}_1(X)$ induce en $\operatorname{Im} d_X$ la topología I-ádica, por el lema 13.8.8. Luego tenemos la inyección $\widehat{\operatorname{Im} d_X} \hookrightarrow \widehat{\mathscr{M}_1(X)}$.

Por tanto, $H^0(X,\mathscr{M})^\wedge = H^0(X,\hat{\mathscr{M}})$ y $H^1(X,\mathscr{M})^\wedge = H^1(X,\hat{\mathscr{M}})$. Ahora por inducción,

$$H^i(X,\mathscr{M})^\wedge = H^{i-1}(X,\mathscr{M}_1)^\wedge = H^{i-1}(X,\hat{\mathscr{M}_1}) = H^i(X,\hat{\mathscr{M}})$$

para $i>1$. □

10. Observación: Sigamos en las hipótesis y notaciones del teorema. Queremos ver que $\varprojlim_n H^i(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M}) = \widehat{H^i(X,\mathscr{M})}$, para todo i. Para $i=0$, $\varprojlim_n H^0(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M}) = H^0(X,\hat{\mathscr{M}}) = \widehat{H^0(X,\mathscr{M})}$. Consideremos las sucesiones exactas

$$0 \to \mathscr{M}/\mathfrak{p}^n\mathscr{M} \to C^0\mathscr{M}/\mathfrak{p}^n C^0\mathscr{M} \xrightarrow{d^n} \mathscr{M}_1/\mathfrak{p}^n\mathscr{M}_1 \to 0$$

Como $\mathscr{M}_1/\mathfrak{p}^n\mathscr{M}_1 \subset C^0\mathscr{M}_1/\mathfrak{p}^n C^0\mathscr{M}_1$, se tiene que $\operatorname{Im} d_X^n = \operatorname{Im} d_X/(\operatorname{Im} d_X \cap I^n \cdot C^0\mathscr{M}_1(X))$. Por tanto, si tomamos límites proyectivos en

$$0 \to \operatorname{Im} d_X^n \to (\mathscr{M}_1/\mathfrak{p}^n\mathscr{M}_1)(X) \to H^1(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M}) \to 0$$

se obtiene la sucesión exacta (porque los morfismos $\operatorname{Im} d_X^{n+1} \to \operatorname{Im} d_X^n$ son epiyectivos)

$$0 \to \widehat{\operatorname{Im} d_X} \to \widehat{\mathscr{M}_1(X)} \to \varprojlim_n H^1(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M}) \to 0$$

Como $0 \to \widehat{\operatorname{Im} d_X} \to \widehat{\mathscr{M}_1(X)} \to \widehat{H^1(X,\mathscr{M})} \to 0$ es exacta, entonces $\varprojlim_n H^1(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M}) = \widehat{H^1(X,\mathscr{M})}$. Ahora por inducción,

$$H^i(X,\mathscr{M})^\wedge = H^{i-1}(X,\mathscr{M}_1)^\wedge = \varprojlim_n H^{i-1}(X,\mathscr{M}_1/\mathfrak{p}^n\mathscr{M}_1) = \varprojlim_n H^i(X,\mathscr{M}/\mathfrak{p}^n\mathscr{M})$$

para $i>1$.

11. Teorema: *Sea $f: X \to Y$ un morfismo propio entre esquemas noetherianos. Sea r el máximo de las dimensiones de las fibras de f. Entonces, $R^i f_*\mathscr{M} = 0$ para todo $i > r$ y para todo módulo coherente $\mathscr{M}$ sobre X.*

Demostración. Sea y un punto de Y. Haciendo el cambio de base plano $\mathrm{Spec}\mathscr{O}_y \to Y$, podemos suponer que $Y = \mathrm{Spec}A$ con A local de punto cerrado y. Completando por el ideal maximal de A, y por el teorema de las funciones formales

$$(R^i f_* \mathscr{M})^\wedge = H^i(X, \widehat{\mathscr{M}}).$$

Como $\widehat{\mathscr{M}}$ está soportado en la fibra de y y ésta es de dimensión menor o igual que r, se deduce que $(R^i f_* \mathscr{M})^\wedge = 0$ para $i > r$. Se concluye el lema de Nakayama, por ser $R^i f_* \mathscr{M}$ un A-módulo finito generado. □

12. Teorema de conexión de Zariski: *Sea $f : X \to Y$ un morfismo propio entre esquemas localmente noetherianos. Se cumple que:*

1. *Si $\mathscr{O}_Y \simeq f_* \mathscr{O}_X$, entonces las fibras de f son conexas.*
2. *Si X es íntegro, Y normal y $f : X \to Y$ birracional, entonces las fibras de f son conexas.*

Demostración. 1. Puede suponerse sin pérdida de generalidad, por cambio de base plano, que $Y = \mathrm{Spec}A$ es afín y que y es un punto cerrado. Completando a lo largo de y y por el teorema de las funciones formales

$$H^0(X, \mathscr{O}_X)^\wedge = H^0(X, \widehat{\mathscr{O}}_X).$$

Si la fibra de y no fuese conexa el soporte de $\widehat{\mathscr{O}}_X$ sería dos cerrados disjuntos y $H^0(X, \widehat{\mathscr{O}}_X)$ sería el producto directo de dos anillos. Ahora bien, $H^0(X, \mathscr{O}_X)^\wedge = H^0(Y, f_* \mathscr{O}_X)^\wedge = \widehat{A}$, que es un anillo local. Contradicción.

2. Basta probar, por el apartado anterior, que $\mathscr{O}_Y = f_* \mathscr{O}_X$. Podemos suponer que $Y = \mathrm{Spec}A$ es afín, siendo A un anillo íntegramente cerrado. Como f es un morfismo propio $f_* \mathscr{O}_X$ es un módulo coherente, luego es el haz de localizaciones de la A-álgebra finita

$$B = (f_* \mathscr{O}_X)(Y) = \mathscr{O}_X(X) = \bigcap_x \mathscr{O}_{X,x} \subseteq \Sigma_X = \Sigma_Y$$

Ahora bien, A es íntegramente cerrado, luego $B = A$ y por tanto $\mathscr{O}_Y = f_* \mathscr{O}_X$. □

13. Teorema de factorización de Stein: *Sea $f : X \to Y$ un morfismo propio de esquemas localmente noetherianos. Se verifica:*

1. *El morfismo f factoriza por*

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ & {\scriptstyle f'} \searrow \quad \nearrow {\scriptstyle g} & \\ & Y' & \end{array}$$

donde f' es un morfismo propio de fibras conexas y g un morfismo finito.

2. *El conjunto X' formado por los puntos de X que están aislados en la fibra de su imagen (por f) es un abierto. Además, $f'(X')$ es un abierto de Y' tal que $f'^{-1}(f'(X')) = X'$ y $X' \simeq f'(X')$.*

Demostración. 1. Sea $Y' = \operatorname{Spec} f_*\mathscr{O}_X$. El morfismo natural $g\colon Y' \to Y$ es finito, porque $f_*\mathscr{O}_X$ es una $\mathscr{O}_Y$-álgebra coherente. Además, f factoriza a través de Y' y el morfismo $f'\colon X \to Y'$ es propio por ser f propio y g separado. Como $f'_*\mathscr{O}_X = \mathscr{O}_{Y'}$, f' tiene fibras conexas por el teorema de conexión de Zariski.

2. Podemos suponer que $Y' = Y$. En estas hipótesis, $f_*\mathscr{O}_X = \mathscr{O}_Y$ y f tiene fibras conexas. Entonces un punto $x \in X$ está aislado en la fibra de su imagen si $x = f^{-1}(f(x))$.

Sea X' el conjunto de los puntos de X que están aislados en la fibra de su imagen. Dado $x \in X'$, probemos que $\mathscr{O}_{X,x} \simeq \mathscr{O}_{Y,f(x)}$: Dado un entorno abierto V de x, sea U un entorno abierto de $f(x)$ incluido en $Y \setminus f(X \setminus V)$. Entonces, $f^{-1}(U) \subseteq V$. Por tanto,

$$\mathscr{O}_{X,x} = \varinjlim_{x \in V} \mathscr{O}_X(V) = \varinjlim_{x \in f^{-1}(U)} \mathscr{O}_X(f^{-1}(U)) = (f_*\mathscr{O}_X)_{f(x)} = \mathscr{O}_{Y,f(x)}.$$

Ahora bien, como $\mathscr{O}_{X,x} \simeq \mathscr{O}_{Y,f(x)}$, existen entornos V_x de x, $U_{f(x)}$ de $f(x)$, de modo que $f\colon V_x \to U_{f(x)}$ es un isomorfismo. Esto muestra que X' es un abierto, que $f(X')$ es un abierto de Y y que $f\colon X' \to f(X')$ es un isomorfismo. □

14. Main Theorem de Zariski: *Un morfismo entre esquemas localmente noetherianos es finito si y sólo si es propio y cuasifinito (esto es, las fibras de cada punto por el morfismo son conjuntos finitos).*

Demostración. La condición necesaria es obvia. La suficiencia es consecuencia del apartado 2. del teorema de factorización de Stein. □

13.9. Transformaciones birracionales entre superficies

María Teresa Sancho

Apliquemos el teorema de conexión de Zariski para probar que todo morfismo birracional entre superficies lisas es composición de transformaciones cuadráticas.

1. Definición: Una transformación racional entre k-esquemas íntegros y separados, $T\colon X \dashrightarrow Y$, es una clase de morfismos de k-esquemas $\varphi_U\colon U \to Y$, donde los U son abiertos de X y donde dos morfismos φ_U, φ_V son equivalentes si coinciden sobre $U \cap V$ (basta con que coincidan sobre el punto genérico, porque coincidirán por la separabilidad de Y, sobre el cierre del punto genérico). Es claro que existe un máximo abierto denso de definición de una transformación racional. Su complementario se llama lugar de puntos fundamentales de la misma.

Si $T\colon X \dashrightarrow Y$, $T'\colon Y \dashrightarrow Z$ son transformaciones racionales y T es dominante (es decir, $\operatorname{Im}\varphi_U$ es densa para algún U), es posible definir la transformación compuesta $T' \circ T\colon X \dashrightarrow Z$ en el modo obvio.

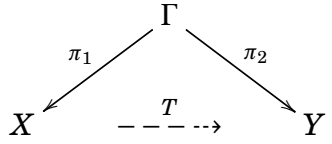
2. Definición: Una transformación birracional es una transformación racional dominante $T\colon X \dashrightarrow Y$ que tiene una transformación racional inversa $S\colon Y \dashrightarrow X$, esto es, tal que $T \circ S$ y $S \circ T$ son las respectivas identidades como transformaciones racionales. Esto equivale claramente a que existe un representante $\varphi_U\colon U \to Y$ de la transformación que establece un isomorfismo de U con un abierto V de Y. Por tanto una transformación racional induce un isomorfismo entre los cuerpos de funciones $\Sigma_Y \xrightarrow{\sim} \Sigma_X$.

Dos esquemas se dicen birracionalmente equivalentes o birracionales si existe una transformación birracional entre ellos.

3. Teorema: *Si X e Y son k-variedades algebraicas íntegras, separadas, existe una correspondencia biunívoca entre isomorfismos $\Sigma_Y \xrightarrow{\sim} \Sigma_X$ (sobre k) y transformaciones birracionales $X \dashrightarrow Y$.*

Demostración. Sea $\Sigma_Y \xrightarrow{\sim} \Sigma_X$ un isomorfismo. Para construir la transformación birracional asociada puede suponerse que $Y = \operatorname{Spec} A$ es afín. Si $A = k[\xi_1, \ldots, \xi_n]$ y $\theta_1, \ldots, \theta_n$ son sus imágenes en Σ_X por el isomorfismo $\Sigma_Y \xrightarrow{\sim} \Sigma_X$, sea $U \subseteq X$ un abierto afín de X donde $\theta_1, \ldots, \theta_n$ son regulares, es decir, $\theta_1, \ldots, \theta_n \in \mathcal{O}_X(U)$. Entonces $\xi_i \mapsto \theta_i$ induce un morfismo $A \to \mathcal{O}_X(U)$, y pasando a espectros un morfismo $\varphi_U\colon U \to Y$ que define la transformación pedida. Se concluye fácilmente. □

Sea $T\colon X \dashrightarrow Y$ una transformación racional, φ_U un representante de T y $U \to U \times Y$ su gráfica, llamaremos *gráfica de la transformación racional* a su cierre Γ en $X \times Y$. Así, una transformación racional se puede representar por una pareja de morfismos



de modo que π_1 es birracional.

Una condición necesaria y suficiente para que una transformación racional entre variedades algebraicas, $T\colon X \dashrightarrow Y$, sea birracional es que las proyecciones de su gráfica, $\pi_1\colon \Gamma \to X$ y $\pi_2\colon \Gamma \to Y$, sean morfismos birracionales.

4. Definición: Dado un punto fundamental $p \in X$, llamaremos transformada total de p, que denotaremos por $T(p)$, a $T(p) := \pi_2(\pi_1^{-1}(p))$.

5. Lema: *Sea $T\colon X - - > Y$ una transformación racional dominante entre variedades íntegras propias. Si X es normal el conjunto de puntos fundamentales es un cerrado de codimensión mayor o igual que 2.*

Demostración. Sea $x \in X$ el punto genérico de una subvariedad irreducible de codimensión 1. El anillo local $\mathcal{O}_{X,x}$ es un anillo de valoración del cuerpo de funciones de X. Por ser Y una variedad propia, el anillo de valoración centra en un punto $y \in Y$. Es decir, tenemos un morfismo dominante $\mathcal{O}_{Y,y} \hookrightarrow \mathcal{O}_{X,x}$. Luego T está definida en un entorno de x. En conclusión el cerrado de puntos fundamentales de T, no puede contener variedades irreducibles de codimensión 1. □

6. Zariski's Main Theorem: *Sea $T\colon X - - > Y$ una transformación birracional entre variedades íntegras propias y supongamos que X es normal. Si $p \in X$ es un punto cerrado fundamental de T, entonces la transformada total $T(p)$ es conexa de dimensión mayor o igual que 1.*

Demostración. Consideremos la gráfica Γ de T y la primera proyección $\pi_1\colon \Gamma \to X$. Por el teorema de conexión de Zariski, las fibras de π_1 son conexas. Si $\pi_1^{-1}(p)$, es de dimensión cero, entonces en un entorno V de p, también. Por tanto, el morfismo $\pi_1^{-1}(V) \to V$, es un morfismo propio de fibras finitas luego es un morfismo finito. Como es birracional y V es normal es isomorfismo. Esto implica que T está definido en V, luego en p. En conclusión, si p es un punto fundamental, $\pi_1^{-1}(p)$ es de dimensión mayor o igual que 1 y $T(p) = \pi_2(\pi_1^{-1}(p))$ es conexo de dimensión mayor que 1. □

Toda transformación birracional, T, entre superficies lisas propias está definida en toda la superficie salvo un número finito de puntos cerrados. Si p es un punto fundamental de T entonces T^{-1} aplica todos los puntos de una curva (salvo un número finito, donde quizás no está definida) en p.

Sea $\mathcal{O}$ un anillo local regular de dimensión de Krull 2. Dado un cerrado irreducible $Y \subset \operatorname{Spec}\mathcal{O}$, definimos la valoración Y-ádica, v_Y, por

$$v_Y(f) = m, \text{ si } f \in \mathfrak{p}_Y^m \text{ y } f \notin \mathfrak{p}_Y^{m+1}$$

con $f \in \mathcal{O}$. Es fácil probar que v_Y es una valoración (la localización de $\mathcal{O}$ en el punto genérico de Y es un anillo local regular).

7. Lema: *Sea $\mathcal{O}$ un anillo local regular de punto cerrado x y H un cerrado irreducible de* Spec$\mathcal{O}$. *Si v_x es la valoración x-ádica, v_H la valoración H-ádica y v una valoración (discreta) centrada en x, entonces $v_H \leq v_x \leq v$ en $\mathcal{O}$.*

Demostración. Para la primera desigualdad basta tener en cuenta que $\mathfrak{p}_H \subset \mathfrak{m}_x$. Para la segunda desigualdad basta tener en cuenta que $\mathfrak{m}_x \subseteq \mathfrak{p}_v$. □

8. Proposición: *Si $f: X \to Y$ es un morfismo birracional entre superficies lisas completas e y es un punto (cerrado) fundamental de f^{-1}, entonces la valoración y-ádica centra en X en una curva de $f^{-1}(y)$ y por tanto coincide con la valoración ádica de esta curva.*

Demostración. Sea $x \in X$ el punto donde centra v_y, $\mathcal{O}_{X,x}$,$\mathcal{O}_{Y,y}$ los anillos de gérmenes en x e y respectivamente y C una curva de $f^{-1}(y)$ que pasa por x. El lema nos dice que $v_C \leq v_x \leq v_y$ en $O_{X,x}$. Por otra parte, $v_y \leq v_C$ en $\mathcal{O}_{Y,y}$, porque si consideramos la inclusión $\mathcal{O}_{Y,y} \subset \mathcal{O}_{X,x}$, tenemos que $\mathfrak{p}_y \cdot \mathcal{O}_{X,x} \subset \mathfrak{p}_C \mathcal{O}_{X,x}$. Se concluye que $v_C = v_y = v_x$. □

9. Proposición: *Sea $f: X \to Y$ un morfismo birracional entre superficies lisas completas, e y un punto fundamental de f^{-1}. Entonces f factoriza a través de la explosión de Y en y.*

Demostración. Sea $\pi: \tilde{Y} \to Y$ la explosión de Y en y y $\pi^{-1}(y) = E$ la fibra excepcional. Sea $\mathcal{O}_{\tilde{Y},E}$ el anillo de gérmenes de $\mathcal{O}_{\tilde{Y}}$ en el punto genérico de E. Tenemos que $\mathcal{O}_{\tilde{Y},E} = \mathcal{O}_{v_y} = \mathcal{O}_{X,C_i}$, para alguna curva irreducible $C_i \subset f^{-1}(y)$. Por tanto, la transformación birracional $T = \pi^{-1} \circ f: X - - > \tilde{Y}$ está definida (y es isomorfismo) en un entorno de los puntos genéricos de C_i y E. Por tanto, los puntos de E (salvo un número finito) se aplican por T^{-1} a lo largo de C_i y la transformación T^{-1} no aplica curvas a puntos. Luego T es un morfismo birracional. □

10. Teorema: *Sea $f: X \to Y$ un morfismo birracional entre superficies lisas completas. Sea $n(f)$ el número de curvas irreducibles de X que se proyectan en algún punto. Entonces $n(f)$ es finito y f es composición de $n(f)$ transformaciones cuadráticas.*

Demostración. La transformación birracional f^{-1}, sólo tiene un número finito de puntos fundamentales, que coinciden con los puntos $y \in Y$ tales que $f^{-1}(y)$ sea de dimensión 1 (y conexa), es decir, unión de curvas irreducibles, que son precisamente las curvas que se proyectan a punto. Sea pues $n = n(f)$. Si $n = 0$, entonces f^{-1} es un morfismo birracional, porque no tiene puntos fundamentales. Luego f es un isomorfismo. Supongamos $n > 0$. Sea $y \in Y$, tal que $f^{-1}(y)$ sea unión de curvas irreducibles. Por la proposición anterior f factoriza a través de la explosión $\pi: \tilde{Y} \to Y$ de Y en y.

Sea $f_1 \colon X \to \tilde{Y}$, tal que $\pi \circ f_1 = f$. Una de las curvas de $f^{-1}(y)$ se proyecta en la fibra excepcional de π. Por tanto, f_1 proyecta a punto menos curvas que f, por inducción sobre n, f_1 factoriza a través de un número finito de explosiones. Luego f también es composición de explosiones (que deberán ser n). □

11. Proposición: *Sea $\mathcal{O}$ un anillo local regular de ideal máximo $\mathfrak{m}_x$, $\mathcal{O}_v$ un anillo de valoración discreta de ideal máximo $\mathfrak{p}_v$ y $\mathcal{O} \subset \mathcal{O}_v$ un morfismo birracional dominante. Si $\mathcal{O}/\mathfrak{p}_v$ es de grado de transcendencia 1 sobre $\mathcal{O}/\mathfrak{m}_x$, entonces la cadena $\mathcal{O}_0 = \mathcal{O} \subset \mathcal{O}_1 \subset \cdots \subset \mathcal{O}_i \subset \ldots \subset \mathcal{O}_v$, obtenida explotando sucesivamente en los puntos donde centra v y tomando sus anillos locales, finitiza.*

Demostración. Observemos que los morfismos de explosión son morfismos proyectivos. Las fibras excepcionales son variedades proyectivas y $\mathcal{O}_v$ centrará en un punto, que sólo puede ser o el punto genérico de una curva o un punto cerrado de las fibras de x, ya que su cuerpo residual es una $\mathcal{O}/\mathfrak{m}_x$-subextensión de $\mathcal{O}_v/\mathfrak{p}_v$, cuyo grado de trascendencia es 1. En el caso que centre en una curva $\mathcal{O}_i$ será anillo de valoración y coincidirá con $\mathcal{O}_v$.

Sea $f \in \mathcal{O}_v$ tal que modulo $\mathfrak{p}_v$ es transcendente sobre $\mathcal{O}/\mathfrak{m}_x$. Si pruebo que $f \in \mathcal{O}_i$ para algún i he terminado. En efecto, si $\mathcal{O}_i$ no es el anillo local en el punto genérico de una curva, entonces el morfismo $\mathcal{O}/\mathfrak{m}_x \hookrightarrow \mathcal{O}_i/\mathfrak{m}_i$ es finito. Por tanto, $f \in \mathcal{O}_i/\mathfrak{m}_i$ no es transcendente y llegamos a contradicción. Veamos que $f \in \mathcal{O}_i$. Escribamos $f = \frac{a}{b}$ donde $a, b \in \mathcal{O}$. Como $v(f) = 0$, se tiene que $v(a) = v(b)$. Dado un ideal I, llamamos $v(I) = \min\{v(g)\}_{g \in I}$. Sea $I := (a, b)$, entonces $v(I) = v(a) = v(b)$. Veamos por inducción sobre $n = v(I)$ que existe un i de modo que $\frac{a}{b} \in \mathcal{O}_i$. Si $v(I) = 0$, entonces $v(a) = v(b) = 0$, luego a y b son invertibles de $\mathcal{O}$. Por tanto, $\frac{a}{b} \in \mathcal{O}$. Suponemos que es cierto para todo a, b tal que $v(I) < n$ y supongamos que $v(I) = n$. Tenemos que $\mathfrak{m} \cdot \mathcal{O}_1 = (t)$, $a = t \cdot a'$ y $b = t \cdot b'$ y $\frac{a}{b} = \frac{a'}{b'}$. Como $v(I) = v(t) + v((a', b')) > v((a', b'))$, se concluye por hipótesis de inducción aplicada a (a', b').

□

12. Definición: Diremos que la tranformación birracional inversa de una transformación cuadrática es una contracción.

13. Teorema: *Toda transformación birracional entre superficies lisas completas es composición de un número finito de transformaciones cuadráticas y de contracciones.*

Demostración. Sea $T \colon X - - > Y$ la transformación birracional. Sea $\{v_i\}$ el conjunto de valoraciones que centran en las curvas de X que se proyectan por T (donde esté definida) en punto. Explotamos en Y sucesivamente en puntos cerrados en los que centren

las v_i, hasta que todas las v_i centren en curvas (lo cual sucede por la proposición anterior). Sea $Z \to Y$ la composición de esta sucesión de explosiones. La transformación birracional $X - - > Z$ no proyecta curvas en puntos. Por tanto, la transformación birracional $Z \to X$ es un verdadero morfismo birracional. Por el teorema de factorización 13.9.10, aplicado a este último morfismo hemos concluido.

□

13.10. Teoremas de Grauert y semicontinuidad

Sea $f : X \to Y$ un morfismo de esquemas y $\mathscr{M}$ un haz coherente en X. Para cada $y \in Y$, denotaremos

$$X_y := f^{-1}(y), \qquad \mathscr{M}(y) := i^*\mathscr{M} = \mathscr{M} \otimes_{\mathscr{O}_{Y,y}} k(y)$$

siendo $i : f^{-1}(y) \hookrightarrow X$ la inmersión natural y $k(y)$ el cuerpo residual de y. Se tiene un morfismo natural

$$R^i f_* \mathscr{M} \otimes_{\mathscr{O}_{Y,y}} k(y) \to H^i(X_y, \mathscr{M}(y))$$

Nuestro objetivo será estudiar este morfismo, es decir, ver la relación que hay entre las fibras de las imágenes directas superiores y la cohomología de las fibras. Además, si los grupos de cohomología $H^i(X_y, \mathscr{M}(y))$ son de dimensión finita, queremos estudiar como varía su dimensión en función del punto y. Los teoremas de Grauert y de semicontinuidad mostrarán que ambas cuestiones están muy relacionadas.

1. Complejo finito de Mumford : *Sea A un anillo noetheriano y*

$$C^\cdot = C^0 \to C^1 \to \cdots \to C^n$$

un complejo finito de A-módulos cuyos grupos de cohomología $H^i(C^\cdot)$ son A-módulos finito generados. Existe un complejo de A-módulos finito generados

$$K^\cdot = K^0 \to L^1 \to \cdots \to L^n$$

con L^j libres, y un cuasi-isomorfismo $K^\cdot \to C^\cdot$. Si además los C^i son A-módulos planos, entonces K^0 también es plano.

Demostración. Supongamos construido un complejo

$$K^\cdot = K^0 \to \cdots \to K^i \to L^{i+1} \to \cdots \to L^n$$

con L^j libres finito generados y K^j planos (si los C^i son planos) y un cuasi-isomorfismo $K^\cdot \to C^\cdot$. Consideremos la sucesión exacta

$$K^{i-1} \xrightarrow{d_{i-1}} K^i \to \operatorname{Coker} d_{i-1} \to 0$$

Dado que $H^i(K^\cdot)$ y L^{i+1} son finito generados, concluimos que $\operatorname{Coker} d_{i-1}$ es finito generado. Sea L^i un libre finito y $\bar{\phi}\colon L^i \to \operatorname{Coker} d_{i-1}$ un epimorfismo. Sea $\phi\colon L^i \to K^i$ un levantamiento de $\bar{\phi}$. Sea $\widetilde{K}^{i-1} := K^{i-1} \times_{K^i} L^i$. El núcleo del morfismo $\widetilde{K}^{i-1} \to L^i$, $(k,l) \mapsto l$ es $\operatorname{Ker} d_{i-1} \times \{0\}$. Tenemos el diagrama conmutativo de filas exactas

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Ker} d_{i-1} & \longrightarrow & K^{i-1} & \longrightarrow & K^i & \longrightarrow & \operatorname{Coker} d_{i-1} \longrightarrow 0 \\
 & & \| & & \uparrow & & \uparrow & & \| \\
0 & \longrightarrow & \operatorname{Ker} d_{i-1} & \longrightarrow & \widetilde{K}^{i-1} & \longrightarrow & L^i & \longrightarrow & \operatorname{Coker} d_{i-1} \longrightarrow 0
\end{array}$$

Tenemos el complejo

$$\widetilde{K}^\cdot = K^0 \to \cdots \to K^{i-2} \to \widetilde{K}^{i-1} \to L^i \to L^{i+1} \to \cdots \to L^n$$

y un morfismo obvio $\widetilde{K}^\cdot \to K^\cdot$ de complejos, que es cuasi-isomorfismo.

Si los K^j son planos, entonces $\widetilde{K}^{i-1}$ también lo es: Observemos que $\operatorname{Ker} \tilde{d}_{i-1} = \operatorname{Ker} d_{i-1}$, por tanto el morfismo $\bigoplus_{j \geq i-1} \tilde{K}^j \to \bigoplus_{j \geq i-1} K^j$ es un cuasisomorfismo. El cono de este morfismo es un complejo acíclico finito, es decir, es una sucesión exacta larga finita. El primer término es $\tilde{K}^{i-1}$ y los demás son planos. Se concluye que $\tilde{K}^{i-1}$ también es plano. □

2. Notación: Dado un punto x de un esquema X denotamos $k(x) := \mathcal{O}_{X,x}/\mathfrak{p}_x$ el cuerpo residual de x.

3. Corolario: *En las hipótesis y notaciones del teorema, y suponiendo que los C^j son módulos planos, se verifica:*

1. *Para todo morfismo de anillos $A \to B$, $K^\cdot \otimes_A B \to C^\cdot \otimes_A B$ es cuasi-isomorfismo.*
2. *Para todo punto $x \in \operatorname{Spec} A$, la cohomología del complejo $C^\cdot \otimes_A k(x)$ es de dimensión finita y la característica*

$$\chi(C^\cdot \otimes_A k(x)) := \sum (-1)^i \dim_{k(x)} H^i(C^\cdot \otimes_A k(x))$$

es una función $\operatorname{Spec} A \to \mathbb{Z}$ localmente constante.

3. *Para cada entero n el conjunto de los puntos $x \in \operatorname{Spec} A$ tales que*

$$\dim_{k(x)} H^i(C^\cdot \otimes_A k(x)) > n$$

es un cerrado de $\operatorname{Spec} A$. *En otras palabras, la función $x \mapsto \dim_{k(x)} H^i(C^\cdot \otimes_A k(x))$ es superiormente semicontinua. En particular, si x es especialización de x', entonces*

$$\dim_{k(x)} H^i(C^\cdot \otimes_A k(x)) \geq \dim_{k(x')} H^i(C^\cdot \otimes_A k(x'))$$

4. *Supongamos que A es reducido. Si la función $x \mapsto \dim_{k(x)} H^i(C^\cdot \otimes_A k(x))$ es constante entonces $H^i(C^\cdot)$ es un módulo localmente libre de rango constante y para todo morfismo de anillos $A \to B$ se tiene que*

$$H^i(C^\cdot) \otimes_A B = H^i(C^\cdot \otimes_A B)$$
$$H^{i-1}(C^\cdot) \otimes_A B = H^{i-1}(C^\cdot \otimes_A B)$$

Demostración. 1. Sea $f : K^\cdot \to C^\cdot$ el cuasi-isomorfismo. Entonces el cono de f es acíclico. Como está formado por módulos planos, $\operatorname{Cono}(f) \otimes_A B$ también es acíclico. Pero $\operatorname{Cono}(f) \otimes_A B$ es el cono de $K^\cdot \otimes_A B \to C^\cdot \otimes_A B$, luego este es un cuasi-isomorfismo.

2. La finitud se deduce del cuasi-isomorfismo $K^\cdot \otimes_A k(x) \to C^\cdot \otimes_A k(x)$ y de ser los K^i finito generados. Además, si $d_i : K^i \to K^{i+1}$ es la diferencial y $d_i(x)$ la inducida al tensar por $k(x)$, entonces

$$\begin{aligned}\dim_{k(x)} H^i(C^\cdot \otimes_A k(x)) = \dim_{k(x)} H^i(K^\cdot \otimes_A k(x)) = \dim_{k(x)} \operatorname{Ker} d_i(x) - \dim_{k(x)} \operatorname{Im} d_{i-1}(x) = \\ = \text{ rango } (K^i) - \dim_{k(x)} \operatorname{Im} d_i(x) - \dim_{k(x)} \operatorname{Im} d_{i-1}(x)\end{aligned}$$

y tomando sumas alternadas, $\chi(C^\cdot \otimes_A k(x)) = \sum (-1)^i \text{ rango } (K^i)$ que no depende del punto x.

3. De la igualdad

$$\begin{aligned}\dim_{k(x)} H^i(C^\cdot \otimes_A k(x)) = & \text{ rango } (K^i) - \dim_{k(x)} \operatorname{Im} d_i(x) - \dim_{k(x)} \operatorname{Im} d_{i-1}(x) \\ & = \dim_{k(x)} \operatorname{Coker} d_{i-1}(x) + \dim_{k(x)} \operatorname{Coker} d_i(x) - \text{ rango } K^{i+1}\end{aligned}$$

se concluye, porque la función $\dim_{k(x)} \operatorname{Coker} d(x) = \dim_{k(x)}(\operatorname{Coker} d \otimes_A k(x))$ es superiormente semicontinua por 0.10.10.

4. Si $x \mapsto \dim_{k(x)} H^i(K^\cdot \otimes_A k(x))$ es una función constante, entonces también lo son $\operatorname{Coker} d_i(x)$ y $\operatorname{Coker} d_{i-1}(x)$. Por 0.9.9, $\operatorname{Coker} d_i$ y $\operatorname{Coker} d_{i-1}$ son módulos localmente libres de rango constante. De las sucesiones exactas

$$0 \to \operatorname{Im} d_i \to K^{i+1} \to \operatorname{Coker} d_i \to 0$$
$$0 \to \operatorname{Ker} d_i \to K^i \to \operatorname{Im} d_i \to 0$$

se deduce que $\operatorname{Im} d_i$ y $\operatorname{Ker} d_i$ son módulos localmente libres de rango constante (análogamente para d_{i-1}) y que

$$(\operatorname{Im} d_i) \otimes_A B = \operatorname{Im}(d_i \otimes 1) \text{ y } (\operatorname{Ker} d_i) \otimes_A B = \operatorname{Ker}(d_i \otimes 1)$$

(análogamente para d_{i-1}). Por tanto, $H^i(K^\cdot \otimes_A B) = H^i(K^\cdot) \otimes_A B$ (análogamente para H^{i-1}) y como $H^i(K^\cdot) \otimes_A k(x) = H^i(K^\cdot \otimes_A k(x))$ es de dimensión constante, $H^i(K^\cdot)$ es localmente libre de rango constante. □

4. Notación: Dado un morfismo de esquemas $f: X \to Y$ y un punto $y \in Y$ denotamos $X_y := X \times_Y \operatorname{Spec} k(y) = f^{-1}(y)$.

5. Teorema (de Grauert-Grothendieck + semicontinuidad): *Sea $f: X \to Y$ un morfismo propio entre esquemas noetherianos y $\mathscr{M}$ un $\mathscr{O}_X$-módulo coherente, plano sobre Y. Entonces:*

1. *La característica de Euler-Poincaré de las fibras:*

$$y \mapsto \sum_{i \geq 0} (-1)^i \dim_{k(y)} H^i(X_y, \mathscr{M}(y))$$

es una función localmente constante de Y en los números enteros.

2. *Semicontinuidad: Para cada entero $n \in \mathbb{Z}$ y cada $i \geq 0$, el conjunto de los puntos $y \in Y$ tales que*

$$\dim_{k(y)} H^i(X_y, \mathscr{M}(y)) > n$$

es un cerrado. Es decir, la función $Y \to \mathbb{Z}$, $y \mapsto \dim_{k(y)} H^i(X_y, \mathscr{M}(y))$, es superiormente semicontinua. En particular, si y es especialización de y' (es decir, $y \in \overline{\{y'\}}$), entonces

$$\dim_{k(y)} H^i(X_y, \mathscr{M}(y)) \geq \dim_{k(y')} H^i(X_{y'}, \mathscr{M}(y'))$$

3. *Teorema de Grauert-Grothendieck. Supongamos que Y es reducido. Dado $i \geq 0$, si la función*

$$y \mapsto \dim_{k(y)} H^i(X_y, \mathscr{M}(y))$$

es constante, entonces la imagen directa superior i-ésima $R^i f_* \mathscr{M}$ es localmente libre de rango constante y para todo morfismo $g: \bar{Y} \to Y$ se tiene que

$$g^* R^i f_* \mathscr{M} = R^i \bar{f}_* (\bar{g}^* \mathscr{M})$$
$$g^* R^{i-1} f_* \mathscr{M} = R^{i-1} \bar{f}_* (\bar{g}^* \mathscr{M}),$$

donde $\bar{f}: X \times_Y \bar{Y} \to \bar{Y}$ y $\bar{g}: X \times_Y \bar{Y} \to X$ son los morfismos naturales.

Demostración. Todo es local en Y (y en $\bar{Y}$), luego podemos suponer $Y = \operatorname{Spec} A$ (y $\bar{Y} = \operatorname{Spec} B$). Sea $\mathscr{U}$ un recubrimiento afín de X y $C^\cdot = \check{C}(\mathscr{U}, \mathscr{M})$ el complejo de cocadenas de Cech asociado al mismo. Es un complejo finito de A-módulos planos. $\bar{\mathscr{U}} = \mathscr{U} \times_Y \bar{Y}$ es un recubrimiento por abiertos afines de $\bar{g}^*\mathscr{M}$ y el complejo de cocadenas de Cech asociado al mismo es $C^\cdot \otimes_A B$. Por tanto,

$$H^i(C^\cdot) = H^i(X, \mathscr{M})$$
$$H^i(C^\cdot \otimes_A B) = H^i(X \times_Y \bar{Y}, \bar{g}^*\mathscr{M})$$

Se concluye por el corolario anterior. □

13.11. Lema de Nakayama para funtores semiexactos

Fernando Sancho

Sea $f : X \to \operatorname{Spec} A$ un morfismo propio y $\mathscr{M}$ un $\mathscr{O}_X$ módulo coherente plano sobre A. Vamos a continuar el estudio de la relación entre las fibras de las imágenes directas superiores $R^i f_*(\mathscr{M})$ y la cohomología de las fibras $H^i(X_y, \mathscr{M}(y))$, es decir, el estudio del morfismo

$$R^i f_*(\mathscr{M}) \otimes_A k(y) \to H^i(X_y, \mathscr{M}(y))$$

Vamos a considerar el siguiente punto de vista: Para cada A-módulo N sea

$$F^i(N) = R^i f_*(\mathscr{M} \otimes f^*\tilde{N})$$

F^i es un funtor semiexacto (concepto que más adelante definiremos). Cuando N es el cuerpo residual de un punto $y \in \operatorname{Spec} A$, obtenemos $F(k(y)) = H^i(X_y, \mathscr{M}(y))$, y cuando tomamos $N = A$ obtenemos $F(A) = R^i f_*(\mathscr{M})$. Tenemos un morfismo natural

$$F^i(A) \otimes_A N \to F^i(N)$$

y queremos saber cuando es isomorfismo al tomar $N = k(y)$. La primera pregunta será saber cuándo es isomorfismo para todo N, es decir, cuándo el morfismo de funtores

$$F^i(A) \otimes (-) \to F^i$$

es isomorfismo. Esto nos lleva a caracterizar cuándo un funtor semiexacto consiste en tensar por un módulo. Veremos que esto se verifica exactamente cuando el funtor es exacto por la derecha, y veremos que si A es local de maximal $\mathfrak{m}$, la exactitud por la

derecha equivale a que el morfismo $F^i(A) \to F^i(A/\mathfrak{m})$ sea epiyectivo. Esto se deducirá de que el funtor es nulo si y sólo si se anula sobre el cuerpo residual de A. Este será el lema de Nakayama para funtores semiexactos. También aplicaremos este lema a los morfismos de Cohen-Macaulay y Gorenstein.

1. Definición: Un funtor $F\colon \mathscr{C} \to \mathscr{C}'$ covariante entre categorías abelianas se dice semiexacto si para toda sucesión exacta en $\mathscr{C}$

$$0 \to M_1 \xrightarrow{i} M_2 \xrightarrow{\pi} M_3 \to 0$$

la sucesión

$$F(M_1) \xrightarrow{F(i)} F(M_2) \xrightarrow{F(\pi)} F(M_3)$$

es exacta (i.e. $\operatorname{Im} F(i) = \operatorname{Ker} F(\pi)$).

2. Ejercicio: Prueba que si F es un funtor semiexacto entonces

$$F(M_1 \oplus M_2) = F(M_1) \oplus F(M_2).$$

3. Lema de Nakayama para funtores semiexactos: *Sea $A \to B$ un morfismo dominante entre anillos locales noetherianos y sea $\mathfrak{m}$ el ideal maximal de A. Sea F un funtor semiexacto de la categoría de A-módulos finito generados en la categoría de B-módulos finito generados, tal que para cualesquiera A-módulos finito generados M y N la aplicación natural*

$$\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_B(F(M),F(N))$$

sea un morfismo de A-módulos. Entonces,

$$F = 0 \Leftrightarrow F(A/\mathfrak{m}) = 0.$$

Demostración. Supongamos $F(A/\mathfrak{m}) = 0$. Si M es un A-módulo finito generado, por 3.2.21 existe una filtración

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

tal que $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, siendo $\mathfrak{p}_i$ un ideal primo de A.

Por tanto, por ser F semiexacto, si $F(A/\mathfrak{p}) = 0$ para todo primo $\mathfrak{p}$, entonces $F(M) = 0$ para todo M. Veamos que $F(A/\mathfrak{p}) = 0$ por inducción sobre la dimensión de $A/\mathfrak{p}$. Si la dimensión es cero, entonces $\mathfrak{p} = \mathfrak{m}$ y es la hipótesis. Si $\dim A/\mathfrak{p} = n > 0$, entonces $\mathfrak{p} \subsetneq \mathfrak{m}$ y tomemos $a \in \mathfrak{m}\setminus\mathfrak{p}$. Se tiene la sucesión exacta

$$0 \to A/\mathfrak{p} \xrightarrow{\cdot a} A/\mathfrak{p} \to A/\mathfrak{p} + (a) \to 0$$

luego $F(A/\mathfrak{p}) \xrightarrow{\cdot a} F(A/\mathfrak{p}) \to F(A/\mathfrak{p}+(a))$ es exacta. Por inducción, $F(A/\mathfrak{q}) = 0$ para todo ideal primo $\mathfrak{q} \supseteq \mathfrak{p}+(a)$, luego de nuevo tendremos que $F(A/\mathfrak{p}+(a)) = 0$. Por lo tanto, $a \cdot F(A/\mathfrak{p}) = F(A/\mathfrak{p})$ y por el lema de Nakayama, $F(A/\mathfrak{p}) = 0$.

□

4. Teorema : *En las hipótesis del lema de Nakayama, las siguientes condiciones son equivalentes:*

1. *F es isomorfo al funtor $F(A) \otimes -$, vía el morfismo natural, $F(A) \otimes_A M \to F(M)$, que se deduce del morfismo*

$$M = \mathrm{Hom}_A(A, M) \to \mathrm{Hom}_B(F(A), F(M)).$$

2. *$F(A) \to F(A/\mathfrak{m})$ es epiyectivo.*

3. *F es exacto por la derecha.*

Demostración. 1. $\Rightarrow$ 2. Es inmediato.

2. $\Rightarrow$ 3. Sea H el funtor semiexacto definido por $H(M) := F(M)/(F(A) \otimes_A M)$. Por hipótesis $H(A/\mathfrak{m}) = 0$, luego $H = 0$ por el lema de Nakayama. Entonces, el morfismo $F(A) \otimes_A M \to F(M)$ es epiyectivo y F es exacto por la derecha.

3. $\Rightarrow$ 1. Por ser M finito generado, existen módulos libres de rango finito, L_1, L_2, tales que $L_1 \to L_2 \to M \to 0$. Por ser F semiexacto $F(L_i) = F(A) \otimes_A L_i$ y por ser F exacto por la derecha la sucesión $F(A) \otimes_A L_1 \to F(A) \otimes_A L_2 \to F(M) \to 0$ es exacta, luego $F(M) = F(A) \otimes_A M$. □

5. Observación : Las implicaciones 1. $\Rightarrow$ 2. y 3. $\Rightarrow$ 1. no requieren la hipótesis de ser A local.

Sean $\{F^i\}_{i \in \mathbb{Z}}$ funtores en las hipótesis del lema de Nakayama, tales que para cada sucesión exacta de A-módulos

$$0 \to M' \to M \to M'' \to 0$$

se tiene la sucesión exacta (funtorial)

$$\cdots \to F^{i-1}(M'') \to F^i(M') \to F^i(M) \to F^i(M') \to \cdots$$

6. Teorema : *Si para cierto índice i se cumple que $F^i(A/\mathfrak{m}) = 0$, entonces $F^{i-1} = F^{i-1}(A) \otimes_A -$.*

Demostración. Por el lema de Nakayama $F^i = 0$. Por tanto, F^{i-1} es exacto por la derecha. Por 13.11.4 concluimos. □

7. Teorema: *Supongamos que $F^i(A) \to F^i(A/\mathfrak{m})$ es epiyectivo. La condición necesaria y suficiente para que $F^{i-1}(A) \to F^{i-1}(A/\mathfrak{m})$ sea epiyectivo es que $F^i(A)$ sea un A-módulo plano.*

Demostración. $\Rightarrow$) Si $F^{i-1}(A) \to F^{i-1}(A/\mathfrak{m})$ es epiyectivo, entonces F^{i-1} es exacto por la derecha, luego F^i es exacto por la izquierda. En conclusión, F^i es exacto, luego $F^i(M) = F^i(A) \otimes_A M$ y $F^i(A)$ es un A-módulo plano.

$\Leftarrow$) Como $F^i(A) \to F^i(A/\mathfrak{m})$ es epiyectivo, F^i es exacto por la derecha y $F^i(M) = F^i(A) \otimes_A M$. Como $F^i(A)$ es plano, F^i es exacto. En conclusión, F^{i-1} es exacto por la derecha y por 13.11.4, $F^{i-1}(A) \to F^{i-1}(A/\mathfrak{m})$ es epiyectivo. □

8. Corolario: *Supongamos que $F^n(A/\mathfrak{m}) = 0$. La condición necesaria y suficiente para que $F^i = F^i(A) \otimes_A -$, para todo $m \leq i \leq n$, es que $F^i(A)$ sea un A-módulo plano, para todo $m < i \leq n$. En particular, $F^i = 0$, para todo $m \leq i \leq n$, si y sólo si $F^i(A) = 0$, para todo $m \leq i \leq n$.*

Demostración. Por el lema de Nakayama para funtores semiexactos $F^n = 0$. Por el teorema 13.11.6, $F^{n-1} = F^{n-1}(A) \otimes_A -$, es decir, $F^{n-1}(A) \to F^{n-1}(A/\mathfrak{m})$ es epiyectivo. Por el teorema 13.11.7, $F^{n-2} = F^{n-2}(A) \otimes_A -$ si y sólo si $F^{n-1}(A)$ es un A-módulo plano. Supuesto que estas dos condiciones equivalentes se cumplen, entonces $F^{n-3} = F^{n-3}(A) \otimes_A -$ si y sólo si $F^{n-2}(A)$ es un A-módulo plano. Etc.

□

13.11.1. Aplicación 1: Fibras de las imágenes directas superiores

Hipótesis $(*)$**:** Supondremos que $f : X \to Y$ es un morfismo propio entre esquemas localmente noetherianos y $\mathscr{M}$ un $\mathscr{O}_X$-módulo coherente plano sobre Y.

Consideremos el funtor semiexacto F^i de la categoría de $\mathscr{O}_Y$-módulos coherentes en sí misma

$$F^i(\mathscr{N}) := R^i f_*(\mathscr{M} \otimes_{\mathscr{O}_X} f^*\mathscr{N})$$

Dado $y \in Y$ observemos que $F^i(k(y)) = H^i(X_y, \mathscr{M}(y))$: Consideremos el diagrama conmutativo de morfismos obvios

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ {\scriptstyle i_y}\uparrow & & \uparrow{\scriptstyle i} \\ X_y & \xrightarrow[f_y]{} & y = \operatorname{Spec} k(y) \end{array}$$

donde i e i_y son afines. Entonces,

$$\begin{aligned} F^i(k(y)) &= R^i f_*(\mathscr{M} \otimes_{\mathscr{O}_X} f^* k(y)) = R^i f_*(i_{y*}\mathscr{M}(y)) = R^i(f \circ i_y)_* \mathscr{M}(y) = R^i(i \circ f_y)_* \mathscr{M}(y) \\ &= i_* R^i f_{y*} \mathscr{M}(y) = H^i(X_y, \mathscr{M}(y)). \end{aligned}$$

Se tiene un morfismo natural $F^i(\mathscr{O}_Y) \otimes \mathscr{N} \to F^i(\mathscr{N})$, esto es,

$$(R^i f_* \mathscr{M}) \otimes \mathscr{N} \to R^i f_*(\mathscr{M} \otimes f^* \mathscr{N})$$

9. Teorema de Grauert: *En las hipótesis* $(*)$*, para cada punto* $y \in Y$ *se cumple:*

a) Si el morfismo natural $R^i f_* \mathscr{M} \otimes k(y) \to H^i(X_y, \mathscr{M}(y))$ *es epiyectivo, entonces es isomorfismo y* $(R^i f_* \mathscr{M}) \otimes \mathscr{N}_y = R^i f_*(\mathscr{M} \otimes f^* \mathscr{N})_y$.

b) Si se verifica a)*, entonces* $R^{i-1} f_* \mathscr{M} \otimes k(y) \to H^{i-1}(X_y, \mathscr{M}(y))$ *es epiyectivo si y sólo si* $R^i f_* \mathscr{M}$ *es localmente libre en un entorno de* y.

Demostración. Como el problema es local puede suponerse $Y = \operatorname{Spec} A$, y haciendo el cambio de base plano, $\operatorname{Spec} A_y \to \operatorname{Spec} A$, puede suponerse que A es local de punto cerrado y. Concluimos por 13.11.4 y 13.11.7. □

En particular, tenemos el siguiente teorema.

10. Teorema: *En las hipótesis* $(*)$*, si para cierto índice* i *y para cierto punto* $y \in Y$ *es* $H^i(X_y, \mathscr{M}(y)) = 0$*, entonces el morfismo natural* $R^{i-1} f_* \mathscr{M} \otimes k(y) \to H^{i-1}(X_y, \mathscr{M}(y))$ *es isomorfismo y* $(R^{i-1} f_* \mathscr{M}) \otimes \mathscr{N}_y = R^{i-1} f_*(\mathscr{M} \otimes f^* \mathscr{N})_y$.

De la acotación cohomológica y de 13.11.8 obtenemos:

11. Corolario: *En las hipótesis* $(*)$*,* $R^i f_* \mathscr{M}$ *es localmente libre en* y*, para todo* $i > i_0$ *si y sólo si* $(R^i f_* \mathscr{M}) \otimes k(y) = H^i(X_y, \mathscr{M}(y))$*, para todo* $i \geq i_0$*.* $(R^i f_* \mathscr{M})_y = 0$*, para todo* $i \geq i_0$*, si y sólo si* $H^i(X_y, \mathscr{M}(y)) = 0$*, para todo* $i \geq i_0$.

12. Teorema: *En las hipótesis de* $(*)$ *y sea* n *el máximo de las dimensiones de las fibras de* f*. Para todo morfismo de esquemas* $g\colon \bar{Y} \to Y$*, se verifica que*

$$g^* R^n f_* \mathscr{M} = R^n \bar{f}_* (\bar{g}^* \mathscr{M})$$

donde $\bar{f}\colon X \times_Y \bar{Y} \to \bar{Y}$ *y* $\bar{g}\colon X \times_Y \bar{Y} \to X$ *son los morfismos naturales.*

Demostración. El teorema es local en $\bar{Y}$, luego podemos suponer que $\bar{Y} = \operatorname{Spec} \bar{A}$ e $Y = \operatorname{Spec} A$, de modo que A es un anillo local de ideal maximal $\mathfrak{m}_y$. Por 13.11.10, $H^n(X, \mathscr{M}) \otimes_A k(y) = H^n(X_y, \mathscr{M}(y))$ y

$$H^n(X, \mathscr{M}) \otimes_A \bar{A} = H^n(X, \mathscr{M} \otimes_{\mathscr{O}_X} f^* \tilde{\bar{A}}).$$

Ahora bien, $H^n(X, \mathscr{M} \otimes_{\mathscr{O}_X} f^* \tilde{\bar{A}}) = H^n(X \times_Y \bar{Y}, \bar{g}^* \mathscr{M})$, porque $\bar{g}$ es un morfismo afín y $\bar{g}_* \bar{g}^* \mathscr{M} = \mathscr{M} \otimes_{\mathscr{O}_X} f^* \tilde{\bar{A}}$. En conclusión,

$$H^n(X, \mathscr{M}) \otimes_A \bar{A} = H^n(X \times_Y \bar{Y}, \bar{g}^* \mathscr{M}).$$

□

13.11.2. Aplicación 2: Morfismos de Cohen-Macaulay y Gorenstein

13. Notación: Supondremos que S es un esquema localmente noetheriano.

14. Definición: Diremos que un morfismo de esquemas $f\colon X \to S$ es de Cohen-Macaulay (resp. Gorenstein) si es plano, de tipo finito y sus fibras son variedades de Cohen-Macaulay (resp. Gorenstein).

Sea X un esquema, $\mathscr{M}$ un módulo coherente y $\mathscr{N}$ un módulo quasi-coherente. Denotaremos por $\underline{\operatorname{Ext}}^i_{\mathscr{O}_X}(\mathscr{M}, \mathscr{N})$ al haz quasi-coherente asociado al prehaz

$$U \rightsquigarrow \operatorname{Ext}^i_{\mathscr{O}_X(U)}(\mathscr{M}(U), \mathscr{N}(U))$$

Sea ahora $f\colon X \to S$ un morfismo de esquemas de tipo finito, plano. Sea $s\colon S \to X$ una inmersión cerrada, sección de f. Consideremos el funtor semiexacto de la categoría de $\mathscr{O}_S$-módulos coherentes en sí misma

$$F^i(\mathscr{M}) = \underline{\operatorname{Ext}}^i_{\mathscr{O}_X}(\mathscr{O}_S, f^* \mathscr{M}).$$

15. Notación: Diremos que un morfismo de esquemas $f\colon X \to S$ es de fibras variedades de dimensión n si para todo punto $y \in S$, $X_y = X \times_S y$ es unión de variedades algebraicas de dimensión n.

16. Teorema : *Sea $f: X \to S$ un morfismo de Gorenstein con sección y supongamos X conexo. Entonces, $\underline{\mathrm{Ext}}^i_{\mathscr{O}_X}(\mathscr{O}_S, \mathscr{O}_X) = 0$ para $i \neq n$, $\underline{\mathrm{Ext}}^n_{\mathscr{O}_X}(\mathscr{O}_S, \mathscr{O}_X)$ es un $\mathscr{O}_S$-módulo de línea, y f es de fibras variedades de dimensión n.*

Demostración. El teorema es local en X, luego podemos suponer que $X = \mathrm{Spec} B$ de punto cerrado x, y $S = \mathrm{Spec} A$ de punto cerrado $s = f(x)$.

Si $P_\cdot \to A$ es una resolución de A por B-módulos libres, entonces $P_\cdot \otimes_A A/\mathfrak{m}_s$ es una resolución de $A/\mathfrak{m}_s$ por $B/\mathfrak{m}_s B$-módulos libres. Por tanto,

$$\mathrm{Ext}^i_B(A, B/\mathfrak{m}_s B) = \mathrm{Ext}^i_{B/\mathfrak{m}_s B}(A/\mathfrak{m}_s, B/\mathfrak{m}_s B).$$

Como f es un morfismo de Gorenstein, $F^i(A/\mathfrak{m}_s) = 0$ para $i \neq n$; por el lema de Nakayama para funtores semiexactos, $F^i = 0$ y $F^i(A) = \mathrm{Ext}^i_B(A, B) = 0$ para $i \neq n$. Además, por 13.11.7, $F^n(A) = \mathrm{Ext}^n_B(A, B)$ es un A-módulo libre. Por último, $\mathrm{Ext}^n_B(A, B)$ es de rango 1 porque

$$\mathrm{Ext}^n_B(A, B) \otimes_A A/\mathfrak{m}_s \overset{13.11.4}{=} \mathrm{Ext}^n_B(A, B/\mathfrak{m}_s B) = \mathrm{Ext}^n_{B/\mathfrak{m}_s}(A/\mathfrak{m}_s, B/\mathfrak{m}_s B) = A/\mathfrak{m}_s.$$

□

Desgraciadamente, los morfismos de Cohen-Macaulay no cumplen una propiedad equivalente. Si $A = k[z]/(z^2)$ y $B = A[x, y]/(x^2, y^2, xy - zx)$, entonces B es una A-álgebra finita y plana, luego $A \hookrightarrow B$ es un morfismo de Cohen-Macaulay. Además, $A = B/(x, y)$. Ahora bien,

$$\mathrm{Hom}_B(A, B) = \{b \in B : xb = yb = 0\} = zxA \oplus zyA$$

que no es un A-módulo plano.

17. Proposición: *Sea $W \to S$ un morfismo de Gorenstein y X un subesquema cerrado conexo de W, plano sobre S. Entonces, $X \to S$ es un morfismo de Cohen-Macaulay (respectivamente, Gorenstein) $\iff$ $\underline{\mathrm{Ext}}^i_{\mathscr{O}_W}(\mathscr{O}_X, \mathscr{O}_W) = 0$ para todo $i \neq d$ y $\underline{\mathrm{Ext}}^d_{\mathscr{O}_W}(\mathscr{O}_X, \mathscr{O}_W)$ es un $\mathscr{O}_S$-módulo plano (respectivamente, un $\mathscr{O}_X$-módulo de línea), donde $d = \dim \mathscr{O}_{W,x} - \dim \mathscr{O}_{X,x}$, para todo $x \in X$.*

Demostración. Es un problema local en X y S, podemos suponer $S = \mathrm{Spec} A$, $W = \mathrm{Spec} B$ y $X = \mathrm{Spec} C$, con B local de ideal maximal $\mathfrak{m}_x$ y A local de ideal maximal $\mathfrak{m}_s := \mathfrak{m}_x \cap A$. Consideremos los funtores semiexactos de la categoría de A-módulos finito generados en la de los C-módulos finito generados:

$$F^i(M) = \mathrm{Ext}^i_B(C, B \otimes_A M).$$

Obviamente, $F^i(A) = \mathrm{Ext}^i_B(C,B)$. Si $P_\cdot \to C$ es una resolución de C por B-módulos libres, entonces $P_\cdot \otimes_A A/\mathfrak{m}_s$ es una resolución de $C \otimes_A A/\mathfrak{m}_s$, pues toda sucesión exacta superiormente acotada de A-módulos planos permanece exacta al tensar por $\otimes_A A/\mathfrak{m}_s$. Por tanto,

$$F^i(A/\mathfrak{m}_s) = \mathrm{Ext}^i_B(C,B/\mathfrak{m}_s B) = \mathrm{Ext}^i_{B/\mathfrak{m}_s B}(C/\mathfrak{m}_s C, B/\mathfrak{m}_s B).$$

Observemos que por ser $W \to S$ un morfismo de Gorenstein, $F^i(A/\mathfrak{m}_s) = 0$, para todo $i > \dim B/\mathfrak{m}_s B$, pues los anillos de Gorenstein son de dimensión inyectiva igual a su dimensión de Krull.

$\Leftarrow$) Por 13.11.8, $\underline{\mathrm{Ext}}^i_{\mathscr{O}_{W_s}}(\mathscr{O}_{X_s},\mathscr{O}_{W_s}) = \underline{\mathrm{Ext}}^i_{\mathscr{O}_W}(\mathscr{O}_X,\mathscr{O}_W) \otimes_{\mathscr{O}_S} k(s)$, para todo i. Luego,

$$\underline{\mathrm{Ext}}^i_{\mathscr{O}_{W_s}}(\mathscr{O}_{X_s},\mathscr{O}_{W_s}) = 0, \text{ para } i \neq d$$

(por 7.6.29, X_s es de Cohen-Macaulay) y $\underline{\mathrm{Ext}}^d_{\mathscr{O}_{W_s}}(\mathscr{O}_{X_s},\mathscr{O}_{W_s}) \simeq \mathscr{O}_{X_s}$ si $\underline{\mathrm{Ext}}^d_{\mathscr{O}_W}(\mathscr{O}_X,\mathscr{O}_W)$ es de línea (luego X_s es de Gorenstein).

$\Rightarrow$) Por Nakayama, $F^i(A) = 0$ para $i \neq d$. Por tanto, F^d es exacto, luego $F^d(A)$ es plano sobre A. Si además $X \to S$ es Gorenstein, de la igualdad $F^d(A) \otimes_A A/\mathfrak{m}_s = F^d(A/\mathfrak{m}_s) = C/\mathfrak{m}_s C$ se concluye que $F^d(A) \simeq C$. □

13.12. Haces de línea amplios y muy amplios

1. Teorema: *Sea X un variedad completa y $\mathscr{L}$ un haz de línea en X. Entonces, $\mathscr{L}$ es muy amplio si y sólo si para cada par de puntos cerrados $x,x' \in X$ (distintos o no) se verifica que el morfismo natural $\Gamma(X,\mathscr{L}) \to \mathscr{L}/\mathfrak{m}_x\mathfrak{m}_{x'}\mathscr{L}$ es epiyectivo, es decir, "la serie lineal completa no tiene puntos base, separa puntos y separa puntos infinitesimalmente próximos".*

Demostración. Sea $\langle s_0,\dots,s_n\rangle = \Gamma(X,\mathscr{L})$ la "serie lineal completa" y supongamos que no tiene puntos base. El morfismo

$$i : X \to \mathbb{P}^n,\ x \mapsto (s_0(x),\dots,s_n(x))$$

inducido es una inmersión cerrada si y sólo si $\mathscr{L}$ es un haz de línea muy amplio.

Si $\mathscr{L}$ no tiene puntos base y separa puntos y separa puntos entonces las fibras de i son finitas y por el Main Theorem de Zariski 13.8.14 i es un morfismo finito. Localmente el morfismo i viene dado por

$$\begin{array}{ccccc} k[x_0/x_i,\dots,x_n/x_i] & \longrightarrow & k[s_0/s_i,\dots,s_n/s_i] & \overset{i^*}{\hookrightarrow} & \mathscr{O}_X(U_i) \\ x_j/x_i & \longmapsto & s_j/s_i & \longmapsto & s_j/s_i. \end{array}$$

Tenemos que probar que las inclusiones $i^*: B = k[s_0/s_i, \dots, s_n/s_i] \hookrightarrow \mathscr{O}_X(U_i)$ son isomorfismos si y sólo si $\mathscr{L}$ no tiene puntos base, separa puntos y separa puntos infinitesimalmente próximos.

El morfismo finito $B \overset{i^*}{\hookrightarrow} \mathscr{O}_X(U_i)$ es un isomorfismo si y sólo si para todo ideal maximal $\mathfrak{m}_y$ de B, el morfismo $B/\mathfrak{m}_y \to \mathscr{O}_X(U_i)/\mathfrak{m}_y\mathscr{O}_X(U_i)$ es un epimorfismo. Es decir, si y sólo si $\mathfrak{m}_y\mathscr{O}_X(U_i)$ está contenido en un único ideal maximal, digamos $\mathfrak{m}_x$ (donde $\mathfrak{m}_x \cap B = \mathfrak{m}_y$) y $B \to \mathscr{O}_X/\mathfrak{m}_x^2$ es epiyectivo. Es decir, las secciones globales de $\mathscr{L}$ que se anulan en x no se anulan, todas a la vez, en otro punto y separan los puntos infinitesimalmente próximos a x. □

2. Definición: Sea X una variedad propia. Diremos que un haz de línea $\mathscr{L}$ en X es amplio si existe un $n > 0$ de modo que $\mathscr{L}^n := \mathscr{L} \otimes_{\mathscr{O}_X} \overset{n}{\cdots} \otimes_{\mathscr{O}_X} \mathscr{L}$ es muy amplio.

El teorema de finitud Serre caracteriza los haces de línea amplios:

3. Proposición: *Sea X una variedad propia y $\mathscr{L}$ un haz de línea en X. $\mathscr{L}$ es un haz de línea amplio si y sólo si para cada módulo coherente $\mathscr{M}$ existe un $m \in \mathbb{N}$ de modo que $\mathscr{M} \otimes \mathscr{L}^n$ es acíclico para $n \geq m$.*

Demostración. Si $\mathscr{L}$ es amplio existe un $n > 0$ de modo que $\mathscr{L}^n$ es muy amplio. Por tanto, X es una variedad proyectiva y podemos decir que $\mathscr{L}^n = \mathscr{O}_X(1)$. Existe un n_0 de modo que $\mathscr{M}, \mathscr{M} \otimes \mathscr{L}, \dots, \mathscr{M} \otimes \mathscr{L}^{n-1}$ verifican el apartado 2. del teorema de finitud de Serre 13.6.8. El número m buscado es $n \cdot n_0$.

Veamos el recíproco. Sea x un punto cerrado y U un entorno afín de x de modo que $\mathscr{L}_{|U} \simeq \mathscr{O}_U$. Sea $C = X \setminus U$ y $\mathfrak{p}_C$ el haz de ideales de las funciones de X que se anulan en C. Existe un $n > 0$ tal que $\mathfrak{m}_x \cdot \mathfrak{p}_C \cdot \mathscr{L}^n$ es acíclico. De la sucesión exacta

$$0 \to \mathfrak{m}_x \cdot \mathfrak{p}_C \cdot \mathscr{L}^n \to \mathfrak{p}_C \cdot \mathscr{L}^n \to \mathfrak{p}_C \cdot \mathscr{L}^n/\mathfrak{m}_x \cdot \mathfrak{p}_C \cdot \mathscr{L}^n \to 0$$

se deduce que existe una sección global de $\mathfrak{p}_C \cdot \mathscr{L}^n$ que no se anula en x, es decir, una sección $s \in \Gamma(X, \mathscr{L}^n)$ que se anula en C y no en x. Por tanto, $V = X \setminus (s)_0 = U \setminus (s)_0$ es un abierto afín que contiene a x. Sustituyendo $\mathscr{L}$ por $\mathscr{L}^n$ podemos suponer que $n = 1$. Si consideramos el sistema inductivo $\mathscr{L} \overset{\cdot s}{\to} \mathscr{L}^2 \overset{\cdot s}{\to} \mathscr{L}^3 \to \cdots$ tenemos que

$$\varinjlim_n \mathscr{L}^n = i_* \mathscr{L}_{|V} = i_* \mathscr{O}_V,$$

donde i es la inmersión abierta $V \hookrightarrow X$. Por tanto, existe un $n_x >> 0$ y secciones globales de $\mathscr{L}^{n_x}$ cuya imagen por el isomorfismo $\mathscr{L}^{n_x}(V) \overset{\cdot s^{-n_x}}{=} \mathscr{O}_X(V)$ forman un sistema generador del álgebra $\mathscr{O}_X(V)$. Luego, el morfismo definido sobre V por las secciones globales de $\mathscr{L}^{n_x}$ es una inmersión cerrada. Considerando un recubrimiento finito de

abiertos afines $\{V_i\}$ de X, con n_i de modo que las secciones globales de $\mathscr{L}^{n_i}$ definan sobre V_i una inmersión cerrada (y alguna sección global se anule exactamente en $X \setminus V_i$), tendremos que para $n = \prod n_i$, $\mathscr{L}^n$ es un haz de línea muy amplio.

□

4. Proposición: *Sea $\pi: X \to Y$ un morfismo finito entre variedades propias. Si $\mathscr{L}$ un haz de línea amplio en Y, entonces $\pi^*\mathscr{L}$ es un haz de línea amplio.*

Demostración. Dado un haz coherente $\mathscr{M}$ en X, observemos que $\pi_*(\mathscr{M} \otimes_{\mathscr{O}_X} \pi^*\mathscr{L}^n) = \pi_*\mathscr{M} \otimes_{\mathscr{O}_Y} \mathscr{L}^n$. Sea $m > 0$, tal que $\pi_*\mathscr{M} \otimes_{\mathscr{O}_Y} \mathscr{L}^n$ es acíclico para todo $n \geq m$. $\mathscr{M} \otimes_{\mathscr{O}_X} \pi^*\mathscr{L}^n$ es acíclico para todo $n \geq m$, porque π es un morfismo afín y

$$H^i(X, \mathscr{M} \otimes_{\mathscr{O}_X} \pi^*\mathscr{L}^n) = H^i(Y, \pi_*(\mathscr{M} \otimes_{\mathscr{O}_X} \pi^*\mathscr{L}^n)) = H^i(Y, \pi_*\mathscr{M} \otimes_{\mathscr{O}_Y} \mathscr{L}^n).$$

Luego, $\pi^*\mathscr{L}$ es un haz de línea amplio.

□

El recíproco también es cierto, pero probemos sólo la siguiente proposición.

5. Proposición: *Sea X una variedad propia y $\{X_i\}$ sus componentes irreducibles. Un haz de línea $\mathscr{L}$ en X es amplio si y sólo si $\mathscr{L}_{|X_{i,red}}$ es amplio en $X_{i,red}$, para todo i.*

Demostración. Tenemos que probar que si $\mathscr{L}_{|X_{i,red}}$ es amplio en $X_{i,red}$, para todo i, entonces $\mathscr{L}$ es amplio. Tenemos que probar que para todo módulo coherente $\mathscr{M}$, para todo $n >> 0$, $\mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{L}^n$ es acíclico. Procedemos por inducción noetheriana sobre el soporte, $(\text{Anul}(\mathscr{M}))_0$, de $\mathscr{M}$. Restringiéndonos a $(\text{Anul}(\mathscr{M}))_0$, podemos suponer que $X = (\text{Anul}(\mathscr{M}))_0$, es decir, $\text{Anul}(\mathscr{M}) = 0$. Sea $i: X_{i,red} \hookrightarrow X$ la inmersión cerrada obvia. Consideremos el epimorfismo natural $\phi: \mathscr{M} \to i_*i^*\mathscr{M}$. Como $\text{Ker}\phi$ y $i_*i^*\mathscr{M}$ están en las hipótesis de inducción, son acíclicos al tensar por $\mathscr{L}^n$, para todo $n >> 0$, entonces $\mathscr{M}$ también.

□

13.13. Apéndice

13.13.1. Lema de Chow

El propósito de esta sección es probar el lema de Chow, según el cual dada una variedad propia X existe una variedad **proyectiva** X' y un morfismo $X' \to X$ **proyectivo** y **birracional**. Antes de dar el enunciado riguroso en su forma general, vamos a dar una idea de la demostración cuando X es una variedad propia irreducible y está recubierto por dos abiertos afines U_1, U_2.

Como U_1, U_2 son de tipo finito, existen variedades proyectivas P_1, P_2 que los contienen como abiertos. Sea $U = U_1 \cap U_2$ y consideremos el subesquema $U \hookrightarrow P_1 \times P_2$, $x \mapsto (x,x)$. $X' = \bar{U}$ es la variedad que buscamos: Los morfismos $p_1 \colon X' \to P_1$, $p_2 \colon X' \to P_2$ son propios, luego $p_1^{-1}(U_1) \to U_1$ y $p_2^{-1}(U_2) \to U_2$ son propios. Además los morfismos $p_1^{-1}(U_1) \to U_1 \hookrightarrow X$ y $p_2^{-1}(U_2) \to U_2 \hookrightarrow X$ son ambos la identidad sobre U, luego coinciden sobre $p_1^{-1}(U_1) \cap p_2^{-1}(U_2)$. En conclusión, tenemos un morfismo propio y birracional $\pi \colon p_1^{-1}(U_1) \cup p_2^{-1}(U_2) \to X$. Por ser propio, $p_1^{-1}(U_1) \cup p_2^{-1}(U_2)$ es propio y coincide con X'.

Para ver que $\pi \colon X' \to X$ es proyectivo, basta ver que $h \colon X' \to P_1 \times P_2 \times X$, deducido de p_1, p_2, π, es una inmersión cerrada. Ahora bien, h es una inmersión cerrada, porque $X' \to P_1 \times P_2$ lo es.

1. Lema de Chow : *Sea Y un esquema noetheriano, X un esquema irreducible y $f \colon X \to Y$ un morfismo propio. Existe un esquema irreducible X' proyectivo sobre Y y un epimorfismo proyectivo $g \colon X' \to X$ de esquemas sobre Y, tal que existe un abierto no vacío U de X de modo que g induce un isomorfismos entre $g^{-1}(U)$ y U.*

Además, si X es íntegro, X' también lo es y g es birracional.

Demostración. Considerando en vez de Y la imagen esquemática de f, podemos suponer que f es epiyectivo e Y irreducible.

a) Construcción de X'.

Sea $Y = \bigcup_i Y_i$ un recubrimiento finito de Y por abiertos afines Y_i y sean $f^{-1}(Y_i) = \bigcup_j X_{ij}$ recubrimientos de $f^{-1}(Y_i)$ por abiertos afines. Los esquemas X_{ij} son afines y de tipo finito sobre Y_i, luego se tienen diagramas conmutativos:

$$\begin{array}{ccccc} X_{ij} & \longrightarrow & \mathbb{A}^{r_{ij}}_{Y_i} & \longrightarrow & \mathbb{P}^{r_{ij}}_{Y_i} \longrightarrow \mathbb{P}^{r_{ij}}_{Y} \\ & \searrow^{f} & & \searrow & \downarrow \qquad\quad \downarrow \\ & & & & Y_i \longrightarrow Y \end{array}$$

donde las flechas horizontales son inmersiones (cerradas o abiertas).

Denotemos las parejas ij por k. $U = \bigcap_k X_k$, no es vacío por ser X irreducible. Se tiene un morfismo natural

$$U \to P = \prod_k \mathbb{P}^{r_k}_Y$$

Sea X' la imagen esquemática de U en P. X' es un esquema proyectivo sobre Y, y las proyecciones $p_k \colon X' \to \mathbb{P}^{r_k}_Y$ establecen isomorfismos $U = p_k^{-1}(U) \xrightarrow{\sim} U$, porque la inmersión $U \hookrightarrow U \times_Y \prod_{k' \neq k} \mathbb{P}^{r_{k'}}_Y$ es cerrada por ser $\prod_{k' \neq k} \mathbb{P}^{r_{k'}}_Y$ separado sobre Y.

b) Construcción de $g \colon X' \to X$.

Sea $Z = \underset{k}{\cup} p_k^{-1}(X_k) \hookrightarrow X'$. $p_{ij}^{-1}(X_{ij}) = X' \cap (\underset{k \neq ij}{\prod} \mathbb{P}_Y^{r_k} \times \mathbb{A}_{Y_i}^{r_{ij}})$ es un abierto de X'. Los morfismos $p_k^{-1}(X_k) \to X_k$ son propios y las composiciones $p_k^{-1}(X_k) \to X_k \hookrightarrow X$, $p_{k'}^{-1}(X_{k'}) \to X_{k'} \hookrightarrow X$ coinciden sobre las intersecciones porque coinciden sobre el abierto U (y $h \in \mathcal{O}_{X'}(W) = 0$ si $h_{|W \cap U} = 0$). En conclusión, tenemos un morfismo propio $g\colon Z \to X$, tal que $g^{-1}(U) = U$.

Sólo queda ver que $Z \hookrightarrow X'$ es isomorfismo. Puesto que es una inmersión abierta, sólo queda ver que es un cerrado, lo cual se deduce del diagrama

$$\begin{array}{ccc} Z & \xrightarrow{g} & X \\ \downarrow & & \downarrow f \\ X' & \longrightarrow & Y \end{array}$$

en el que tanto f como los morfismos horizontales son propios.

c) $g\colon X' \to X$ es proyectivo.

Basta ver que el morfismo inducido $h\colon X' \to P \times X$ es una inmersión cerrada, que lo es por ser $X' \to P$ una inmersión cerrada.

□

13.13.2. Cohomología de los morfismos propios

Vamos a demostrar el teorema de finitud para un morfismo propio. Este teorema se reduce al teorema de finitud para los morfismos proyectivos mediante el lema de Chow y un artificio técnico conocido como el lema de "dévissage" debido a Grothendieck. La demostración sigue esencialmente la de Grothendieck en E.G.A. III.

2. Lema de "dévissage": *Sea X un esquema noetheriano y $\mathscr{C}'$ una subcategoría plena de la categoría $\mathscr{C}$ de módulos coherentes sobre X (esto es, si $\mathscr{M}, \mathscr{N}$ son objetos de $\mathscr{C}'$, entonces* $\mathrm{Hom}_{\mathscr{C}'}(\mathscr{M}, \mathscr{N}) = \mathrm{Hom}_{\mathscr{C}}(\mathscr{M}, \mathscr{N})$*). Supongamos que se cumple:*

1. *$\mathscr{C}'$ es exacta, en el siguiente sentido: Si $0 \to \mathscr{M}' \to \mathscr{M} \to \mathscr{M}'' \to 0$ es una sucesión exacta de módulos coherentes y dos de ellos están en $\mathscr{C}'$, entonces también lo está el tercero.*

2. *Todo sumando directo de un objeto de $\mathscr{C}'$ está en $\mathscr{C}'$.*

3. *Para cada subesquema cerrado irreducible reducido Y de X, existe un módulo coherente de $\mathscr{C}'$ de soporte Y.*

Entonces $\mathscr{C}' = \mathscr{C}$.

Demostración. Sea $P(Y)$ la siguiente propiedad de los cerrados de X: "Todo módulo coherente cuyo soporte está contenido en Y está en $\mathscr{C}'$". Por el principio de recurrencia noetheriana basta probar que si $P(Z)$ se verifica para todo subesquema cerrado Z de Y diferente de Y, se verifica $P(Y)$.

Sea, pues, $\mathscr{M}$ un módulo coherente cuyo soporte está contenido en Y y $\mathfrak{p}$ el haz de ideales de todas las funciones que se anulan en Y. Se tiene $\mathfrak{p}^n\mathscr{M} = 0$ para n bastante grande. Para $1 \leq k \leq n$ se tiene una sucesión exacta

$$0 \to \mathfrak{p}^{k-1}\mathscr{M}/\mathfrak{p}^k\mathscr{M} \to \mathscr{M}/\mathfrak{p}^k\mathscr{M} \to \mathscr{M}/\mathfrak{p}^{k-1}\mathscr{M} \to 0$$

Como $\mathscr{C}'$ es exacta, basta probar, por inducción sobre k, que los módulos $\mathfrak{p}^{k-1}\mathscr{M}/\mathfrak{p}^k\mathscr{M}$ están en $\mathscr{C}'$. Es decir, puede suponerse $\mathfrak{p}\mathscr{M} = 0$. Distingamos ahora dos casos:

a) Y no es irreducible.

Sea $Y = Y' \cup Y''$ unión de dos subesquemas cerrados (reducidos) distintos de Y, y sean $\mathfrak{p}', \mathfrak{p}''$ los ideales que los definen. Sea $\mathscr{M}' = \mathscr{M} \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{p}'$, $\mathscr{M}'' = \mathscr{M} \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{p}''$. El morfismo natural $\phi\colon \mathscr{M} \to \mathscr{M}' \oplus \mathscr{M}''$ es un isomorfismo en los puntos de $X \setminus (Y' \cap Y'')$ ya que $\mathfrak{p}\mathscr{M} = 0$ (compruébese), luego su núcleo y su conúcleo tienen soporte contenido en $Y' \cap Y''$ y, por la hipótesis, pertenecen a $\mathscr{C}'$. Como $\mathscr{M}'$ tiene soporte en Y' y $\mathscr{M}''$ en Y'', también están en $\mathscr{C}'$. Se concluye ahora por ser $\mathscr{C}'$ exacta a partir de las sucesiones

$$0 \to \operatorname{Im}\phi \to \mathscr{M}' \oplus \mathscr{M}'' \to \operatorname{Coker}\phi \to 0$$
$$0 \to \operatorname{Ker}\phi \to \mathscr{M} \to \operatorname{Im}\phi \to 0$$

b) Y es irreducible y reducido.

Por 3., existe un módulo coherente $\mathscr{G}$ de $\mathscr{C}'$ de soporte Y. Podemos suponer que $\mathfrak{p}\mathscr{G} = 0$. Sea y el punto genérico de Y y $\Sigma := \mathscr{O}_{X,y}/\mathfrak{p}$. nula. $\mathscr{G}_y$ y $\mathscr{M}_y$ son Σ-espacios vectoriales y por tanto existe un isomorfismo de Σ-espacios vectoriales $\mathscr{M}_y^q \simeq \mathscr{G}_y^m$, con $q = \dim_\Sigma \mathscr{G}_y$ y $m = \dim_\Sigma \mathscr{M}_y$.

Como $\mathscr{M}^q$ y $\mathscr{G}^m$ son coherentes, existe un entorno abierto U de y en X y un isomorfismo $\mathscr{M}^q_{|U} \simeq \mathscr{G}^m_{|U}$. Sea $\mathscr{N}' \hookrightarrow \mathscr{M}^q_{|U} \oplus \mathscr{G}^m_{|U}$ la gráfica de dicho isomorfismo. Por el teorema de extensión de módulos coherentes, existe un submódulo coherente $\mathscr{N}$ de $\mathscr{M}^q \oplus \mathscr{G}^m$ que es $\mathscr{N}'$ sobre U y 0 sobre $X - Y$. Los morfismos naturales $\mathscr{N} \to \mathscr{M}^q$, $\mathscr{N} \to \mathscr{G}^m$ son isomorfismos sobre U y sobre $X \setminus Y$, luego sus núcleos y conúcleos tienen soportes contenidos en $Y \setminus (Y \cap U)$ y por tanto, pertenecen a $\mathscr{C}'$. Por otra parte, $\mathscr{G}^m$ pertenece a $\mathscr{C}'$ por pertenecer $\mathscr{G}$ y ser $\mathscr{C}'$ exacta. Se concluye sucesivamente, por la exactitud de $\mathscr{C}'$, que $\mathscr{N}$ está en $\mathscr{C}'$ y que $\mathscr{M}^q$ está en $\mathscr{C}'$. Por 2. se termina. □

3. Observación: Si no imponemos 2., el lema sigue siendo válido si en 3. añadimos que la fibra del módulo en el punto genérico y de Y es isomorfo a $\mathscr{O}_{Y,y}$.

4. Teorema (de finitud): *Sea Y un esquema localmente noetheriano y $f: X \to Y$ un morfismo propio. Para todo $\mathcal{O}_X$-módulo coherente $\mathcal{M}$, las imágenes directas superiores $R^i f_* \mathcal{M}$ son haces coherentes.*

Demostración. La cuestión es local en Y, luego puede suponerse Y noetheriano (y por tanto X). Considérese ahora la categoría $\mathscr{C}'$ de módulos coherentes sobre X cuyos objetos son los módulos cuyas imágenes directas superiores son módulos coherentes. Se sigue fácilmente de la sucesión exacta de cohomología y de la noetherianidad de Y que $\mathscr{C}'$ es exacta. Además todo sumando directo de un objeto de $\mathscr{C}'$ esté en $\mathscr{C}'$ ya que las imágenes directas superiores transforman sumas directas en sumas directas. Para concluir, basta probar que $\mathscr{C}'$ satisface la hipótesis 3. del lema de "dévissage". Dicha condición se reduce fácilmente a probar que si X es irreducible, existe un haz $\mathcal{M}$ en $\mathscr{C}'$ cuya fibra en el punto genérico x de X no es nula.

Por el lema de Chow, existe un esquema irreducible X' y un epimorfismo proyectivo $g: X' \to X$ tal que $f \circ g: X' \to Y$ es proyectivo. Si consideramos el haz $\mathcal{O}'(1)$ del morfismo $g: X' \to X$, por el teorema de finitud para los morfismos proyectivos existe un entero n tal que: a) $R^i g_* \mathcal{O}'(n) = 0$ para $i > 0$ y b) $g^* g_* \mathcal{O}'(n) \to \mathcal{O}'(n)$ es epiyectivo. El haz $\mathcal{M} = g_* \mathcal{O}'(n)$ es coherente (por ser g proyectivo) y su fibra en el punto genérico x de X no es nula por b). Para ver que $\mathcal{M}$ está en $\mathscr{C}'$ basta observar que $R^j f_*(\mathcal{M}) \simeq R^j (f \circ g)_* \mathcal{O}'(n)$ (porque $R^i g_* \mathcal{O}'(n) = 0$ para $i > 0$) con lo que $R^j f_* \mathcal{M}$ es coherente, pues $\mathcal{O}'(n)$ lo es y $f \circ g$ es un morfismo proyectivo. □

13.14. Problemas

1. Sabiendo que los módulos quasi-coherentes inyectivos son flascos (en esquemas localmente noetheriano, 12.1.28), prueba que los módulos quasi-coherentes sobre un esquema afín son acíclicos.

2. Sea C la curva del plano proyectivo real de ecuación afín $x^2 + y^2 = 0$. Demuestra:

   a) El cierre entero de $\mathbb{R}$ en Σ_C es $\mathbb{C}$.

   b) $\Gamma(C, \mathcal{O}_C) = \mathbb{R}$.

   c) La desingularización de C es isomorfa a la recta proyectiva compleja.

   d) El origen es un punto racional de C y $\dim_k H^1(C, \mathcal{O}_C) = 0$.

3. Sea X un esquema quasi-compacto semiseparado y $\mathcal{M}$ un $\mathcal{O}_X$-módulo quasi-coherente. Si $\mathcal{M}$ es inyectivo prueba que es acíclico.

   Resolución: Sea $i: U \hookrightarrow X$ un abierto afín. Observemos que $\mathcal{M}_U = i_* \mathcal{M}_{|U}$ es acíclico, porque $R^n i_* \mathcal{M}_{|U} = 0$ luego $H^n(X, \mathcal{M}_U) = H^n(U, \mathcal{M}_{|U}) = 0$ para todo $n > 0$.

Sea $\{U_i\}$ un recubrimiento finito de X por abiertos afines. El morfismo natural $\mathscr{M} \to \oplus_i \mathscr{M}_{|U_i}$ es inyectivo. Por tanto, $\mathscr{M}$ es acíclico porque es un sumando directo de $\oplus_i \mathscr{M}_{|U_i}$ que es acíclico.

4. Sea X un esquema noetheriano separado y $U \hookrightarrow X$ un abierto afín. Dado un haz F en X, denotemos F_U el haz definido por $F_U(V) := F(U \cap V)$. Prueba que si $\mathscr{M}$ es un haz $\mathfrak{p}$-afínmente acíclico en X entonces $\widetilde{(\mathscr{M}_U)} = (\widehat{\mathscr{M}})_U$ y es acíclico.

5. Sean $\pi_i : X_i \to S$, i=1,2, dos morfismos separados entre esquemas noetherianos. Sea $\mathscr{M}$ un haz quasi-coherente en X_1 plano sobre S, tal que $R^i\pi_{1,*}\mathscr{M}$ son $\mathscr{O}_S$-módulos plano para todo i. Sea $\mathscr{N}$ un haz quasi-coherente en X_2. Sean

$$f_i : X_1 \times_S X_2 \to X_i \text{ y } \pi : X_1 \times_S X_2 \to S$$

las proyecciones obvias y $\mathscr{M} \otimes_{\mathscr{O}_S} \mathscr{N} := f_1^*\mathscr{M} \otimes_{\mathscr{O}_{X_1 \times_S X_2}} f_2^*\mathscr{N}$. Prueba que se cumple que

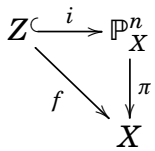
$$R^n\pi_*(\mathscr{M} \otimes_{\mathscr{O}_S} \mathscr{N}) = \bigoplus_{i+j=n} R^i\pi_{1,*}\mathscr{M} \otimes_{\mathscr{O}_S} R^j\pi_{2,*}\mathscr{N}$$

Resolución: Puede suponerse S afín. Considérense en X_1 y X_2 sendos recubrimientos por abiertos afines y en $X_1 \times_S X_2$ el correspondiente recubrimiento producto. Ahora ya, calcúlense las imágenes directas superiores con la ayuda de la cohomología Cech y úsese la fórmula de Kunneth algebraica.

6. Sea $\mathscr{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Prueba que un A-módulo M de tipo finito es de dimensión proyectiva finita si y sólo si para un $n \in \mathbb{N}$ se verifica que $\mathrm{Ext}^n_{\mathscr{O}}(M, \mathscr{O}/\mathfrak{m}) = 0$.

7. Sean X y Z dos k-variedades algebraicas cuasiproyectivas íntegras y $f : Z \to X$ un morfismo proyectivo birracional. Se cumple que f es el morfismo de explosión de X por un cierto haz de ideales I de X.

Resolución: Sigamos la demostración de Hartshorne. Como hemos supuesto que f es un morfismo proyectivo, existe un espacio proyectivo $\pi : \mathbb{P}^n_X \to X$, una inmersión cerrada $i : Z \hookrightarrow \mathbb{P}^n_X$ y un diagrama conmutativo



Sea $\mathscr{O}_Z(1) = i^*\mathscr{O}_{\mathbb{P}^n_X}(1)$. Por el teorema 12.3.4, $\mathscr{O}_Z$ es isomorfo a la localización homogénea de la $\mathscr{O}_X$-álgebra $B = \oplus_n f_*\mathscr{O}_Z(n)$. Si consideramos la sucesión exacta

obvia $0 \to I_Z \to \mathcal{O}_{\mathbb{P}^n_X} \to i_*\mathcal{O}_Z \to 0$. Por 13.6.8, para $m >> 0$, $\pi_*\mathcal{O}_{\mathbb{P}^n_X}(m) \to f_*\mathcal{O}_Z(m)$ es epiyectivo y B coincide, salvo en los primeros términos, con el cociente de $\mathcal{O}_X[x_0,\dots,x_n]$, por el ideal homogéneo de las funciones que se anulan en Z. Por tanto, para $m >> 0$, los elementos de grado m de B generan algebraicamente los de grado md. Si consideramos la inmersión de $\mathbb{P}^n_X \hookrightarrow \mathbb{P}^N_X$ definida por el haz de línea $\mathcal{O}_{\mathbb{P}^n_X}(m)$ y sustituimos $\mathbb{P}^n_X$ por $\mathbb{P}^N_X$, podremos decir que B está generado algebraicamente por los elementos de grado 1.

Sea Σ_Z el haz constante en Z, el cuerpo de funciones de Z. Consideremos una inmersión $\mathcal{O}_Z(1) \hookrightarrow \Sigma_Z$. Por tanto, tenemos la inyección $B_1 = f_*\mathcal{O}_Z(1) \hookrightarrow f_*\Sigma_Z$. Como f es birracional $f_*\Sigma_Z = \Sigma_X$ y tenemos la inyección $B_1 \hookrightarrow \Sigma_X$. Si consideramos el morfismo $\mathcal{O}_Z(n) = \mathcal{O}_Z(1) \otimes_{\mathcal{O}_Z} \dots \otimes_{\mathcal{O}_Z} \mathcal{O}_Z(1) \hookrightarrow \Sigma_Z \otimes_{\mathcal{O}_Z} \dots \otimes_{\mathcal{O}_Z} \Sigma_Z = \Sigma_Z$, del mismo modo tenemos que $B_n = f_*\mathcal{O}_Z(n) \hookrightarrow \Sigma_X$. La imagen del morfismo $B_1 \otimes_{\mathcal{O}_X} \dots \otimes_{\mathcal{O}_X} B_1 \hookrightarrow \Sigma_X \otimes_{\mathcal{O}_X} \dots \otimes_{\mathcal{O}_X} \Sigma_X = \Sigma_X$ es B_n. En conclusión, $X = \mathrm{Proj}B$ y si $B_1 = f_*\mathcal{O}_Z(1)$ fuera un haz de ideales de $\mathcal{O}_X$ habríamos concluido.

Sea $I \subseteq \mathcal{O}_X$ el ideal anulador de las clases de B_1 en $\Sigma_X/\mathcal{O}_X$. Luego $I \cdot B_1 \subset \mathcal{O}_X$. Recordemos que X es cuasiproyectiva y consideremos un haz de línea $\mathcal{M}$ muy amplio en X. Por el teorema de finitud de Serre 13.6.8, sabemos que existe un $m >> 0$, de modo que $\mathcal{M}^m \otimes_{\mathcal{O}_X} I$ está generado por sus secciones globales, luego existe un morfismo no nulo $\mathcal{O}_X \to \mathcal{M}^m \otimes_{\mathcal{O}_X} I$ y de aquí un morfismo no nulo $\mathcal{M}^{-m} \to I$. Sea $\mathcal{L} = \mathcal{M}^{-m}$, por construcción, $\mathcal{L} \otimes_{\mathcal{O}_X} B_1 = \mathcal{M}^{-m} \otimes_{\mathcal{O}_X} B_1 = \mathcal{M}^{-m} \cdot B_1 \subset \mathcal{O}_X$. Luego, $f_*(f^*\mathcal{L} \otimes \mathcal{O}_Z(1)) \subset \mathcal{O}_X$.

Si sustituimos $\mathcal{O}_{\mathbb{P}^n_X}(1)$, por $\pi^*\mathcal{L} \otimes \mathcal{O}_{\mathbb{P}^n_X}(1)$, es decir, consideramos el isomorfismo $\mathbb{P}^n_X \simeq \mathbb{P}^n_X$ que aplica uno en el otro, tendremos que B_1 es un haz de ideales de $\mathcal{O}_X$.

Capítulo 14

Teoría de la dualidad en curvas algebraicas

14.1. Introducción

En este capítulo hacemos una introducción a la Geometría Algebraica Global estudiando las curvas algebraicas. El teorema central será el teorema de Riemann-Roch. Por una parte exigirá la introducción de los haces de línea, cohomología, teoría de dualidad, y por otra dará las relaciones entre los distintos invariantes (género geométrico, género aritmético, longitud del conductor, grado de un divisor, grado del divisor canónico). Además posibilitará la demostración del teorema de Hurwitz, la existencia de haces línea muy amplios, etc.

Si X es una variedad diferenciable compacta orientada, tenemos el isomorfismo

$$H^i(X,\mathbb{R}) \simeq H^{n-i}(X,\mathbb{R})^*$$

que asigna a cada forma diferencial cerrada ω_i la forma lineal $H^{n-i}(X,\mathbb{R}) \to \mathbb{R}$ definida por $\omega_{n-i} \mapsto \int_X \omega_i \wedge \omega_{n-i}$. El objetivo de la teoría de la dualidad es dualizar la cohomología. Ahora, en Geometría Algebraica, sea C es una curva completa y consideremos el funtor sobre la categoría de $\mathcal{O}_C$-módulos quasi-coherentes

$$\mathscr{M} \rightsquigarrow H^1(C,\mathscr{M})^*.$$

Este funtor es exacto por la izquierda y transforma límites inductivos en proyectivos. Por el teorema de representabilidad, es representable por un $\mathcal{O}_C$-módulo quasi-coherente ω_C. Es decir,

$$\mathrm{Hom}_C(\mathscr{M},\omega_C) = H^1(C,\mathscr{M})^*.$$

Probaremos que si C es no singular, entonces $\omega_C = \Omega_{C/k}$. Además, el morfismo $\mathrm{Id}\colon \Omega_{C/k} \to \Omega_{C/k}$ se corresponderá por dualidad con una forma lineal

$$\mathrm{Res}\colon H^1(C,\Omega_{C/k}) \to k,$$

que es el residuo clásico del análisis complejo.

La teoría de dualidad, junto con el Riemann-Roch fuerte, permite el cálculo de la dimensión de los espacios de las funciones con polos de órdenes prefijados en determinados puntos. Dicho cálculo resuelve muchos problemas de tipo geométrico. Veremos diversas aplicaciones de la teoría de dualidad: Teorema de Hurwitz, clasificación de las curvas elípticas e hiperelípticas, inmersión canónica de una curva en un espacio proyectivo, etc.

14.2. Teorema de Riemann-Roch débil

Sea C una curva completa y $x_1,\dots,x_n$ puntos cerrados no singulares de C. Dado $D = \sum_i n_i \cdot x_i$, denotaremos $\mathscr{L}_D$, al de haz de línea sobre C, definido por

$$\mathscr{L}_D(V) = \{f \in \mathscr{O}_C(V \cap U')\colon v_{x_i}(f) \geq -n_i, \text{ para los } x_i \in V\}$$

donde $U' = C \setminus \{x_i\}_i$.

1. Teorema de Riemann-Roch débil: *Sea C una curva completa y $\mathscr{L}_D$ el haz de línea definido por D. Se cumple que*

$$\chi(C,\mathscr{L}_D) = \chi(C,\mathscr{O}_C) + \mathrm{gr}\, D.$$

Demostración. Dado un punto cerrado $x \in C$ no singular, consideremos la sucesión exacta

$$0 \to \mathscr{L}_{-x} \to \mathscr{O}_C \to k(x) \to 0$$

donde $k(x)$ es un haz concentrado en x, de modo que $h^0(C,k(x)) = \dim_k k(x) = \mathrm{gr}\, x$ y $h^1(C,k(x)) = 0$. Tensando por $\mathscr{L}_D$ resulta la sucesión exacta

$$0 \to \mathscr{L}_{D-x} \to \mathscr{L}_D \to k(x) \to 0$$

Luego $\chi(C,\mathscr{L}_D) = \chi(C,\mathscr{L}_{D-x}) + \chi(C,k(x)) = \chi(\mathscr{L}_{D-x}) + \mathrm{gr}\, x$. Así pues, el teorema de Riemann-Roch se verificará para $\mathscr{L}_D$ si y solo si se verifica para $\mathscr{L}_{D-x}$. Por tanto, por suma y resta de puntos a D, el teorema de Riemann-Roch se verificará para $\mathscr{L}_D$ si y solo si se verifica para $\mathscr{O}_C$, y en este caso es obvio. □

2. Lema: *Sea X un esquema localmente noetheriano íntegro.*

1. *Sea $\mathscr{M} \neq 0$ un haz coherente libre de torsión. Existe un haz coherente L, libre de torsión, de rango 1 y un morfismo inyectivo $L \hookrightarrow \mathscr{M}$, tal que $\mathscr{M}/L$ no tiene torsión.*

2. *Sea $\mathscr{M} \neq 0$ un haz quasi-coherente libre de torsión. Existe un haz de ideales L de rango 1 (es decir, no nulo) y un morfismo inyectivo $L \hookrightarrow \mathscr{M}$.*

Demostración. Sea $g \in X$ el punto genérico y $\Sigma = \mathscr{O}_{X,g}$.

1. Sea $s \in \mathscr{M}_g$ no nula. Consideremos el haz constante $\mathscr{M}_g$. Tanto $\mathscr{M}$ como el haz constante $\Sigma \cdot s$ son subhaces de $\mathscr{M}_g$. Sea $L := \Sigma \cdot s \cap \mathscr{M}$ el "haz de ceros y polos de s". Se cumple:

a) L es coherente y libre de torsión porque $\mathscr{M}$ lo es.

b) L es de rango 1 porque $L_g = \Sigma \cdot s \cap \mathscr{M}_g = \Sigma \cdot s$.

c) L está incluido en $\mathscr{M}$, $(\mathscr{M}/L)_g = \mathscr{M}_g/\Sigma \cdot s$ y el núcleo de $\mathscr{M} \to (\mathscr{M}/L)_g$ es L, luego el morfismo de haces $\mathscr{M}/L \to (\mathscr{M}/L)_g$ es inyectivo.

Con todo, hemos concluido.

2. Dada $s \in \mathscr{M}_g$ no nula, tómese $L := \mathscr{O}_X \cdot s \cap \mathscr{M}$. □

3. Teorema: *Sea $\mathscr{M}$ un módulo coherente y localmente libre de rango r sobre una curva C completa y no singular. Se cumple que*

$$\chi(\mathscr{M}) = r \cdot \chi(\mathscr{O}_C) + \operatorname{gr}(D(\Lambda^r_{\mathscr{O}_C}\mathscr{M}))$$

donde $D(\Lambda^r_{\mathscr{O}_C}\mathscr{M})$ es el divisor asociado al haz de línea $\Lambda^r_{\mathscr{O}_C}\mathscr{M}$.

Demostración. Lo vamos a demostrar por inducción sobre el rango de $\mathscr{M}$. Si $r = 1$, es el teorema de Riemann-Roch débil. Sea $\mathscr{L}$ un subhaz de línea de $\mathscr{M}$ tal que $\mathscr{M}/\mathscr{L}$ sea localmente libre de rango $r-1$ (existe por el Lema 14.2.2). Por la sucesión exacta larga de cohomología asociada a

$$0 \to \mathscr{L} \to \mathscr{M} \to \mathscr{M}/\mathscr{L} \to 0$$

y por inducción sobre el rango, se obtiene que

$$\begin{aligned}\chi(\mathscr{M}) &= \chi(\mathscr{L}) + \chi(\mathscr{M}/\mathscr{L}) = \chi(\mathscr{O}_C) + \operatorname{gr} D(\mathscr{L}) + (r-1)\cdot\chi(\mathscr{O}_C) + \operatorname{gr} D(\Lambda^{r-1}_{\mathscr{O}_C}(\mathscr{M}/\mathscr{L})) \\ &= r \cdot \chi(\mathscr{O}_C) + D(\Lambda^r_{\mathscr{O}_C}\mathscr{M}),\end{aligned}$$

donde la última igualdad se deduce de la igualdad $\mathscr{L} \otimes_{\mathscr{O}_C} \Lambda^{r-1}_{\mathscr{O}_C}(\mathscr{M}/\mathscr{L}) = \Lambda^r_{\mathscr{O}_C}\mathscr{M}$. □

Las siguientes proposiciones serán útiles en la teoría de dualidad.

4. Proposición : *Sea C una curva completa, $x \in C$ un punto no singular y $\mathscr{M}$ un módulo coherente de rango r. Denotemos $\mathscr{M}_{nx} = \mathscr{M} \otimes_{\mathscr{O}_C} \mathscr{L}_{nx}$. Entonces,*

1. *Para todo $n >> 0$, $h^1(C, \mathscr{M}_{nx}) = cte$ y $h^0(C, \mathscr{M}_{nx}) = r \cdot \mathrm{gr}\, x \cdot n + \ cte.$*

2. *Para todo $n >> 0$, $h^1(C, \mathscr{M}_{-nx}) = r \cdot \mathrm{gr}\, x \cdot n + cte$ y $h^0(C, \mathscr{M}_{-nx}) = cte'$.*

Demostración. 1. Si $\mathscr{M}$ es de rango cero, entonces $\mathscr{M}_{nx} = \mathscr{M}$, luego $H^0(C, \mathscr{M}_{nx}) = H^0(C, \mathscr{M})$ y $H^1(C, \mathscr{M}_{nx}) = 0$, de donde se concluye.

Sea $T(\mathscr{M})$ la torsión de $\mathscr{M}$. Si tensamos por $\mathscr{L}_{nx}$ la sucesión exacta

$$0 \to T(\mathscr{M}) \to \mathscr{M} \to \mathscr{M}/T(\mathscr{M}) \to 0,$$

obtenemos la sucesión exacta $0 \to T(\mathscr{M}) \to \mathscr{M}_{nx} \to (\mathscr{M}/T(\mathscr{M}))_{nx} \to 0$. Por lo tanto, $h^0(C, \mathscr{M}_{nx}) = h^0(C, T(\mathscr{M})) + h^0(C, (\mathscr{M}/T(\mathscr{M}))_{nx})$ y $h^1(C, \mathscr{M}_{nx}) = h^1(C, (\mathscr{M}/T(\mathscr{M}))_{nx})$. En conclusión, podemos suponer que $\mathscr{M}$ no tiene torsión.

Consideremos la sucesión exacta

$$0 \to \mathscr{L}_{(n-1)x} \to \mathscr{L}_{nx} \to k(x) \to 0$$

Tensando por $\otimes_{\mathscr{O}_C} \mathscr{M}$ y teniendo en cuenta que $\mathscr{M}$ no tiene torsión, se obtiene la sucesión exacta

$$0 \to \mathscr{M}_{(n-1)x} \to \mathscr{M}_{nx} \to \mathscr{M} \otimes_{\mathscr{O}_C} k(x) \to 0$$

Tomando cohomología, tenemos un epimorfismo $H^1(C, \mathscr{M}_{(n-1)x}) \to H^1(C, \mathscr{M}_{nx})$. Por lo tanto, existe un n_0 tal que $h^1(C, \mathscr{M}_{nx}) = cte$, para $n > n_0$. Ahora, para todo $n > n_0$, $h^0(C, \mathscr{M}_{(n+1)x}) = h^0(C, \mathscr{M}_{nx}) + h^0(C, \mathscr{M} \otimes_{\mathscr{O}_c} k(x))$. Ahora bien, $\Gamma(C, \mathscr{M} \otimes_{\mathscr{O}_c} k(x)) = \mathscr{M}/\mathfrak{m}_x \mathscr{M}$, que es un $k(x)$-espacio vectorial de dimensión r, porque $\mathscr{M}_x$ es libre de torsión de rango r, luego libre de rango r. En conclusión, $h^0(C, \mathscr{M}_{(n+1)x}) = h^0(C, \mathscr{M}_{nx}) + r \cdot \mathrm{gr}\, x$, y por tanto

$$h^0(C, \mathscr{M}_{nx}) = h^0(C, \mathscr{M}_{n_0 x}) + (n - n_0) \cdot r \cdot \mathrm{gr}\, x = r \cdot \mathrm{gr}\, x \cdot n + \ \mathrm{cte}.$$

2. Pruébese primero que se puede suponer que $\mathscr{M}$ no tiene torsión y a continuación considérese la sucesión exacta $0 \to \mathscr{M}_{(-n-1)x} \to \mathscr{M}_{-nx} \to \mathscr{M} \otimes_{\mathscr{O}_C} k(x) \to 0$.

□

5. Proposición: *Sea C una curva completa, $x \in C$ un punto no singular y $\mathscr{M}$ un haz quasi-coherente. Si para todo $n >> 0$ se cumple que $h^0(C, \mathscr{M}_{nx}) \leq r \cdot \mathrm{gr}\, x \cdot n +$ cte., entonces $\mathscr{M}$ es un módulo coherente de rango menor o igual que r.*

Demostración. Vamos a proceder por inducción sobre r.

Consideremos la inclusión natural $0 \to T(\mathscr{M}) \to \mathscr{M}$. Tensando por $\mathscr{L}_{nx}$, tenemos $0 \to T(\mathscr{M}) \to \mathscr{M}_{nx}$. Por tanto, $h^0(C, T(\mathscr{M})) < \infty$. Ahora bien, $H^0(C, T(\mathscr{M})) = \underset{x \in C}{\oplus} T(\mathscr{M})_x$, luego solo para un número finito de puntos cerrados $T(\mathscr{M})_x \neq 0$ y éstos son k-espacios vectoriales de dimensión finita. En consecuencia, $T(\mathscr{M})$ es un módulo coherente de rango cero.

Haciendo cociente por $T(\mathscr{M})$ podemos suponer que $\mathscr{M}$ no tiene torsión.

Sea $L \hookrightarrow \mathscr{M}$ un submódulo coherente de rango 1. Consideremos la sucesión exacta

$$0 \to L_{nx} \to \mathscr{M}_{nx} \to (\mathscr{M}/L)_{nx} \to 0$$

Por la sucesión exacta larga de cohomología y por inducción sobre r, $\mathscr{M}/L$ es coherente de rango menor o igual que $r-1$, luego $\mathscr{M}$ es coherente de rango menor o igual que r. □

6. Ejercicio: Sea C una curva completa no singular y $x \in C$ un punto cerrado. Probar que $C \backslash x$ es una curva afín.

Resolución: Por 14.2.4, $h^0(C, \mathscr{L}_{(n+1)x}) \neq h^0(C, \mathscr{L}_{nx})$ para $n >> 0$, luego existe una función $f \in \Sigma_C$ con un único polo (de orden $n+1$) en x. Por tanto, el morfismo afín definido por f

$$f : C \to \mathbb{P}^1$$

verifica que $f^{-1}(\infty) = (n+1)x$, luego $C \backslash x = f^{-1}(\mathbb{P}^1 \backslash \infty)$, que es afín.

14.3. Teoremas de dualidad y Riemann-Roch fuerte

Sea C una curva completa sobre k. Consideremos el funtor sobre la categoría de módulos quasi-coherentes sobre C definido por

$$\mathscr{M} \rightsquigarrow H^1(C, \mathscr{M})^*$$

Este funtor es exacto por la izquierda, ya que $H^2(C, \mathscr{M}) = 0$ para todo haz quasi-coherente $\mathscr{M}$, y transforma límites inductivos en proyectivos, porque la cohomología conmuta con límites inductivos. Por tanto, es representable. Es decir, existe un módulo quasi-coherente ω_C y un elemento $\mathrm{res} \in H^1(C, \omega_C)^*$ de modo que para todo módulo quasi-coherente $\mathscr{M}$, el morfismo

$$\mathrm{Hom}(\mathscr{M}, \omega_C) \to H^1(C, \mathscr{M})^*,$$

que asigna a cada morfismo $f : \mathscr{M} \to \omega_C$ la imagen de res por el morfismo inducido por f, $H^1(C, \omega_C)^* \to H^1(C, \mathscr{M})^*$, es isomorfismo.

1. Definición: Una pareja (ω_C, res) que represente el funtor $H^1(C,-)^*$ se denomina par dualizante de C. El módulo ω_C se denomina haz dualizante de C, y la igualdad

$$H^1(C,\mathscr{M})^* = \text{Hom}_{\mathscr{O}_C}(\mathscr{M},\omega_C)$$

se denomina isomorfismo de dualidad.

Si (ω'_C, res') es otro par dualizante, existe un único isomorfismo $\phi\colon \omega_C \to \omega'_C$ que transforma res' en res, por el morfismo $H^1(C,\omega'_C)^* \to H^1(C,\omega_C)^*$ inducido por ϕ. En particular, el haz dualizante es único salvo isomorfismos.

2. Teorema de Riemann-Roch fuerte: *Sea C una curva completa, $\{x_i\}$ puntos no singulares de C, $D = \sum_i n_i x_i$ y $\mathscr{L}_D$ el haz de línea asociado a D. Se verifica que*

$$h^0(C,\mathscr{L}_D) - h^0(C,\omega_C \underset{\mathscr{O}_C}{\otimes} \mathscr{L}_{-D}) = \chi(C,\mathscr{O}_C) + \text{gr}\, D$$

Demostración. Tenemos que

$$H^1(C,\mathscr{L}_D)^* = \text{Hom}_{\mathscr{O}_C}(\mathscr{L}_D,\omega_C) = \text{Hom}_{\mathscr{O}_C}(\mathscr{O}_C,\omega_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D}) = \Gamma(C,\omega_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D}).$$

Por tanto, $h^1(C,\mathscr{L}_D) = h^0(C,\omega_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D})$. Se concluye por el Riemann-Roch débil. □

3. Proposición: *El haz dualizante ω_C es un haz coherente de rango 1 sin torsión. En particular, si C es una curva completa no singular, ω_C es un haz de línea.*

Demostración. Probemos que el dualizante no tiene torsión. Si T es un módulo coherente incluido en la torsión de ω_C, se verifica $\text{Hom}_{\mathscr{O}_C}(T,\omega_C) = H^1(C,T)^* = 0$ porque T es flasco. Por tanto, $T = 0$ y ω_C es libre de torsión.

Nos falta ver que ω_C es coherente de rango 1. Sea x un punto no singular de C. Tenemos que $H^0(C,(\omega_C)_{nx}) = \text{Hom}_{\mathscr{O}_C}(\mathscr{O}_C,\omega_C \otimes \mathscr{L}_{nx}) = \text{Hom}_{\mathscr{O}_C}(\mathscr{L}_{-nx},\omega_C) = H^1(C,\mathscr{L}_{-nx})^*$. Por 14.2.4,

$$h^0(C,(\omega_C)_{nx}) = \text{gr}\, x \cdot n + \text{ cte}$$

para $n >> 0$, luego (14.2.5) ω_C es coherente de rango 1. □

4. Definición: Sea C una curva completa. Llamaremos género aritmético de C a $h^1(C,\mathscr{O}_C)$ y género geométrico al género aritmético de su desingularización. Los denotaremos g_a y g respectivamente.

5. Proposición: *Sea C una curva completa.*

1. *El género aritmético de C es $h^0(C,\omega_C)$.*

2. Si C es no singular, entonces $h^1(C,\omega_C) = h^0(C,\mathscr{O}_C)$.

Demostración. 1. $H^0(C,\omega_C) = \mathrm{Hom}_{\mathscr{O}_C}(\mathscr{O}_C,\omega_C) = H^1(C,\mathscr{O}_C)^*$. Por tanto, $g_a = h^0(C,\omega_C)$.
2. $H^1(C,\omega_C)^* = \mathrm{Hom}_{\mathscr{O}_C}(\omega_C,\omega_C) = \mathrm{Hom}_{\mathscr{O}_C}(\mathscr{O}_C,\mathscr{O}_C) = H^0(C,\mathscr{O}_C)$. □

6. Definición: Sea C una curva completa no singular. Llamaremos divisores canónicos a los divisores cuyo haz de línea asociado sea el haz dualizante.

7. Proposición: *Si K es un divisor canónico de una curva C completa y no singular, entonces*

$$\mathrm{gr}\, K = 2\,\chi(C,\mathscr{O}_C).$$

En particular, si k es íntegramente cerrado en Σ_C, entonces

$$\mathrm{gr}\, K = 2g - 2.$$

Demostración. Es una consecuencia inmediata del Riemann-Roch débil para $\mathscr{L}_K = \omega_C$ y de la proposición anterior. □

8. Ejercicio: Sea C una curva completa sobre un cuerpo k íntegramente cerrado en Σ_C. Prueba que $h^1(C,\omega_C) = 1$.

Resolución: $\mathrm{Hom}_{\mathscr{O}_C}(\omega_C,\omega_C) = k$, porque todo endomorfismo de ω_C es multiplicar por una $f \in \Sigma_C$ y el morfismo $f\cdot\colon \Gamma(C,\omega_C) \to \Gamma(C,\omega_C)$ está anulado por el polinomio característico.

9. Ejercicio: Sea L un haz coherente libre de torsión de rango 1 sobre una curva completa C, tal que $h^0(C,L) = g_a$ y $h^1(C,L) = h^0(C,\mathscr{O}_C)$. Probar que L es isomorfo al haz dualizante.

Resolución: $\mathrm{Hom}_{\mathscr{O}_C}(L,\omega_C) = H^1(C,L)^* \neq 0$, entonces tenemos un morfismo no nulo $L \to \omega_C$, que ha de ser inyectivo. Sea T el conúcleo, que es de torsión. El morfismo $H^1(C,L) \to H^1(C,\omega_C)$ es epiyectivo y $h^0(C,\mathscr{O}_C) \leq h^1(C,\omega_C)$ (pruébese), luego $h^1(C,L) = h^1(C,\omega_C)$. Además, $h^0(C,L) = h^1(C,\mathscr{O}_C) = h^0(C,\omega_C)$. Por tanto, $h^0(C,T) = 0$, luego $T = 0$ y $L = \omega_C$.

10. Ejercicio: Sea $C \overset{i}{\hookrightarrow} \mathbb{P}^2$ una curva plana irreducible de grado n, sobre un cuerpo algebraicamente cerrado. Demuéstrese que $\mathscr{O}_C(n-3)$ es el haz dualizante de C. (Pista: Tensa la sucesión exacta $0 \to \mathscr{O}_{\mathbb{P}^2}(-n) \to \mathscr{O}_{\mathbb{P}^2} \to i_*\mathscr{O}_C \to 0$ por $\mathscr{O}_{\mathbb{P}^2}(n-3)$ y utiliza el ejercicio anterior).

14.4. Dualizante de una curva lisa

1. Definición: Sea X un k-esquema. Denotamos por $\Omega_{X/k}$ y lo denominamos haz de diferenciales de Kähler de X, al haz asociado al prehaz

$$U \rightsquigarrow \Omega_{\mathscr{O}_X(U)/k}$$

para cada abierto U de X.

Procedamos con mayor generalidad.

2. Definición: Sea $f: X \to Y$ un morfismo de esquemas. Sea $\delta: X \to X \times_Y X$ el morfismo diagonal y Δ el núcleo del morfismo $\mathscr{O}_{X\times_Y X} \to \delta_*\mathscr{O}_X$. Llamaremos haz de diferenciales relativas de X sobre Y, y lo denotaremos $\Omega_{X/Y}$, a

$$\Omega_{X/Y} := \delta^*\Delta.$$

Si $V = \operatorname{Spec} A$ es un abierto afín de Y y $U = \operatorname{Spec} B$ es un abierto afín de X contenido en $f^{-1}(V)$, entonces $\Omega_{X/Y}(U) = \Omega_{B/A}$.

3. Ejercicio: Sea $\mathbb{P}^1$ la variedad de Riemann de $k(x)$. Calcular el divisor de ceros y polos de $dx \in \Omega_{k(x)/k}$. Demostrar que $\Omega_{\mathbb{P}^1/k} \simeq \mathscr{O}_{\mathbb{P}^1}(-2)$.

Sea C una curva no singular sobre un cuerpo algebraicamente cerrado. Sea $U = \operatorname{Spec} A$ un abierto afín. Consideremos la sucesión exacta

$$0 \to \Delta_A \to A \otimes_k A \xrightarrow{\pi} A \to 0.$$

El morfismo π es un epimorfismo de un anillo regular de dimensión 2 en un anillo regular de dimensión 1. Por tanto, Δ_A es un ideal de $A \otimes A$ localmente principal, luego $\Delta_A/\Delta_A^2 = \Omega_{C/k}(U)$ es un A-módulo localmente principal. En conclusión, obtenemos la siguiente proposición.

4. Proposición: *Si C es una curva no singular sobre un cuerpo perfecto, entonces $\Omega_{C/k}$ es un haz de línea.*

5. Teorema: *Si C es una curva completa no singular sobre un cuerpo k algebraicamente cerrado, entonces*

$$\omega_C \simeq \Omega_{C/k}.$$

Demostración. Sea $x \in C$ un punto cerrado y $\mathfrak{m}_x = \mathscr{L}_{-x}$ el haz de ideales de las funciones que se anulan en x. Se tiene la sucesión exacta, de morfismos obvios

$$0 \to \omega_C \xrightarrow{i} \underline{\operatorname{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x, \omega_C) \xrightarrow{\pi} \underline{\operatorname{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \omega_C/\mathfrak{m}_x\omega_C) \to 0 \qquad (*)$$

Tomando la sucesión exacta larga de cohomología, teniendo en cuenta la igualdad $\underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x, \omega_C) = \omega_C \otimes \mathscr{L}_x$ y dualidad, se obtiene

$$\mathrm{Hom}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \omega_C/\mathfrak{m}_x\omega_C) \xrightarrow{\delta_x} H^1(C, \omega_C) \to H^1(C, \omega_C \otimes \mathscr{L}_x) \simeq H^0(C, \mathscr{L}_{-x})^* = 0$$

Por dimensiones, $\mathrm{Hom}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \omega_C/\mathfrak{m}_x\omega_C) \xrightarrow{\delta_x} H^1(C, \omega_C)$. Así pues, cada $\xi \in H^1(C, \omega_C)$ no nulo, se corresponde con un isomorfismo

$$\delta_x^{-1}(\xi)\colon \mathfrak{m}_x/\mathfrak{m}_x^2 = \omega_C/\mathfrak{m}_x\omega_C$$

Sustituyendo x por un "punto general" obtendremos el isomorfismo $\Omega_{C/k} \simeq \omega_C$. Veámoslo.

Sean y $\pi_1, \pi_2\colon C \times_k C \to C$ las proyecciones en el primer y segundo factor. Denotemos $\omega_C \otimes_k \mathscr{O}_C = \pi_1^*\omega_C$. Sea $i\colon C \to C \times_k C$ el morfismo diagonal y Δ el ideal de la diagonal, es decir, el núcleo del epimorfismo $\mathscr{O}_{C\times_k C} \to i_*\mathscr{O}_C$, que es un $\mathscr{O}_{C\times_k C}$-módulo de línea. Observemos que $\Delta/\Delta^2 = i_*\Omega_{C/k}$ y $(\omega_C \otimes_k \mathscr{O}_C)/\Delta\cdot(\omega_C \otimes_k \mathscr{O}_C) = i_*\omega_C$.

Consideremos la sucesión exacta

$$0 \to \omega_C \otimes_k \mathscr{O}_C \to \underline{\mathrm{Hom}}_{\mathscr{O}_{C\times_k C}}(\Delta, \omega_C \otimes_k \mathscr{O}_C) \to \underline{\mathrm{Hom}}_{\mathscr{O}_{C\times_k C}}(i_*\Omega_{C/k}, i_*\omega_C) \to 0$$

Restringiendo a $C \times x$ se obtiene la sucesión exacta $(*)$. Tomando imágenes directas π_{2*}, obtenemos un morfismo $\underline{\mathrm{Hom}}_{\mathscr{O}_C}(\Omega_{C/k}, \omega_C) \xrightarrow{\delta} R^1\pi_{2*}(\omega_C \otimes_k \mathscr{O}_C)$. Aplicando 13.4.6 al morfismo $C \to \mathrm{Spec}\, k$ y el cambio de base $C \to \mathrm{Spec}\, k$, obtenemos que $R^1\pi_{2*}(\omega_C \otimes_k \mathscr{O}_C) = H^1(C, \omega_C) \otimes_k \mathscr{O}_C$. Así pues, δ es un morfismo entre haces de línea, que en fibras sobre cada punto cerrado $x \in C$ es igual a δ_x, luego δ es un isomorfismo.

Con todo, se tiene el diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Hom}_{\mathscr{O}_C}(\Omega_{C/k}, \omega_C) & \xrightarrow{\delta_C} & H^1(C, \omega_C) \\ \downarrow & & \| \\ \mathrm{Hom}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \omega_C/\mathfrak{m}_x\omega_C) & \xrightarrow{\delta_x} & H^1(C, \omega_C) \end{array}$$

luego cada $\xi \in H^1(C, \omega_C)$ no nulo se corresponde con un morfismo

$$\delta_C^{-1}(\xi)\colon \Omega_{C/k} \to \omega_C$$

que es isomorfismo, porque al tomar fibra en cada x es el isomorfismo $\delta_x^{-1}(\xi)$. □

14.5. Residuo

1. Definición: Llamaremos residuo de una curva C completa y no singular, a la única aplicación lineal

$$\mathrm{Res}\colon H^1(C,\Omega_{C/k}) \to k$$

tal que $\mathrm{Res}(\delta_C(\mathrm{Id})) = 1$, siendo δ_C el isomorfismo canónico

$$\delta_C\colon \mathrm{Hom}_{\mathscr{O}_C}(\Omega_{C/k},\Omega_{C/k}) = H^1(C,\Omega_{C/k})$$

construido en la demostración del teorema anterior.

La pareja $(\Omega_{C/k},\mathrm{Res})$ representa el functor $H^1(C,-)^*$. Es un par dualizante canónico.

2. Observaciones: 1. Dado $\phi \in H^1(C,\mathscr{M})^*$ existe un único morfismo $i\colon \mathscr{M} \to \Omega_{C/k}$ tal que $\phi = \mathrm{Res}\circ i_*$, donde $i_*\colon H^1(C,\mathscr{M}) \to H^1(C,\Omega_{C/k})$ es el morfismo inducido por i en cohomología.

2. La imagen de Id por el morfismo natural

$$\mathrm{Hom}_{\mathscr{O}_C}(\Omega_{C/k},\Omega_{C/k}) \to \mathrm{Hom}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2,\Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k})$$

es $d_x\colon \mathfrak{m}_x/\mathfrak{m}_x^2 \to \Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k}$, $\bar{a} \mapsto d_x a$. Por tanto, $\delta_C(\mathrm{Id}) = \delta_x(d_x)$ y $\mathrm{Res}(\delta_x(d_x)) = 1$.

Sea C una curva completa y (ω_C,res) un par dualizante, con $\mathrm{res} \in H^1(C,\omega_C)^*$. Sea Σ el cuerpo de funciones de C y ω_Σ la fibra de ω_C en el punto genérico. Seguiremos denotando ω_Σ el haz constante ω_Σ. Consideremos la sucesión exacta

$$0 \to \omega_C \to \omega_\Sigma \to \omega_\Sigma/\omega_C \to 0$$

donde la inyectividad se deduce de que ω_C es un módulo coherente sin torsión.

Para simplificar notaciones, denotaremos ω_x el germen en x del dualizante ω_C, y análogamente $\mathscr{O}_x$ el anillo local de $\mathscr{O}_C$ en x.

Obviamente, el germen de ω_Σ/ω_C en el punto genérico es cero, luego para todo abierto U de C se tiene $(\omega_\Sigma/\omega_C)(U) = \bigoplus_{x\in U} \omega_\Sigma/\omega_x$. De la sucesión exacta anterior se deduce la sucesión exacta

$$\omega_\Sigma \to \bigoplus_{x\in C} \omega_\Sigma/\omega_x \to H^1(C,\omega_C) \to 0$$

Denotemos res_x la composición de los morfismos naturales

$$\omega_\Sigma \to \omega_\Sigma/\omega_x \hookrightarrow \bigoplus_{x\in C} \omega_\Sigma/\omega_x \to H^1(C,\omega_C) \xrightarrow{\mathrm{res}} k$$

Si $\theta = \overline{\oplus_x \bar{\theta}_x} \in H^1(C, \omega_C)$, entonces $\mathrm{res}(\overline{\oplus_x \bar{\theta}_x}) = \sum_x \mathrm{res}_x(\theta_x)$ y si $\theta \in \omega_\Sigma$, entonces

$$0 = \mathrm{res}(\overline{\oplus_x \bar{\theta}}) = \sum_x \mathrm{res}_x(\theta)$$

Por definición, si $\theta_x \in \omega_x$, entonces $\mathrm{res}_x(\theta_x) = 0$. También es cierto el recíproco, en el siguiente sentido.

3. Proposición: *Sea $\theta \in \omega_\Sigma$. Si $\mathrm{res}_x(\mathcal{O}_x \cdot \theta) = 0$, para todo $x \in U$, entonces $\theta \in \omega_C(U)$. Si $\mathrm{res}_x(\mathcal{O}_x \cdot \theta) = 0$, entonces $\theta \in \omega_{C,x}$.*

Demostración. Sea $U' = C \setminus \{\text{polos de } \theta \text{ en } U\}$. Sea W el $\mathcal{O}_C$-módulo coherente definido como el subhaz de ω_Σ dado por

$$W_{|U} = \omega_{C|U} + \mathcal{O}_U \cdot \theta, \qquad W_{|U'} = \omega_{C|U'}.$$

Por definición de W, tenemos $W_\Sigma = \omega_\Sigma$ y una inclusión $\omega_C \overset{i}{\hookrightarrow} W$. Además, por las hipótesis sobre θ, se tiene un morfismo $\mathrm{res}' \colon H^1(C, W) \to k$, que hace conmutativo el diagrama

$$\begin{array}{ccc} [\oplus_{x \in C} \omega_\Sigma/\omega_x]/\omega_\Sigma & \xrightarrow{\text{epi}} & [\oplus_{x \in C} \omega_\Sigma/W_x]/\omega_\Sigma \\ \downarrow{\scriptstyle \text{res}} & \swarrow{\scriptstyle \text{res}'} & \\ k & & \end{array}$$

Es decir, $i^*(\mathrm{res}') = \mathrm{res}$, siendo $i^* \colon H^1(C, W)^* \to H^1(C, \omega_C)^*$ el morfismo inducido por i. Por definición de dualizante, existe un morfismo $j \colon W \to \omega_C$ tal que $j^*(\mathrm{res}) = \mathrm{res}'$, vía el morfismo $j^* \colon H^1(C, \omega_C)^* \to H^1(C, W)^*$. Por dualidad, $j \circ i = \mathrm{Id}$ y por ser ω_C y W módulos de rango uno sin torsión, la inclusión $i \colon \omega_C \hookrightarrow W$ es una igualdad. En conclusión, $W = \omega_C$ y $\theta \in \omega_C(U)$.

Por último, existe un entorno abierto pequeño U de x de modo que $\theta \in \omega(U - x)$. Luego, si $res_x(\mathcal{O}_x \cdot \theta) = 0$ entonces $\theta \in \omega(U)$ y $\theta \in \omega_x$. □

Sea C una curva no singular completa sobre un cuerpo algebraicamente cerrado, $x \in C$ un punto cerrado y $t \in \Sigma$ un parámetro en x (es decir, $t \cdot \mathcal{O}_x = \mathfrak{m}_x$). Obsérvese que $\Omega_{\Sigma/k}/\Omega_{\mathcal{O}_x/k} = \{\sum_{i>0}^{n} a_i \frac{dt}{t^i},\ a_i \in k, n \in \mathbb{N}\}$.

4. Proposición: $\mathrm{Res}_x(\frac{dt}{t}) = 1$.

Demostración. En el isomorfismo

$$\delta_x \colon \mathrm{Hom}_{\mathcal{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k}) = H^1(C, \Omega_{C/k})$$

construido en la demostración de 14.4.5, vimos que $\delta_x(\mathrm{Id}_x) = \delta_C(\mathrm{Id})$, donde el morfismo $\mathrm{Id}_x : \mathfrak{m}_x/\mathfrak{m}_x^2 \to \Omega_{C/k} \otimes_{\mathscr{O}_C} k(x)$ está definido por $d_x a \mapsto \overline{da}$. Por tanto, $\mathrm{Res}(\delta_x(\mathrm{Id}_x)) = 1$.

El haz $\underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x, \Omega_{C/k}) = \Omega_{C/k} \otimes_{\mathscr{O}_C} \mathscr{L}_x$ es un subhaz de $\Omega_{\Sigma/k} = \Omega_{C/k} \otimes_{\mathscr{O}_C} \Sigma_C$. El morfismo

$$\underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x, \Omega_{C/k})_x \to \underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k})$$

transforma $\frac{dt}{t}$ en Id_x. Además, $\underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k})$ está soportado en x. Del diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega_{C/k} & \longrightarrow & \underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x, \Omega_{C/k}) & \longrightarrow & \underline{\mathrm{Hom}}_{\mathscr{O}_C}(\mathfrak{m}_x/\mathfrak{m}_x^2, \Omega_{C/k}/\mathfrak{m}_x\Omega_{C/k}) & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow \phi & & \\
0 & \longrightarrow & \Omega_{C/k} & \longrightarrow & \Omega_{\Sigma/k} & \longrightarrow & \Omega_{\Sigma/k}/\Omega_{C/k} & \longrightarrow & 0
\end{array}$$

se concluye que $\phi(\mathrm{Id}_x) = (0, \ldots, \frac{dt}{t}, \ldots, 0)$, luego

$$\mathrm{Res}_x(\frac{dt}{t}) = \mathrm{Res}(\overline{(0, \ldots, \frac{dt}{t}, \ldots, 0)}) = \mathrm{Res}(\delta_x(\mathrm{Id}_x)) = 1.$$

□

Denotemos $\bar{y} \in k[y]/(y^n)$ por ϵ, luego $k[\epsilon] = k[y]/(y^n)$. Sea $C_\epsilon = C \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, k[\epsilon]$, que como espacio topológico es igual a C. Observemos que $\mathscr{O}_{C_\epsilon}(U) = \mathscr{O}_C(U) \otimes_k k[\epsilon]$

5. Proposición: *El funtor* $\mathscr{M} \rightsquigarrow H^1(\mathscr{M}, C_\epsilon)^\times := \mathrm{Hom}_{k[\epsilon]}(H^1(\mathscr{M}, C_\epsilon), k[\epsilon])$ *es representable pos* $\Omega_{C_\epsilon/k[\epsilon]}$.

Demostración. Sea w_{C_ϵ} el representante del funtor. Sea $\pi : C_\epsilon \to C$ el morfismo natural. Tenemos

$$\begin{aligned}
\mathrm{Hom}_{\mathscr{O}_C}(\mathscr{M}, \pi_* w_{C_\epsilon}) &= \mathrm{Hom}_{\mathscr{O}_{C_\epsilon}}(\pi^*\mathscr{M}, w_{C_\epsilon}) = H^1(C_\epsilon, \pi^*\mathscr{M})^\times = (H^1(C, \mathscr{M}) \otimes_k k[\epsilon])^\times \\
&= H^1(C, \mathscr{M})^* \otimes_k k[\epsilon] = \mathrm{Hom}_{\mathscr{O}_C}(\mathscr{M}, \Omega_{C/k}) \otimes_k k[\epsilon] = \mathrm{Hom}_{\mathscr{O}_C}(\mathscr{M}, \Omega_{C/k} \otimes_k k[\epsilon]).
\end{aligned}$$

Luego, $\pi_* w_{C_\epsilon} = \Omega_{C/k} \otimes_k k[\epsilon]$ y $w_{C_\epsilon} = \Omega_{C_\epsilon/k[\epsilon]}$.

□

Denotemos $\Omega_{C_\epsilon/k[\epsilon]} = \Omega_{C_\epsilon}$ y $\Omega_{C/k} = \Omega_C$. Observemos que

$$H^1(C_\epsilon, \Omega_{C_\epsilon}) = H^1(C_\epsilon, \pi^*\Omega_C) = H^1(C, \Omega_C \otimes_k k[\epsilon]) = H^1(C, \Omega_C) \otimes_k k[\epsilon] \simeq k[\epsilon].$$

Igual que hemos hecho en C con Ω_C (en la demostración de 14.4.5), tenemos la sucesión exacta

$$0 \to \Omega_{C_\epsilon} \otimes_{k[\epsilon]} \mathscr{O}_{C_\epsilon} \to \underline{\mathrm{Hom}}_{\mathscr{O}_{C_\epsilon \times_{k[\epsilon]} C_\epsilon}}(\Delta, \Omega_{C_\epsilon} \otimes_{k[\epsilon]} \mathscr{O}_{C_\epsilon}) \to \underline{\mathrm{Hom}}_{\mathscr{O}_{C_\epsilon \times_{k[\epsilon]} C_\epsilon}}(i_*\Omega_{C_\epsilon}, i_*\Omega_{C_\epsilon}) \to 0$$

(que se obtiene también de aplicar π^* a la correspondiente sucesión que aparece en la demostración de 14.4.5) y de nuevo tomando $R^1\pi_{2*}$ obtenemos un morfismo

$$\underline{\mathrm{Hom}}_{\mathscr{O}_{C_\epsilon}}(\Omega_{C_\epsilon}, \Omega_{C_\epsilon}) \xrightarrow{\delta_\epsilon} H^1(C_\epsilon, \Omega_{C_\epsilon}) \otimes_{k[\epsilon]} \mathscr{O}_{C_\epsilon}$$

que es un isomorfismo porque es el que se obtiene de aplicar π^* al correspondiente isomorfismo de 14.4.5. Tomando secciones globales tenemos la igualdad $\mathrm{Hom}_{\mathscr{O}_{C_\epsilon}}(\Omega_{C_\epsilon}, \Omega_{C_\epsilon}) = H^1(C_\epsilon, \Omega_{C_\epsilon})$ y el diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Hom}_{\mathscr{O}_{C_\epsilon}}(\Omega_{C_\epsilon}, \Omega_{C_\epsilon}) & \xrightarrow{\delta_{C_\epsilon}} & H^1(C_\epsilon, \Omega_{C_\epsilon}) \\ \uparrow{\scriptstyle \pi^*} & & \uparrow{\scriptstyle \pi^*} \\ \mathrm{Hom}_{\mathscr{O}_C}(\Omega_C, \Omega_C) & \xrightarrow{\delta_C} & H^1(C, \Omega_C) \end{array}$$

Se define $\mathrm{Res}_{C_\epsilon} : H^1(C_\epsilon, \Omega_{C_\epsilon}) \to k[\epsilon]$ como la única aplicación $k[\epsilon]$-lineal que cumple que $\mathrm{Res}_{C_\epsilon}(\delta_{C_\epsilon}) = 1$. Tenemos que $\mathrm{Res}_{C_\epsilon} \circ \pi^* = \mathrm{Res}_C$.

Sea g el punto génerico de C (o C_ϵ) y consideremos la sucesión exacta

$$0 \to \Omega_{C_\epsilon} \to (\Omega_{C_\epsilon})_g \to (\Omega_{C_\epsilon})_g / \Omega_{C_\epsilon} \to 0$$

Tenemos que $(\Omega_{C_\epsilon})_g / \Omega_{C_\epsilon} = \bigoplus_{x \in C = C_\epsilon} (\Omega_{C_\epsilon})_g / (\Omega_{C_\epsilon})_x$ y la sucesión exacta

$$(\Omega_{C_\epsilon})_g \to \bigoplus_{x \in C = C_\epsilon} (\Omega_{C_\epsilon})_g / (\Omega_{C_\epsilon})_x \to H^1(C_\epsilon, \Omega)$$

La composición

$$(\Omega_{C_\epsilon})_g \to (\Omega_{C_\epsilon})_g / (\Omega_{C_\epsilon})_x \hookrightarrow \bigoplus_{x \in C = C_\epsilon} (\Omega_{C_\epsilon})_g / (\Omega_{C_\epsilon})_x \to H^1(C_\epsilon, \Omega)$$

la denotamos $\mathrm{Res}_{C_\epsilon, x}$. De nuevo, $\mathrm{Res}_{C_\epsilon} = \sum_{x \in C} \mathrm{Res}_{C_\epsilon, x}$.

Sea $x \in C$ un punto cerrado y consideremos el ideal $\mathfrak{m}_x = (t) \subset \mathscr{O}_{C,x}$ Sea $\mathfrak{m}_{\tilde{x}} = (f) \subset \mathscr{O}_{C_\epsilon, x}$, tal que $\bar{f} = t \in \mathscr{O}_{C_\epsilon, x}/(\epsilon) = \mathscr{O}_{C,x}$. Como $f = t + \epsilon \cdot g$, tenemos que $t^n = (f - \epsilon \cdot g)^n \in (f)$ y observemos que $\mathscr{O}_{C_\epsilon, x}/(t^n) = \mathscr{O}_{C,x}/(t^n) \otimes_k k[\epsilon] = k[x,y]/(x^n, y^n)$. Ahora es fácil probar, pasando a $\mathscr{O}_{C_\epsilon, x}/(t^n)$, que $\mathscr{O}_{C_\epsilon, x}/\mathfrak{m}_{\tilde{x}} = k[\epsilon]$ y que $\mathfrak{m}_{\tilde{x}}/\mathfrak{m}_{\tilde{x}}^2$ es un $k[\epsilon]$-módulo libre de base $\bar{f}$. Por otra parte, es fácil probar que f es un no divisor de cero. De nuevo tendremos las sucesiones exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega_{C_\epsilon/k} & \longrightarrow & \underline{\mathrm{Hom}}_{\mathscr{O}_{C_\epsilon}}(\mathfrak{m}_{\tilde{x}}, \Omega_{C_\epsilon}) & \longrightarrow & \underline{\mathrm{Hom}}_{\mathscr{O}_{C_\epsilon}}(\mathfrak{m}_{\tilde{x}}/\mathfrak{m}_{\tilde{x}}^2, \Omega_{C_\epsilon}/\mathfrak{m}_{\tilde{x}}\Omega_{C_\epsilon}) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow \phi & & \\ 0 & \longrightarrow & \Omega_{C_\epsilon} & \longrightarrow & (\Omega_{C_\epsilon})_g & \longrightarrow & (\Omega_{C_\epsilon})_g/\Omega_{C_\epsilon} & \longrightarrow & 0 \end{array}$$

y que $\mathrm{Res}_{C_\epsilon,x}(\frac{df}{f}) = 1$.

6. Teorema: *Sea C una curva no singular sobre un cuerpo algebraicamente cerrado, x un punto cerrado y t un parámetro en x. Entonces,*

$$\mathrm{Res}_x\left(\frac{dt}{t^m}\right) = 0 \text{ para todo } m > 1.$$

Demostración. Sigamos notaciones anteriores. Tenemos

$$1 = \mathrm{Res}_{C_\epsilon,x}(\frac{d(t+\epsilon)}{t+\epsilon}) = \mathrm{Res}_{C_\epsilon,x}(\frac{d(t)}{t+\epsilon}) = \mathrm{Res}_{C_\epsilon,x}(\sum_{i=0}^{n-1}(\frac{(-\epsilon)^i}{t^{i+1}}\cdot dt) = \sum_{i=0}^{n-1}(-\epsilon)^i \mathrm{Res}_{C_\epsilon,x}(\frac{dt}{t^{i+1}})$$
$$= \sum_{i=0}^{n-1}(-\epsilon)^i \mathrm{Res}_x(\frac{dt}{t^{i+1}}).$$

Luego, $\mathrm{Res}_x(\frac{dt}{t^{i+1}}) = 0$, para todo $1 < i < n$.

□

14.6. Teorema de Mittag-Leffler

Concluyamos esta sección con la formulación clásica del teorema de Riemann-Roch.

Sea C una curva completa no singular sobre un cuerpo algebraicamente cerrado. En primer lugar, explicitemos las igualdades

$$H^0(C, \Omega_{C/k}) = \mathrm{Hom}_{\mathscr{O}_C}(\mathscr{O}_C, \Omega_{C/k}) = H^1(C, \mathscr{O}_C)^*.$$

Dada $w \in H^0(C, \Omega_{C/k})$, define el morfismo $\mathscr{O}_C \to \Omega_{C/k}$, $f \mapsto f \cdot w$, y este morfismo define la composición de morfismos

$$\begin{array}{ccc} H^1(C, \mathscr{O}_C) \to H^1(C, \Omega_{C/k}) & \overset{\mathrm{Res}}{\to} & k \\ \bar{l} \longmapsto \overline{l \cdot w} & \longmapsto & \mathrm{Res}(l \cdot w) \end{array}$$

con $\bar{l} \in \Gamma(C, \Sigma/\mathscr{O}_C)/\Sigma$. Explícitamente, $H^0(C, \Omega_{C/k}) = H^1(C, \mathscr{O}_C)^*$, $w \mapsto \mathrm{Res}(- \cdot w)$. Dualmente tenemos la igualdad $H^1(C, \mathscr{O}_C) = H^0(C, \Omega_{C/k})^*$, $\bar{l} \mapsto \mathrm{Res}(l \cdot -)$.

Por tanto, $\bar{l} = 0$ si y solo si $\mathrm{Res}(l \cdot w) = 0$ para toda $w \in H^0(C, \Omega_{C/k})$. Ahora bien, l son ciertos desarrollos de Laurent en ciertos puntos (y cero en los demás), luego $\bar{l} = 0$ si y solo si existe una función meromorfa $f \in \Sigma$ cuyos desarrollos de Laurent son los dichos y no tenga polos fuera de los puntos mencionados.

1. Teorema : *Dado $l \in \Gamma(C, \Sigma/\mathscr{O}_C)$, que son ciertos desarrollos de Laurent en ciertos puntos (y cero en los demás), existe una función meromorfa $f \in \Sigma$ cuyos desarrollos de Laurent son los dichos y no tenga polos fuera de los puntos mencionados si y solo si* $\mathrm{Res}(l \cdot w) = 0$*, para toda $w \in H^0(C, \Omega_{C/k})$.*

Consideremos la sucesión exacta

$$0 \to k \to \Sigma \xrightarrow{i} \Gamma(C, \Sigma/\mathscr{O}_C) \xrightarrow{\pi} H^1(C, \mathscr{O}_C) = H^0(C, \Omega_{C/k})^* \to 0$$

Sean $x_1, \ldots, x_r$ puntos cerrados de la curva C, $D = \sum_i m_i \cdot x_i$ con $m_i \geq 0$ y $V = \{l \in \Gamma(C, \Sigma/\mathscr{O}_C)\colon l_x \in \Sigma/\mathscr{O}_{C,x}$ es un desarrollo de Laurent de orden menor o igual que m_i si $x = x_i$ y $l_x = 0$ si $x \neq x_i$ para todo $i\}$. Tenemos la sucesión exacta

$$0 \to k \to H^0(C, \mathscr{L}_D) \xrightarrow{i} V \xrightarrow{\pi_{|V}} H^0(C, \Omega_{C/k})^*$$

Es decir, $H^0(C, \mathscr{L}_D)/k = \{l \in V\colon \pi(l) = 0\} = \{l \in V\colon \mathrm{Res}(l \cdot w) = 0$, para todo $w \in H^0(C, \Omega_{C/k})\}$. La dimensión de V es igual a $\mathrm{gr}D$. Si r es el rango de $\pi_{|V}$ tenemos que $h^0(C, \mathscr{L}_D) = \mathrm{gr}D - r + 1$ (y por el teorema de Riemann-Roch, $h^1(C, \mathscr{L}_D) = g - r$). Calculemos r como el rango de un sistema de ecuaciones lineales: Sea $w_1, \ldots, w_g$ una base de $H^0(C, \Omega_{C/k})$ y $e_1, \ldots, e_g$ la base dual, entonces $\pi(l) = (Res(l \cdot w_1), \ldots, Res(l \cdot w_g))$. Dados desarrollos de Laurent en los puntos x_i de orden m_i cualesquiera, $l = (l_{x_i}) = (\sum_{0 < j \leq m_i} a_{ij}/t_i^j)$, entonces

$$Res(l \cdot w_1) = \sum_i Res_{x_i}\Big(\sum_{0<j\leq m_i} \frac{a_{ij}}{t_i^j} \cdot w_1\Big) = \sum_i \sum_{0<j\leq m_i} a_{ij} \cdot Res_{x_i}\Big(\frac{w_1}{t_i^j}\Big) = 0$$

$$\cdots$$

$$Res(l \cdot w_g) = \sum_i Res_{x_i}\Big(\sum_{0<j\leq m_i} \frac{a_{ij}}{t_i^j} \cdot w_g\Big) = \sum_i \sum_{0<j\leq m_i} a_{ij} \cdot Res_{x_i}\Big(\frac{w_g}{t_i^j}\Big) = 0$$

es un sistema de ecuaciones lineales en las variables a_{ij} de rango r.

14.7. Morfismo traza

Sea $\pi\colon \widetilde{C} \to C$ un morfismo finito entre curvas completas. Denotemos $\widetilde{\mathscr{O}}$ y $\mathscr{O}$ los haces de anillos de $\widetilde{C}$ y C respectivamente, y sean $(\widetilde{\omega}, \widetilde{\mathrm{res}})$, (ω, res) pares dualizantes de $\widetilde{C}$ y C respectivamente.

1. Definición: Llamaremos traza al morfismo

$$\mathrm{Tr}\colon \pi_*\widetilde{\omega} \to \omega$$

que se corresponde con $\widetilde{\mathrm{res}}$ por las igualdades

$$\mathrm{Hom}_{\mathscr{O}}(\pi_*\widetilde{\omega},\omega) = H^1(C,\pi_*\widetilde{\omega})^* = H^1(\widetilde{C},\widetilde{\omega})^*.$$

Es decir, $\mathrm{Tr}\colon \pi_*\widetilde{\omega} \to \omega$ es el único morfismo tal que el morfismo inducido en cohomología $\mathrm{Tr}^*\colon H^1(C,\omega)^* \to H^1(\widetilde{C},\widetilde{\omega})^* = H^1(C,\pi_*\widetilde{\omega})^*$ cumple que

$$\mathrm{Tr}^*(\mathrm{res}) = \widetilde{\mathrm{res}}.$$

Dados los morfismos $\pi_1\colon C_1 \to C$, de morfismo traza $\mathrm{Tr}_1\colon \pi_{1*}\omega_{C_1} \to \omega_C$, el morfismo $\pi_2\colon C_2 \to C_1$ de morfismo traza $\mathrm{Tr}_{2/1}\colon \pi_{2*}\omega_{C_2} \to \omega_{C_1}$ y la composición $\pi_1\circ\pi_2\colon C_2 \to C$ de morfismo traza $\mathrm{Tr}_2\colon \pi_{1*}\pi_{2*}\omega_{C_2} \to \omega_C$, entonces

$$\mathrm{Tr}_2 = \mathrm{Tr}_1 \circ \pi_{1*}(\mathrm{Tr}_{2/1}),$$

porque $(\mathrm{Tr}_1\circ\pi_{1*}(\mathrm{Tr}_{2/1}))^*(\mathrm{res}_C) = (\pi_{1*}(\mathrm{Tr}_{2/1}))^*(\mathrm{res}_{C_1}) = \mathrm{res}_{C_2}$.

2. Teorema: *Se cumple el isomorfismo*

$$\pi_*\widetilde{\omega} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\omega),\ m \mapsto \mathrm{Tr}(-\cdot m),$$

donde $\mathrm{Tr}(-\cdot m)(b) := \mathrm{Tr}(b\cdot m)$*. Por tanto, dado* $\phi \in \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\omega) = \pi_*\tilde{\omega}$*, se cumple que* $\mathrm{Tr}(\phi) = \phi(1)$.

Si además C es no singular, entonces

$$\pi_*\widetilde{\omega} = \omega \otimes_{\mathscr{O}} (\pi_*\widetilde{\mathscr{O}})^*$$

Demostración. De las igualdades

$$\begin{aligned}\mathrm{Hom}_{\mathscr{O}}(\mathscr{M},\pi_*\widetilde{\omega}) &= \mathrm{Hom}_{\widetilde{\mathscr{O}}}(\pi^*\mathscr{M},\widetilde{\omega}) = H^1(\widetilde{C},\pi^*\mathscr{M})^* = H^1(C,\pi_*\pi^*\mathscr{M})^*\\ &= \mathrm{Hom}_{\mathscr{O}}(\pi_*\pi^*\mathscr{M},\omega) = \mathrm{Hom}_{\mathscr{O}}(\mathscr{M}\otimes_{\mathscr{O}}\pi_*\widetilde{\mathscr{O}},\omega)\\ &= \mathrm{Hom}_{\mathscr{O}}(\mathscr{M},\underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\omega))\end{aligned}$$

se deduce que $\pi_*\widetilde{\omega} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\omega)$.

Explicitemos este isomorfismo en términos del morfismo Tr. Consideremos $\mathscr{M} = \pi_*\widetilde{\omega}$. Como hemos visto, $\mathrm{Id} \in \mathrm{Hom}_{\mathscr{O}}(\pi_*\widetilde{\omega},\pi_*\widetilde{\omega})$ induce por un lado el morfismo natural $f\colon \pi^*\pi_*\widetilde{\omega} \to \widetilde{\omega}$, y por otro lado un morfismo $g\colon \pi_*\widetilde{\omega}\otimes\pi_*\widetilde{\mathscr{O}} = \pi_*\pi^*\pi_*\widetilde{\omega} \to \omega$ (que induce

la igualdad $\pi_*\widetilde{\omega} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}}, \omega)$), de modo que en $H^1(\tilde{C}, \pi^*\pi_*\widetilde{\omega})^* = H^1(C, \pi_*\pi^*\pi_*\widetilde{\omega})^*$, $f^*(\widetilde{res}) = g^*(res)$. Por tanto, $f^*(\mathrm{Tr}^*(res)) = g^*(res)$ y el triángulo

$$\begin{array}{ccc} \pi_*\pi^*\pi_*\widetilde{\omega} & \longrightarrow & \omega \\ \downarrow & \nearrow_{\mathrm{Tr}} & \\ \pi_*\widetilde{\omega} & & \end{array}$$

es conmutativo. Luego, el morfismo $\pi_*\widetilde{\omega} \otimes \pi_*\widetilde{\mathscr{O}} = \pi_*\pi^*\pi_*\widetilde{\omega} \to \omega$ asigna a $m \otimes b$ el elemento $\mathrm{Tr}(bm)$. Se concluye que $\pi_*\widetilde{\omega} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}}, \omega)$, $m \mapsto \mathrm{Tr}(- \cdot m)$.

La segunda parte se deduce de que el morfismo natural $\omega \otimes_{\mathscr{O}} (\pi_*\widetilde{\mathscr{O}})^* \to \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}}, \omega)$ es isomorfismo, porque ω es de línea. □

3. Supongamos que π es plano. Consideremos el morfismo natural

$$1 \otimes \mathrm{tr} \colon \pi_*\pi^*\omega = \omega \otimes_{\mathscr{O}} \pi_*\tilde{\mathscr{O}} \to \omega,\ w \otimes b \mapsto \mathrm{tr}(b)w.$$

Existe un (único) morfismo de $\pi_*\tilde{\mathscr{O}}$-módulos, $i \colon \omega \otimes_{\mathscr{O}} \pi_*\tilde{\mathscr{O}} \to \pi_*\tilde{\omega}$, de modo que $i^*(\widetilde{res}) = (1 \otimes \mathrm{tr})^*(res)$. En efecto, dar un morfismo de $\pi_*\tilde{\mathscr{O}}$-módulos, $i \colon \pi_*\pi^*\omega \to \pi_*\tilde{\omega}$ es equivalente a dar un morfismo de $\tilde{\mathscr{O}}$-módulos $\pi^*\omega \to \tilde{\omega}$, que está determinado por $i^*(\widetilde{res})$.

Por tanto, el triángulo

$$\begin{array}{ccc} \omega \otimes_{\mathscr{O}} \pi_*\tilde{\mathscr{O}} & \xrightarrow{1\otimes\mathrm{tr}} & \omega \\ & \searrow^{i} \quad \nearrow_{\mathrm{Tr}} & \\ & \pi_*\tilde{\omega} & \end{array}$$

es conmutativo e i es el único morfismo de $\pi_*\tilde{\mathscr{O}}$-módulos que compuesto con Tr es igual a $1 \otimes \mathrm{tr}$.

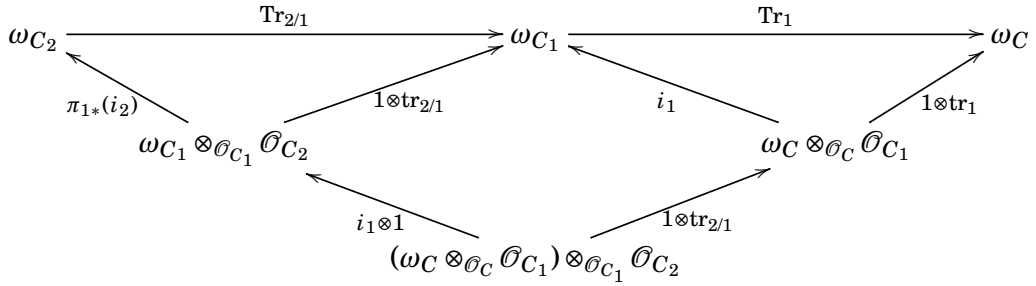
4. Proposición: *Vía la identificación $\pi_*\tilde{\omega} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\tilde{\mathscr{O}}, \omega)$, se cumple que $i(w \otimes b) = \mathrm{tr}(b \cdot -) \cdot w$, donde $(\mathrm{tr}(b \cdot -) \cdot w)(b') = \mathrm{tr}(bb') \cdot w$.*

Demostración. En efecto, $i(w \otimes b)(b') = \mathrm{Tr}(b' \cdot i(w \otimes b)) = \mathrm{Tr}(i(w \otimes bb')) = \mathrm{tr}(bb') \cdot w$. □

Dada una composición de morfismos finitos fielmente planos $A \to B \to C$, entonces con las notaciones obvias se cumple que $\mathrm{tr}_{B/A} \circ \mathrm{tr}_{C/B} = \mathrm{tr}_{C/A}$. Si $C_2 \xrightarrow{\pi_2} C_1 \xrightarrow{\pi_1} C$ es una composición de morfismos finitos planos entre curvas completas y $i_1 \colon \omega_C \to \pi_{1*}\omega_{C_1}$, $i_{1/2} \colon \omega_{C_1} \to \pi_{2*}\omega_{C_2}$ y $i_2 \colon \omega_C \to (\pi_1 \circ \pi_2)_*\omega_{C_2}$ los morfismos naturales recién definidos, entonces la composición

$$\omega_C \xrightarrow{i_1} \pi_{1*}\omega_{C_1} \xrightarrow{\pi_{1*}(i_2)} (\pi_1 \circ \pi_2)_*\omega_{C_2}$$

es el morfismo i_2, como se deduce del diagrama (simplificado) conmutativo siguiente



Sea $\pi\colon \widetilde{C}\to C$ un morfismo entre curvas no singulares sobre un cuerpo k algebraicamente cerrado y supongamos que el morfismo π es separable, es decir, el morfismo inducido entre sus cuerpos de fracciones, $\Sigma\to\widetilde{\Sigma}$, es separable.

5. Observación: El morfismo $\mathrm{Tr}\colon \pi_*\widetilde{\omega}\to\omega$ induce un morfismo

$$\mathrm{Tr}\colon \bigoplus_{x\in C}(\widetilde{\omega}_{\widetilde{\Sigma}}/\pi_*\widetilde{\omega})_x=\bigoplus_{\tilde{x}\in\tilde{C}}\widetilde{\omega}_{\widetilde{\Sigma}}/\widetilde{\omega}_{\tilde{x}}\longrightarrow\bigoplus_{x\in C}\omega_\Sigma/\omega_x$$

o equivalentemente, un morfismo $\mathrm{Tr}_x\colon \bigoplus_{\tilde{x}\mapsto x}\widetilde{\omega}_{\widetilde{\Sigma}}/\widetilde{\omega}_{\tilde{x}}\longrightarrow\omega_\Sigma/\omega_x$, para cada $x\in C$. De la igualdad $\mathrm{Tr}^*(\mathrm{res})=\widetilde{\mathrm{res}}$ se deduce que

$$\sum_{\tilde{x}\mapsto x}\widetilde{\mathrm{res}}_{\tilde{x}}(\theta)=\mathrm{res}_x(\mathrm{Tr}_x(\theta))$$

para toda $\theta\in\bigoplus_{\tilde{x}\mapsto x}\widetilde{\omega}_{\widetilde{\Sigma}}/\widetilde{\omega}_{\tilde{x}}$.

Vamos a probar que el morfismo natural $i'\colon \Omega_C\otimes\pi_*\tilde{\mathcal{O}}\to\pi_*\Omega_{\tilde{C}}$, $i'(da\otimes b):=bda$ es igual a i. Supongamos en primer lugar que $\Sigma\to\widetilde{\Sigma}$ es una extensión de Galois de grupo G. Tanto i como i' conmutan con la acción natural de G y son morfismos de $\pi_*\tilde{\mathcal{O}}$-módulos. Por tanto, existe $a\in\Sigma$ tal que $i'=a\cdot i$. Sea $x\in C$ un punto que no sea un punto rama de π y $\tilde{x}$, tal que $\pi(\tilde{x})=x$. Sea t un parámetro en x, que lo es en todos los puntos $g\cdot\tilde{x}$, para todo $g\in G$. Observemos que

$$(\Omega_\Sigma\otimes_\Sigma\tilde{\Sigma})/\Omega_{\mathcal{O}_x}\otimes(\pi_*\tilde{\mathcal{O}})_x=\oplus_{g\in G}(\Omega_\Sigma\otimes_\Sigma\tilde{\Sigma})/\Omega_{\mathcal{O}_x}\otimes\tilde{\mathcal{O}}_{g\tilde{x}}$$

y que el morfismo inducido $1\otimes\mathrm{tr}\colon \oplus_{g\in G}(\Omega_\Sigma\otimes_\Sigma\tilde{\Sigma})/\Omega_{\mathcal{O}_x}\otimes\tilde{\mathcal{O}}_{g\tilde{x}}\to\Omega_\Sigma/\Omega_{\mathcal{O}_x}$, verifica que $1\otimes\mathrm{tr}(dt/t,0,\dots,0)=dt/t$. Sea $\theta\in(\Omega_\Sigma\otimes_\Sigma\tilde{\Sigma})/\Omega_{\tilde{\mathcal{O}}}\otimes\pi_*\tilde{\mathcal{O}}$ nula en todo punto salvo en x, donde sea $(dt/t,0,\dots,0)$. Entonces, $i^*(\widetilde{Res})(\theta)=(1\otimes\mathrm{tr})^*(Res)(\theta)=Res_x(dt/t)=1$ y por tanto $i'^*(\widetilde{Res})(\theta)=a(x)$. Por otra parte, $i'^*(\widetilde{Res})(\theta)=\widetilde{Res}(i'(\theta))=\widetilde{Res}_{\tilde{x}}(dt/t)=1$. Luego, $a(x)=1$ para todo punto x que no sea un punto rama, luego $a=1$ e $i'=i$.

Ahora en general. Sea $\tilde{\tilde{\Sigma}}$ el cuerpo de descomposición de la extensión separable $\Sigma \to \tilde{\Sigma}$. Sea $\tilde{\tilde{C}}$ la variedad de Riemann de $\tilde{\tilde{\Sigma}}$ y $\tilde{\pi}\colon \tilde{\tilde{C}} \to \tilde{C}$ el morfismo inducido por el morfismo $\tilde{\Sigma} \hookrightarrow \tilde{\tilde{\Sigma}}$. Del diagrama

$$\Omega_C \xrightarrow{\ i\ } \tilde{\pi}_*\Omega_{\tilde{C}} \longrightarrow (\pi\circ\tilde{\pi})_*\Omega_{\tilde{\tilde{C}}}$$

$$b_1 db_2 \longmapsto b_1 db_2$$

$$a_1 da_2 \longmapsto a_1 da_2$$

se concluye que $i(a_1 da_2) = a_1 da_2$.

Podemos explicitar el morfismo $Tr\colon \pi_*\Omega_{\tilde{\mathcal{O}}} \to \Omega_{\mathcal{O}}$:

$$Tr(bda) = Tr(i(da\otimes b)) = (1\otimes tr)(da\otimes b) = tr(b)da,$$

entonces en el punto genérico $Tr\colon \Omega_{\tilde{\Sigma}} = \tilde{\Sigma}\otimes\Omega_\Sigma \to \Omega_\Sigma$, $Tr(bda) = tr(b)da$. Por tanto, el diagrama

$$\begin{array}{ccc} \pi_*\Omega_{\tilde{C}} & \xrightarrow{\quad Tr\quad} & \Omega_C \\ & {\scriptstyle \sum_{g\in \mathrm{Hom}_C(\tilde{\tilde{C}},\tilde{C})} g^*} \searrow \quad \swarrow & \\ & (\pi\circ\tilde{\pi})_*\Omega_{\tilde{\tilde{C}}} & \end{array}$$

es conmutativo y $Tr(w) = \sum_{g\in \mathrm{Hom}_C(\tilde{\tilde{C}},\tilde{C})} g^*(w)$.

6. Proposición: *Sea C una curva no singular sobre un cuerpo algebraicamente cerrado, x un punto cerrado y t un parámetro en x. Entonces,*

$$\mathrm{Res}_x\left(\frac{dt}{t^n}\right) = 0 \text{ para todo } n > 1.$$

Demostración. Consideremos el morfismo $\pi\colon C \to \mathbb{P}^1$, inducido por la inclusión $k(t) \hookrightarrow \Sigma_C$. Denotemos $o = \pi(x)$. Sea θ el elemento de $\bigoplus_{y\in C} \Omega_\Sigma/\Omega_{\mathcal{O}_y}$ que es $\frac{dt}{t^n}$ en x y cero en las demás componentes. Sea $\tilde{\Sigma}$ el cuerpo de descomposición de la extensión de cuerpos $\Sigma_{\mathbb{P}^1} \to \Sigma$, $\tilde{C}$ la variedad de Riemann de $\tilde{\Sigma}$, $\tilde{\pi}\colon \tilde{C} \to C$ el morfismo natural, $\tilde{x} \in \tilde{C}$ tal que $\tilde{\pi}(\tilde{x}) = x$, $G = \mathrm{Aut}_{\mathbb{P}^1}(\tilde{C})$, $D = \{g \in G\colon g(\tilde{x}) = \tilde{x}\}$ y $H = \mathrm{Aut}_C(\tilde{C})$. Observemos que θ en $\bigoplus_{\tilde{y}\in\tilde{C}} \Omega_{\tilde{\Sigma}}/\Omega_{\tilde{\mathcal{O}}_{\tilde{y}}}$ es igual a $\frac{dt}{t^n}$ en $g(\tilde{x})$ para todo $\bar{g} \in H/D$ y cero en los demás puntos, luego

$\sum_{\bar{g}\in G/H} g^*\theta$ es igual a $\frac{dt}{t^n}$ en $g(\tilde{x})$ para todo $\bar{g}\in G/D$ y es cero en los demás puntos. Por tanto, $Tr(\theta)$ es igual a $\frac{dt}{t^n}$ en o y es cero en los demás puntos de $\mathbb{P}^1$ y

$$\mathrm{Res}_x\left(\frac{dt}{t^n}\right)=\mathrm{Res}_C(\theta)=\mathrm{Res}_{\mathbb{P}^1}(Tr(\theta))=\mathrm{Res}_o\left(\frac{dt}{t^n}\right)$$

luego basta probar el enunciado para la recta proyectiva. Sea $h_\lambda\colon\mathbb{P}^1\to\mathbb{P}^1$ el automorfismo definido por $h_\lambda(\alpha)=\lambda\cdot\alpha$. Por la canonicidad del residuo, ha de ser invariante por automorfismos, luego

$$\mathrm{Res}_o\left(\frac{dt}{t^n}\right)=\mathrm{Res}_o\left(\frac{d(\lambda\cdot t)}{(\lambda\cdot t)^n}\right)=\frac{1}{\lambda^{n-1}}\mathrm{Res}_o\left(\frac{dt}{t^n}\right)$$

y se concluye que $\mathrm{Res}_o\left(\frac{dt}{t^n}\right)=0$ para $n>1$. □

14.8. Dualizante de curvas singulares

Supondremos el cuerpo base k algebraicamente cerrado.

1. Proposición: *Sea C una curva completa y $\pi\colon\widetilde{C}\to C$ el morfismo de desingularización. Sea ω módulo dualizante de C. Entonces, para cada abierto U de C*

$$\omega(U)=\{w\in\Omega_{\Sigma/k}\colon \sum_{\pi(\tilde{x})=x}\mathrm{Res}_{\tilde{x}}(f\cdot w)=0,\ \textit{para todo } x\in U \textit{ y toda } f\in\mathscr{O}_x\}.$$

Demostración. $\pi_*\Omega_{\widetilde{C}}=\underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\omega)$, por el Teorema 14.7.2 y por ser $\widetilde{C}$ no singular. Localizando en el punto genérico, se obtiene que ω_Σ se identifica con Ω_Σ, de modo que ω es un subhaz de Ω_Σ y el morfismo traza $\pi_*\Omega_{\widetilde{C}}\to\omega$ es una igualdad en el punto genérico. De la Proposición 14.5.3 se obtiene que

$$\omega(U)=\{w\in\Omega_{\Sigma/k}\colon \mathrm{res}_x(a\cdot w)=0,\ \text{para todo } x\in U \text{ y todo } a\in\mathscr{O}_x\}$$

y se concluye porque $\mathrm{res}_x(a\cdot w)=\sum_{\tilde{x}\mapsto x}\mathrm{Res}_{\tilde{x}}(a\cdot w)$ (véase la Observación 14.7.5). □

2. Proposición: *Sea $\pi\colon\widetilde{C}\to C$ un morfismo finito y birracional entre curvas completas, y sea $\widetilde{C}$ no singular. Se tiene un isomorfismo natural*

$$\omega/\pi_*\Omega_{\widetilde{C}}\simeq(\pi_*\widetilde{\mathscr{O}}/\mathscr{O})^*$$

donde $*$ denota el dual sobre el cuerpo base k.

Si ω es de línea y α es el ideal conductor (es decir, el anulador de $\pi_*\widetilde{\mathscr{O}}/\mathscr{O}$), entonces $\pi_*\Omega_{\widetilde{C}}=\alpha\cdot\omega$ y

$$l(\mathscr{O}/\alpha)=l(\pi_*\widetilde{\mathscr{O}}/\mathscr{O}).$$

Demostración. El morfismo

$$\begin{array}{lcl} \omega_x/(\pi_*\Omega_{\widetilde{C}})_x & \xrightarrow{R} & \mathrm{Hom}_k((\pi_*\widetilde{\mathscr{O}})_x/\mathscr{O}_x,k) \\ \bar{w} & \mapsto & R(\bar{w})\colon \bar{f} \overset{\text{def}}{\longmapsto} \sum\limits_{\tilde{x}\mapsto x} \mathrm{Res}_{\tilde{x}}(fw) \end{array}$$

es inyectivo, para todo x. Para concluir que el morfismo R es un isomorfismo basta probar que $h^0(\omega/\pi_*\Omega_{\widetilde{C}}) = h^0(\pi_*\widetilde{\mathscr{O}}/\mathscr{O})$. Ahora bien,

$$h^0(\omega/\pi_*\Omega_{\widetilde{C}}) = \chi(\omega/\pi_*\Omega_{\widetilde{C}}) = \chi(\omega) - \chi(\pi_*\Omega_{\widetilde{C}}) = -\chi(\mathscr{O}) + \chi(\pi_*\widetilde{\mathscr{O}}) = \chi(\pi_*\widetilde{\mathscr{O}}/\mathscr{O}) = h^0(\pi_*\widetilde{\mathscr{O}}/\mathscr{O}).$$

Si ω es de línea, entonces $\pi_*\Omega_{\widetilde{C}} = \underline{\mathrm{Hom}}_{\mathscr{O}}(\pi_*\widetilde{\mathscr{O}},\mathscr{O}) \otimes_{\mathscr{O}} \omega = \alpha \otimes_{\mathscr{O}} \omega = \alpha \cdot \omega$. Por tanto, $l(\mathscr{O}/\alpha) = l(\omega/\alpha\cdot\omega) = l(\omega/\pi_*\Omega_{\widetilde{C}}) = l((\pi_*\widetilde{\mathscr{O}}/\mathscr{O})^*) = h^0((\pi_*\widetilde{\mathscr{O}}/\mathscr{O})^*) = h^0(\pi_*\widetilde{\mathscr{O}}/\mathscr{O}) = l(\pi_*\widetilde{\mathscr{O}}/\mathscr{O})$. □

Dualizante de curvas planas

Toda curva es birracional a una curva plana. Por ello, vamos a computar el dualizante de una curva plana.

3. Proposición: *Sea $C \hookrightarrow \mathbb{P}^2$ una curva proyectiva plana e irreducible de grado n. Se cumple que*

$$\omega_C = \mathscr{O}_C(n-3).$$

Demostración. Sea $p_n(x_0,x_1,x_2)$ el polinomio homogéneo de grado n que define a la curva C. Tensando la sucesión exacta

$$(*) \qquad 0 \to \mathscr{O}_{\mathbb{P}^2}(-n) \xrightarrow{p_n\cdot} \mathscr{O}_{\mathbb{P}^2} \to i_*\mathscr{O}_C \to 0$$

por $\mathscr{O}_{\mathbb{P}^2}(n-3)$ obtenemos la sucesión exacta

$$0 \to \mathscr{O}_{\mathbb{P}^2}(-3) \xrightarrow{\cdot p_n} \mathscr{O}_{\mathbb{P}^2}(n-3) \to i_*\mathscr{O}_C(n-3) \to 0$$

De la sucesión exacta larga de cohomología y del cómputo de la cohomología de los $\mathscr{O}_{\mathbb{P}^2}(n)$, obtenemos que $h^1(C,\mathscr{O}_C(n-3)) = 1$. Tenemos, pues, un morfismo $\mathscr{O}_C(n-3) \to \omega_C$. Este morfismo es isomorfismo: en efecto, para todo $m \geq 0$, $h^0(C,\mathscr{O}_C(n-3)(m)) = h^0(C,\mathscr{O}_C(n+m-3)) = h^1(C,\mathscr{O}_C(-m))$, como se deduce de la sucesión exacta (*) tensando por $\mathscr{O}_{\mathbb{P}^2}(m)$ y $\mathscr{O}_{\mathbb{P}^2}(-m)$. Teniendo en cuenta la igualdad $h^1(C,\mathscr{O}_C(-m)) = h^0(C,\omega_C(m))$, obtenemos que $h^0(C,\mathscr{O}_C(n-3)(m)) = h^0(C,\omega_C(m))$, para todo $m \geq 0$, y se concluye. □

Sea $p(x,y)=0$ la ecuación afín de la curva en las coordenadas afines $x=\frac{x_1}{x_0}$, $y=\frac{x_2}{x_0}$. Supongamos que $\partial p(x,y)/\partial y = p_y(x,y)$ es un polinomio de grado $n-1$. La proyección de la curva C en el eje X es separable, es decir, el morfismo $k(x)\hookrightarrow\Sigma$ es separable. Tenemos $\Sigma = k(x,\bar{y})$, con $p(x,\bar{y})=0$. Denotemos $\pi\colon C\to\mathbb{P}^1$ dicho morfismo. Sea $U=\operatorname{Spec}k[x]$ y $V=\pi^{-1}(U)=\operatorname{Spec}B$. Por 3.8.35 (donde no es necesario que el dominio B sea de Dedekind)

$$\operatorname{Hom}_{k[x]}(B,k[x]) = \langle \frac{1}{p_y(x,\bar{y})},\dots,\frac{\bar{y}^{n-1}}{p_y(x,\bar{y})}\rangle\cdot \operatorname{tr}.$$

Teniendo en cuenta que $\pi_*\omega_C = \underline{\operatorname{Hom}}_{\mathscr{O}_{\mathbb{P}^1}}(\pi_*\mathscr{O}_C,\mathscr{O}_{\mathbb{P}^1})\otimes_{\mathscr{O}_{\mathbb{P}^1}}\omega_{\mathbb{P}^1}$ se concluye que

$$\omega_C(V) = \left\{ \frac{q(x,\bar{y})}{p_y(x,\bar{y})}dx,\ \text{con } q(x,y) \text{ de grado menor o igual que } n-1 \text{ en } y \right\}.$$

Efectuando un cálculo similar en el abierto $U'=\operatorname{Spec}k[\frac{1}{x}]$ se obtiene que

$$\omega_C(C) = \left\{ \frac{q(x,\bar{y})}{p_y(x,\bar{y})}dx,\ \text{con } q(x,y) \text{ de grado menor o igual que } n-3 \right\}$$

y su dimensión ha de coincidir con $h^1(C,\mathscr{O}_C)$. Explícitamente, tenemos que

$$\omega_C \overset{x_0^{n-3}\cdot}{=} \mathscr{O}_C(n-3)\cdot\frac{dx}{p_y(x,\bar{y})}.$$

Por último, si $\widetilde{\pi}\colon \widetilde{C}\to C$ es el morfismo de desingularización de C y α es el conductor, sabemos que $\widetilde{\pi}_*\Omega_{\widetilde{C}/k} = \alpha\cdot\omega_C$. De la sucesión exacta

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widetilde{\pi}_*\Omega_{\widetilde{C}/k} & \longrightarrow & \omega_C & \longrightarrow & \widetilde{\pi}_*\Omega_{\widetilde{C}/k}/\omega_C & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & \alpha\cdot\omega_C = \alpha\cdot\mathscr{O}_C(n-3) & \longrightarrow & \mathscr{O}_C(n-3) & \longrightarrow & \mathscr{O}_C(n-3)/\alpha\cdot\mathscr{O}_C(n-3) & \longrightarrow & 0
\end{array}$$

obtenemos que

$$\Gamma(\widetilde{C},\Omega_{\widetilde{C}/k}) = \left\{ \frac{q(x,\bar{y})}{p_y(x,\bar{y})}dx,\ \text{con } q(x,y)\in\alpha \text{ de grado menor o igual que } n-3 \right\}.$$

14.9. Aplicaciones de la teoría de dualidad

14.9.1. Teorema de Hurwitz

1. Definición: Un morfismo de esquemas $f\colon X\to Y$ se dice plano si para todo $x\in X$ existen entornos afines U de x y V de $f(x)$, con $f(U)\subseteq V$, tales que el morfismo $\mathscr{O}_Y(V)\to\mathscr{O}_X(U)$ es plano.

Es fácil ver que f es plano si y solo si para todo $x \in X$, el morfismo $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ es plano. Se dice que f es fielmente plano si es plano y epiyectivo.

Sea $\pi\colon \widetilde{C} \to C$ un morfismo finito entre curvas completas y no singulares. El haz de funciones de C es localmente un anillo de ideales principales, y los anillos de secciones de $\widetilde{\mathscr{O}}$ no tienen torsión, luego π es un morfismo plano. En conclusión, para cada abierto afín U de C, el morfismo $\pi^{-1}(U) \to U$ es un revestimiento.

Sea $\widetilde{x} \in \widetilde{C}$ un punto cerrado y $x = \pi(\widetilde{x})$. Se dice que $\widetilde{x}$ es un punto de ramificación de π, si $(\widetilde{\mathscr{O}}_{\widetilde{x}}/\mathfrak{m}_x\widetilde{\mathscr{O}}_{\widetilde{x}})$ no es una $\mathscr{O}_x/\mathfrak{m}_x$-álgebra separable. Los puntos de ramificación coinciden con los puntos donde el haz de diferenciales relativas $\Omega_{\widetilde{C}/C}$ es no nulo: en efecto, $(\Omega_{\widetilde{C}/C})_{\widetilde{x}}$ es un $\widetilde{\mathscr{O}}_{\widetilde{x}}$-módulo nulo si y solo si, por Nakayama, lo es

$$(\Omega_{\widetilde{C}/C})_{\widetilde{x}} \otimes_{\mathscr{O}_x} \mathscr{O}_x/\mathfrak{m}_x = \Omega_{(\widetilde{\mathscr{O}}_{\widetilde{x}}/\mathfrak{m}_x\widetilde{\mathscr{O}}_{\widetilde{x}})/(\mathscr{O}_x/\mathfrak{m}_x)}$$

es decir, si y solo si$(\widetilde{\mathscr{O}}_{\widetilde{x}}/\mathfrak{m}_x\widetilde{\mathscr{O}}_{\widetilde{x}})$ es una $\mathscr{O}_x/\mathfrak{m}_x$-álgebra separable.

2. Proposición: *Sea $\pi\colon \widetilde{C} \to C$ un morfismo finito entre curvas completas y no singulares. Sea $D = \sum n_x \cdot x$ un divisor en C y $\mathscr{L}_D$ el haz de línea asociado. Entonces*

$$\pi^* \mathscr{L}_D = \mathscr{L}_{\pi^{-1}D}$$

donde $\pi^{-1}D = \sum n_x \cdot \pi^{-1}(x)$ y $\pi^{-1}(x)$ son los puntos de la fibra de x, contados con su multiplicidad.

Demostración. Sea $t \in \Sigma$ un generador de $\mathfrak{m}_x$ en un entorno de x. Sabemos que $\mathscr{L}_D = t^{-n_x} \cdot \mathscr{O}_U$ en un entorno afín U de x tal que $D \cap U = x$ ó $D \cap U = \emptyset$. Sea $V = \pi^{-1}(U)$, que es un abierto afín de $\widetilde{C}$, y $\pi^*\colon \mathscr{O}(U) \hookrightarrow \widetilde{\mathscr{O}}(V)$ el morfismo inducido entre los anillos de funciones. Entonces

$$(\pi^*(t)) = t \cdot \widetilde{\mathscr{O}}(V) = \mathfrak{m}_{\widetilde{x}_1}^{n_1} \cdots \mathfrak{m}_{\widetilde{x}_r}^{n_r}$$

donde $\widetilde{x}_1, \ldots, \widetilde{x}_r$ son los puntos de la fibra de x y $n_1, \ldots, n_r$ son la multiplicidad con que aparece cada uno. Por tanto,

$$\begin{aligned}(\pi^*(\mathscr{L}_D))_{|V} &= \pi^*_{|V}((\mathscr{L}_D)_{|U}) = \pi^*_{|V}(t^{-n_x} \cdot \mathscr{O}_U) = t^{-n_x} \cdot \mathscr{O}_U \otimes_{\mathscr{O}_U} \widetilde{\mathscr{O}}_V \\ &= (\mathfrak{m}_{\widetilde{x}_1}^{n_1} \cdots \mathfrak{m}_{\widetilde{x}_r}^{n_r})^{-n_x} = (\mathscr{L}_{\pi^{-1}D})_{|V}\end{aligned}$$

con lo que se concluye.

□

3. Teorema de Hurwitz: *Sea $\pi\colon \widetilde{C} \to C$ un morfismo finito entre curvas completas no singulares, separable entre sus cuerpos de funciones. El módulo de las diferenciales relativas $\Omega_{\widetilde{C}/C}$ es de torsión y*

$$2\widetilde{g} - 2 = \operatorname{gr}\pi \cdot (2g - 2) + \dim_k \Gamma(\widetilde{C}, \Omega_{\widetilde{C}/C})$$

donde $\widetilde{g}$ y g son los géneros de $\widetilde{C}$ y C respectivamente.

Demostración. Con las notaciones obvias, $(\Omega_{\widetilde{C}/C})_{\widetilde{\Sigma}} = \Omega_{\widetilde{\Sigma}/\Sigma} = 0$, por ser $\Sigma \to \widetilde{\Sigma}$ separable. Por tanto, $\Omega_{\widetilde{C}/C}$ es un haz coherente cuya fibra en el punto genérico es cero, luego es de torsión.

Consideremos la sucesión exacta

$$\pi^*\Omega_C \xrightarrow{\pi^*} \Omega_{\widetilde{C}} \to \Omega_{\widetilde{C}/C} \to 0$$

El morfismo π^* ha de ser inyectivo, porque es isomorfismo en el punto genérico y son módulos sin torsión.

Denotemos por $\widetilde{K}$ y K divisores canónicos de $\widetilde{C}$ y C. Tenemos la sucesión exacta

$$0 \to \mathscr{L}_{\pi^{-1}K} \to \mathscr{L}_{\widetilde{K}} \to \Omega_{\widetilde{C}/C} \to 0$$

Tomando características, tenemos $\chi(\mathscr{L}_{\widetilde{K}}) = \chi(\mathscr{L}_{\pi^{-1}K}) + \dim_k \Gamma(\widetilde{C}, \Omega_{\widetilde{C}/C})$. Por Riemann-Roch esta igualdad equivale a que $\operatorname{gr}(\widetilde{K}) = \operatorname{gr}(\pi^{-1}K) + \dim_k \Gamma(\widetilde{C}, \Omega_{\widetilde{C}/C})$. Teniendo en cuenta que $\operatorname{gr}(\pi^{-1}K) = \operatorname{gr}(\pi)\cdot\operatorname{gr}\widetilde{K}$, se concluye la fórmula de Hurwitz.

□

4. Definición: Diremos que un morfismo finito $\pi\colon \widetilde{C} \to C$ es un revestimiento no ramificado si es separable entre sus cuerpos de funciones y no tiene puntos de ramificación (es decir, las diferenciales relativas $\Omega_{\widetilde{C}/C}$ son nulas).

5. Corolario: *La recta proyectiva no tiene revestimientos no ramificados, salvo los isomorfismos. (Se dice que $\mathbb{P}^1$ es simplemente conexa).*

Demostración. Sea $\pi\colon C \to \mathbb{P}^1$ un revestimiento no ramificado. Por Hurwitz, $2g-2 = \operatorname{gr}\pi\cdot(2\cdot 0-2)$, luego $g=0$ y $\operatorname{gr}\pi = 1$. □

6. Definición: Sea $p>0$ un número primo y X un $\mathbb{Z}/p\mathbb{Z}$-esquema reducido. Denotaremos por X_p al espacio anillado $(X, \mathscr{O}_X^p)$ donde $\mathscr{O}_X^p(U) := \mathscr{O}_X(U)^p = \{a^p \in \mathscr{O}_X(U), \forall a \in \mathscr{O}_X(U)\}$, que resulta ser un haz en X.

Dado una $\mathbb{Z}/p\mathbb{Z}$-álgebra A se cumple que $\operatorname{Spec}A = \operatorname{Spec}A^p$, por tanto X_p es un esquema. Si k es un cuerpo de característica p perfecto y X es un k-esquema entonces X_p es un k-esquema.

Existe un morfismo natural $i\colon X \to X_p$, que es la identidad entre los espacios topológicos subyacentes y entre los haces de anillos las inclusiones $\mathscr{O}_X(U)^p \hookrightarrow \mathscr{O}_X(U)$ obvias. Si X es un k-esquema, siendo k un cuerpo perfecto de característica p, entonces i es un morfismo de k-esquemas.

Existe también un isomorfismo natural de $\mathbb{Z}/p\mathbb{Z}$-esquemas $X_p \to X$, que es la identidad entre los espacios topológicos y entre los haces de anillos los isomorfismos $\mathcal{O}_X(U) \to \mathcal{O}_X(U)^p$, $a \mapsto a^p$. Ahora bien, si X es un k-esquema sobre un cuerpo k-perfecto, este morfismo no es un morfismo de k-esquemas.

7. Proposición : *Todo morfismo $f : C \to C'$ entre curvas completas y no singulares, sobre un cuerpo perfecto de característica p, factoriza a través de una composición*

$$C \xrightarrow{i} C_p \xrightarrow{i} C_{p^2} \to \cdots \xrightarrow{i} C_{p^n} \xrightarrow{f'} C'$$

donde $C_{p^j} = (C_{p^{j-1}})_p$ para cada j, y f' es separable.

Demostración. Sean Σ, Σ' los cuerpos de fracciones de C, C‘. La extensión $\Sigma' \to \Sigma$ factoriza a través de una composición $\Sigma' \to K \to \Sigma$ donde $\Sigma' \to K$ es separable y $K \to \Sigma$ es puramente inseparable. Para concluir basta ver que $K = \Sigma^{p^n}$.

Sea $p^n = \dim_K \Sigma$. Entonces $\Sigma^{p^n} \subseteq K$ y concluiremos la igualdad si probamos que $\dim_{\Sigma^{p^n}} \Sigma = p^n$. Sea $x \in \Sigma$ un elemento trascendente. Del diagrama

$$\begin{array}{ccc} \Sigma^{p^n} & \longrightarrow & \Sigma \\ \uparrow & & \uparrow \\ k(x)^{p^n} & \longrightarrow & k(x) \end{array}$$

y de las igualdades $\dim_{k(x)} \Sigma = \dim_{k(x)^{p^n}} \Sigma^{p^n}$ y $\dim_{k(x)^{p^n}} k(x) = p^n$, deducimos la igualdad $\dim_{\Sigma^{p^n}} \Sigma = p^n$ buscada.

□

8. Teorema de Lüroth: *Sea k un cuerpo algebraicamente cerrado. Si L es una k-subextensión de $k(x)$, entonces $L = k(p(x))$, para cierto $p(x) \in k(x)$.*

Demostración. La inclusión $L \subset k(x)$ induce un morfismo entre las variedades de Riemann

$$f : \mathbb{P}^1 \to C'$$

Supongamos que $L \hookrightarrow k(x)$ es una extensión finita separable. Por el teorema de Hurwitz, $2 \cdot 0 - 2 = \operatorname{gr} f \cdot (2g' - 2) + \dim_k \Gamma(\mathbb{P}^1_{p^n}, \Omega_{\mathbb{P}^1_{p^n}/C'})$. Por tanto, $g' = 0$ y $C' = \mathbb{P}^1$. Es decir, $L = k(p(x))$.

Si $L \hookrightarrow k(x)$ no es una extensión finita separable, entonces $\operatorname{car} k = p$ y f factoriza, por la proposición anterior, por una composición

$$\mathbb{P}^1 \to \mathbb{P}^1_{p^n} \xrightarrow{f'} C'$$

donde $\mathbb{P}^1_{p^n}$ es isomorfo a $\mathbb{P}^1$ y f' es separable. Como $\mathbb{P}^1_{p^n}$ es un k-esquema isomorfo a $\mathbb{P}_1$, concluimos por el párrafo anterior.

□

14.9.2. Proyectividad de las curvas completas no singulares

Las curvas las supondremos completas no singulares sobre un cuerpo algebraicamente cerrado.

9. Lema : *Sea C una curva completa no singular sobre un cuerpo algebraicamente cerrado.*

1. *La condición necesaria y suficiente para que la serie lineal $\Gamma(C,\mathscr{L}_D)$ no tenga puntos base es que $h^0(C,\mathscr{L}_{D-x}) < h^0(C,\mathscr{L}_D)$, para todo punto cerrado $x \in C$.*

2. *La condición necesaria y suficiente para que $\mathscr{L}_D$ sea un haz de línea muy amplio es que $h^0(C,\mathscr{L}_D) = h^0(C,\mathscr{L}_{D-x-y}) + 2$ para cualquier pareja de puntos cerrados $x, y \in C$.*

Demostración. 1. Observemos que $\mathfrak{m}_x\mathscr{L}_D = \mathscr{L}_{D-x}$. Las secciones globales de $\mathfrak{m}_x\mathscr{L}_D$ se identifican con las secciones $s \in \Gamma(C,\mathscr{L}_D)$ tales que en gérmenes pertenezcan a $\mathfrak{m}_x\mathscr{L}_D$. Es decir,

$$H^0(C,\mathfrak{m}_x\mathscr{L}_D) = \{s \in H^0(C,\mathscr{L}_D)\colon s_x \in \mathfrak{m}_x(\mathscr{L}_D)_x\} = \{s \in H^0(C,\mathscr{L}_D)\colon s(x) = 0\}.$$

Por tanto, $\Gamma(C,\mathfrak{m}_x\cdot\mathscr{L}_D) \underset{\neq}{\subset} \Gamma(C,\mathscr{L}_D)$ si y solo si existe $s \in H^0(C,\mathscr{L}_D)$ tal que $s(x) \neq 0$, es decir, si y solo si x no es un punto base.

2. Observemos que $\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D = \mathscr{L}_{D-x-y}$ y que $\mathscr{L}_D/\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D \simeq \mathscr{O}_C/\mathfrak{m}_x\cdot\mathfrak{m}_y$, luego $h^0(C,\mathscr{L}_D/\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D) = 2$. Ahora ya, de la sucesión exacta

$$0 \to H^0(C,\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D) \to H^0(C,\mathscr{L}_D) \to H^0(C,\mathscr{L}_D/\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D)$$

se concluye que $H^0(C,\mathscr{L}_D) \to H^0(C,\mathscr{L}_D/\mathfrak{m}_x\cdot\mathfrak{m}_y\cdot\mathscr{L}_D)$ es epiyectivo (es decir, $\mathscr{L}_D$ es muy amplio) si y solo si $h^0(C,\mathscr{L}_D) = h^0(C,\mathscr{L}_{D-x-y}) + 2$.

□

10. Proposición: *Sea g el género geométrico de C.*

1. *Si $\operatorname{gr} D > 2g$, entonces $\mathscr{L}_D$ es muy amplio.*

2. Si $\mathrm{gr}\, D = 2g$*, entonces las secciones globales de* $\mathscr{L}_D$ *no tienen puntos base.*

Demostración. 1. Observemos que $h^1(C, \mathscr{L}_D) = h^0(C, \mathscr{L}_{K-D}) = 0$ por ser D un divisor de grado mayor que el canónico. Lo mismo ocurre con $D - x$ y $D - x - y$. Por Riemann-Roch,

$$h^0(C, \mathscr{L}_D) = \chi(C, \mathscr{L}_D) = \chi(C, \mathscr{O}_C) + \mathrm{gr} D$$
$$h^0(C, \mathscr{L}_{D-x}) = \chi(C, \mathscr{L}_{D-x}) = \chi(C, \mathscr{O}_C) + \mathrm{gr} D - 1$$
$$h^0(C, \mathscr{L}_{D-x-y}) = \chi(C, \mathscr{L}_{D-x-y}) = \chi(C, \mathscr{O}_C) + \mathrm{gr} D - 2$$

Se concluye fácilmente por el lema anterior.

□

11. Teorema : *Toda curva completa y no singular sobre un cuerpo algebraicamente cerrado es una curva proyectiva.*

Demostración. Si D es un divisor de grado $2g + 1$, entonces $\mathscr{L}_D$ es muy amplio por la proposición anterior, luego define una inmersión cerrada de la curva en un espacio proyectivo. □

Sea C una curva completa y no singular de género mayor que 1 y K un divisor canónico. Entonces $3K$ es un divisor muy amplio, es decir, $\mathscr{L}_{3K}$ es un haz de línea muy amplio. Por tanto, $\mathscr{L}_{3K}$ define una inmersión cerrada de C en $\mathbb{P}^{5g-6}$, canónica salvo proyectividades, de modo que C es una curva alabeada de grado $6g - 6$ y los hiperplanos de $\mathbb{P}^{5g-6}$ cortan a C en divisores linealmente equivalentes a $3K$.

14.9.3. Curvas elípticas e hiperelípticas

Sea C una curva completa no singular, sobre un cuerpo k algebraicamente cerrado. Supondremos que $\mathrm{car}\, k \neq 2$.

12. Proposición : *En las curvas de género menor o igual que dos el dualizante no es muy amplio.*

Demostración. Si el género es dos y el dualizante es muy amplio, entonces el dualizante define una inmersión cerrada de la curva en la recta proyectiva, luego la curva sería la recta proyectiva que es de género cero, contradicción. Si el género es 1 o cero es obvio. □

13. Definición : Las curvas de género mayor o igual que 2 cuyo haz dualizante no es muy amplio se denominan curvas hiperelípticas. Las curvas de género 1 se denominan curvas elípticas.

Si C es una curva de género mayor que uno y no hiperelíptica, el dualizante define una inmersión canónica $C \hookrightarrow \mathbb{P}^{g-1}$ que identifica C con una curva no singular de grado $2g-2$.

14. Proposición: *1. La condición necesaria y suficiente para que el dualizante sea muy amplio es que para cada par de puntos $x, y \in C$ (distintos o no), se verifique que $h^1(C, \omega_C \otimes \mathscr{L}_{-x-y}) = h^1(C, \omega_C)$.*

2. Supongamos que el género de C es distinto de cero. C es una curva elíptica o hiperelíptica si y solo si existen $x, y \in C$ (distintos o no) tales que $h^0(C, \mathscr{L}_{x+y}) = 2$.

Demostración. 1. Denotemos $\omega_C = \mathscr{L}_K$. La condición $h^1(C, \mathscr{L}_{K-x-y}) = h^1(C, \mathscr{L}_K)$ para todo $x, y \in C$ equivale a que $h^0(C, \mathscr{L}_K) = h^0(C, \mathscr{L}_{K-x-y}) + 2$. Por el Lema 14.9.9 se concluye.

2. Por el apartado 1., C es una curva elíptica o hiperelíptica si y solo si existen $x, y \in C$ (distintos o no) tales que $h^1(C, \mathscr{L}_{K-x-y}) \neq h^1(C, \mathscr{L}_K)$, que por dualidad equivale a decir $h^0(C, \mathscr{L}_{x+y}) \neq 1$. Observemos que $h^0(C, \mathscr{L}_x) = 1$, porque si fuera mayor existiría una función f con un único polo, en x y de orden 1, que definiría un isomorfismo $f : C \to \mathbb{P}^1$. Por tanto, C es una curva elíptica o hiperelíptica si y solo si existen $x, y \in C$ (distintos o no) tales que $h^0(C, \mathscr{L}_{x+y}) = 2$.

□

15. Corolario: *Una curva de género mayor que cero es elíptica o hiperelíptica si y solo si admite un morfismo de grado dos en la recta proyectiva.*

Demostración. C es elíptica o hiperelíptica $\Leftrightarrow$ existen $x, y \in C$ tales que $h^0(C, \mathscr{L}_{x+y}) = 2$ $\Leftrightarrow$ existe una función racional $f \in \Sigma$ cuyo divisor de polos es $x + y$ (si el divisor de polos fuese de grado 1 entonces la curva sería la recta proyectiva, contradicción) $\Leftrightarrow$ existe un morfismo $f : C \to \mathbb{P}^1$ de grado dos. □

16. Definición: Supongamos que el género de C es mayor que uno. Se dice que $x \in C$ es un punto hiperelíptico si $h^0(C, L_{2x}) = 2$ (en particular, C es hiperelíptica).

Si $f : C \to \mathbb{P}^1$ es un morfismo de grado 2, entonces los puntos de ramificación son puntos hiperelípticos.

17. Corolario: *Toda curva elíptica o hiperelíptica es birracionalmente isomorfa a una curva plana de ecuaciones $y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i)$, donde g es el género de la curva y los α_i son disntintos entre sí (suponemos $\operatorname{car} k \neq 2$).*

Demostración. Sea $\pi\colon C \to \mathbb{P}^1$ un morfismo de grado dos de la curva en la recta proyectiva. Podemos suponer que el punto del infinito es un punto rama. Sea Σ el cuerpo de funciones de C. El morfismo inducido $\Sigma_{\mathbb{P}^1} \hookrightarrow \Sigma_C$ es de grado dos, luego $\Sigma_C = k(x)(\xi)$, de modo que $\xi^2 + s\xi + t = 0$, con $s,t \in k(x)$. Cambiando ξ por $\xi + \frac{s}{2}$, podemos suponer que $\xi^2 + u = 0$, con $u \in k(x)$. Es decir, $\xi^2 = \frac{p(x)}{q(x)}$, con $p(x), q(x) \in k[x]$. Sustituyendo ξ por $\xi \cdot q(x)$, podemos suponer que $\xi^2 = p(x)$, con $p(x) \in k[x]$. Sustituyendo ξ por $\xi \cdot (x-\alpha)^n$ (para n conveniente), podemos suponer que las raíces de $p(x)$ son simples. Los puntos de ramificación de π se proyectan por π en las raíces de $p(x)$ y el punto del infinito. Por Hurwitz, el número de puntos de ramificación de π es $2g+2$ (y todos ellos han de ser de índice de ramificación 2), luego $p(x) = \prod_{i=1}^{2g+1} (x - \alpha_i)$. Con todo, C es birracionalmente isomorfa a la curva plana $y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i)$. □

18. Proposición: *Sea C una curva completa no singular de género g mayor que 1. Entonces, un morfismo $\pi\colon C \to \mathbb{P}^{g-1}$ es de grado $2g-2$ (es decir, $\pi^{-1}(H)$ es un divisor de grado $2g-2$ para todo hiperplano H de $\mathbb{P}^{g-1}$) de imagen una curva alabeada si y solo si π es (salvo proyectividades) el morfismo canónico, es decir, el morfismo definido por el haz dualizante y la serie lineal completa.*

Demostración. El dualizante $\mathscr{L}_K$ no tiene puntos base: Si $h^0(C, \mathscr{L}_{K-x}) = h^0(C, \mathscr{L}_K)$ entonces por dualidad $h^0(C, \mathscr{L}_x) > h^0(C, \mathscr{O}_C)$. Luego existe una función con un único polo (en x) y éste de multiplicidad 1, que define un isomorfismo de C con $\mathbb{P}^1$. Pero el género de C no es cero y hemos llegado a contradicción.

En conclusión el dualizante (y sus secciones globales) definen un morfismo de grado $2g-2$, $C \to \mathbb{P}^{g-1}$.

Si $\pi\colon C \to \mathbb{P}^{g-1}$ es un morfismo alabeado de grado $2g-2$ entonces éste viene definido por un haz de línea $\mathscr{L}_D$ tal que $h^0(C, \mathscr{L}_D) \geq g$ y $\operatorname{gr} D = 2g-2$. Por el teorema de Riemann-Roch, $h^0(C, \mathscr{L}_{K-D}) > 0$. Lo cual implica que D es equivalente a K y que π es el morfismo inducido por el canónico y sus secciones globales.

□

19. Proposición: *Si C es una curva hiperelíptica entonces existe un único morfismo de grado 2, $C \to \mathbb{P}^1$, salvo proyectividades.*

Demostración. Nos falta probar la unicidad.

Sean $\pi, \pi'\colon C \to \mathbb{P}^1$ dos morfismos de grado 2. Sea $i\colon \mathbb{P}^1 \to \mathbb{P}^{g-1}$, $\alpha \mapsto (1, \alpha, \ldots, \alpha^{g-1})$ el morfismo inducido por $\mathscr{O}_{\mathbb{P}^1}(g-1)$ y sus secciones globales.

Por la proposición anterior existe una proyectividad $\tau\colon \mathbb{P}^{g-1} \to \mathbb{P}^{g-1}$ que hace conmutativo el siguiente diagrama

$$\begin{array}{ccccc} C & \xrightarrow{\pi} & \mathbb{P}^1 & \xrightarrow{i} & \mathbb{P}^{g-1} \\ & \searrow^{\pi'} & & & \| \tau \\ & & \mathbb{P}^1 & \xrightarrow{i} & \mathbb{P}^{g-1} \end{array}$$

τ induce una proyectividad $\tau'\colon \mathbb{P}^1 \to \mathbb{P}^1$, tal que $\tau' \circ \pi = \pi'$. □

Observemos que el morfismo canónico es igual a $i \circ \pi$.

20. Corolario: *El conjunto de curvas hiperelípticas de género g, módulo isomorfismos, es igual al conjunto de los subconjuntos (divisores) de $2g+2$ puntos distintos de $\mathbb{P}^1$, módulo proyectividades.*

Demostración. Dados $2g+2$ puntos distintos $\alpha_1, \ldots, \alpha_{2g+2} \in \mathbb{P}^1$, la curva C completa no singular birracional a la curva plana $y^2 - \prod_{i=1}^{2g+2}(x - \alpha_i) = 0$ resulta ser una curva de género g. La proyección "vertical" de esta curva en $y = 0$ es un morfismo de grado dos que ramifica en $\alpha_1, \ldots, \alpha_{2g+2}$. La composición de este morfismo con una proyectividad τ ramifica en $\tau(\alpha_1), \ldots, \tau(\alpha_{2g+2})$, luego como vimos en la demostración de 14.9.17, C es birracional a $y^2 - \prod_{i=1}^{2g+2}(x - \tau(\alpha_i)) = 0$.

Si C es birracional a otra curva plana $y^2 - \prod_{i=1}^{2g+2}(x - \alpha'_i) = 0$, entonces tenemos otro morfismo de grado dos en la recta proyectiva ($y = 0$) que ramifica en $\alpha'_1, \ldots, \alpha'_{2g+2}$. Por la proposición anterior existe una proyectividad $\tau\colon \mathbb{P}^1 \to \mathbb{P}^1$ tal que $\tau(\alpha_i) = \alpha'_i$, para todo i.

Con todo se concluye.

□

Pasemos ahora a estudiar las curvas elípticas. El dualizante de una curva elíptica es de grado cero y tiene secciones, luego es isomorfo al haz de anillos de la curva.

21. Proposición: *El grupo de automorfismos de una curva elíptica actúa transitivamente sobre los puntos racionales de la curva.*

Demostración. Sean $x, y \in C$ dos puntos racionales. El haz de línea $\mathscr{L}_{x+y}$ no tiene puntos base, por 14.9.10. Además, $h^0(C, \mathscr{L}_{x+y}) = 2$, por Riemann-Roch. Por tanto, $\mathscr{L}_{x+y}$ define un morfismo finito

$$\pi\colon C \to \mathbb{P}^1$$

Las fibras de los puntos de $\mathbb{P}^1$ son los divisores efectivos linealmente equivalentes a $x+y$. En particular, $\pi(x)=\pi(y)$. Sea $k(x)\hookrightarrow\Sigma$ la extensión de grado 2 inducida por π entre los cuerpos de fracciones. Σ es una extensión de Galois de $k(x)$, por ser de grado 2. Sea σ el generador de $\mathrm{Aut}_{k(x)}(\Sigma)=\mathbb{Z}/2\mathbb{Z}$. El morfismo $\bar{\sigma}\colon C\to C$ inducido por σ conmuta con π, luego deja estables las fibras de π. Es más, $\bar{\sigma}$ intercambia los dos puntos de cada fibra (esto se debe al hecho de que $C/\langle\bar{\sigma}\rangle=\mathbb{P}^1$, pero demos una demostración ad hoc: Sea $\pi(x)=\pi(y)$ y $f\in\Sigma$ con un cero en x y no en y. Si $\bar{\sigma}(x)=x$ y $\bar{\sigma}(y)=y$, entonces $f\cdot\sigma(f)\in k(x)$ tiene un cero en x y no en y, luego esta función por un lado se anula en $\pi(x)$ y por el otro no se anula en $\pi(y)=\pi(x)$). En conclusión, $\bar{\sigma}(x)=y$. □

22. Proposición: *Sea C una curva elíptica y $\pi_1,\pi_2\colon C\to\mathbb{P}^1$ dos morfismos de grado dos. Existen automorfismos $\tau\colon C\to C$, $\sigma\colon\mathbb{P}^1\to\mathbb{P}^1$ de modo que el diagrama*

$$\begin{array}{ccc} C & \xrightarrow{\tau} & C \\ \downarrow{\scriptstyle\pi_1} & & \downarrow{\scriptstyle\pi_2} \\ \mathbb{P}^1 & \xrightarrow[\sigma]{} & \mathbb{P}^1 \end{array}$$

es conmutativo.

Demostración. Por Hurwitz, π_1 y π_2 ramifican en cuatro puntos. Sea x un punto de ramificación de π_1, y un punto de ramificación de π_2 y τ un automorfismo de C tal que $\tau(x)=y$. El morfismo π_2 es el morfismo definido por el haz de línea $\mathscr{L}_{2y}$ y el morfismo $\pi_1\circ\tau$ también es el morfismo definido por el haz de línea $\mathscr{L}_{2y}$. Por tanto, π_2 y $\pi_1\circ\sigma$ difieren en un automorfismo σ de $\mathbb{P}^1$. □

En la Proposición 14.9.17 se probó que si $\pi\colon C\to\mathbb{P}^1$ es un morfismo de grado dos, existe $y\in\Sigma$ tal que $\Sigma=k(x,y)$, con $y^2=(x-\alpha_0)\cdot(x-\alpha_1)\cdot(x-\alpha_2)$ y $\infty,\alpha_0,\alpha_1,\alpha_2\in\mathbb{P}^1$ son los puntos (distintos) donde ramifica π. Componiendo con una proyectividad, podemos suponer que $\alpha_0=0$ y $\alpha_1=1$ y tendremos que C viene dada por la ecuación

$$y^2=x\cdot(x-1)\cdot(x-\lambda).$$

En el diagrama de la proposición anterior, σ aplica la ramificación de π_1 en la de π_2. Otra ecuación $y^2=x\cdot(x-1)\cdot(x-\lambda')$ define la misma curva si y solo si existe una proyectividad σ tal que $\{\infty,0,1,\lambda'\}=\{\sigma(\infty),\sigma(0),\sigma(1),\sigma(\lambda)\}$. Componiendo con la involución que permuta dos parejas de puntos convenientes de $\{\infty,0,1,\lambda'\}$, podemos suponer que σ permuta los puntos $\{\infty,0,1\}$ y queda determinada por esta permutación. El grupo de las proyectividades que permutan los puntos $\{\infty,0,1\}$, es isomorfo al grupo simétrico de las permutaciones de tres letras, S_3. En conclusión,

$$\{\text{Curvas elípticas}\}=k\setminus\{1,0\}/S_3$$

Si σ es la proyectividad que permuta ∞ con 0 y deja fijo el 1, entonces $\sigma(\lambda) = \frac{1}{\lambda}$. Si σ' es la proyectividad que permuta 1 con 0 y deja fijo ∞, entonces $\sigma'(\lambda) = 1 - \lambda$. Se verifica además que $S_3 = \langle \sigma, \sigma' \rangle$. Definamos[1]

$$j(\lambda) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

Se verifica que

$$k(\lambda)^{S_3} = k(j(\lambda))$$

pues $j(\lambda)$ es S_3-invariante y la inclusión $k(j(\lambda)) \hookrightarrow k(\lambda)$ es de grado 6, porque el divisor de ceros de $j(\lambda)$ es de grado 6. Por tanto, $\mathbb{P}^1/S_3 = \mathbb{P}^1$, $\mathbb{P}^1 \setminus \{\infty, 0, 1\}/S_3 = \mathbb{P}^1 - \infty$ y el morfismo de paso al cociente es

$$\begin{array}{ccc} \mathbb{P}^1 & \to & \mathbb{P}^1/S_3 = \mathbb{P}^1 \\ \lambda & \mapsto & j(\lambda) \end{array}$$

Con todo,

$$\{\text{Curvas elípticas}\} \Longleftrightarrow \mathbb{A}_1$$

$$y^2 = x(x-1)(x-\lambda) \longmapsto j(\lambda)$$

23. Teorema : *Sea C una curva elíptica sobre un cuerpo algebraicamente cerrado y $\mathrm{Pic}^0(C)$ el grupo de los divisores de C de grado cero módulo el subgrupo de los divisores principales. Fijado un punto cerrado $x \in C$, la aplicación*

$$\begin{array}{ccc} \{\textit{Puntos cerrados de } C\} & \to & \mathrm{Pic}^0(C) \\ y & \mapsto & \mathscr{L}_{y-x} \end{array}$$

es biyectiva.

Demostración. Es inyectiva: si $\mathscr{L}_{y-x} \simeq \mathscr{L}_{y'-x}$, entonces $\mathscr{L}_{y-y'} \simeq \mathscr{O}$, luego existe una función racional $f \in \Sigma$ tal que $D(f) = y' - y$. Si $y' \neq y$, esta función define un isomorfismo $f : C \to \mathbb{P}^1$, contradicción.

Es epiyectiva: sea D un divisor de grado cero. Por Riemann-Roch $h^0(C, \mathscr{L}_{D+x}) = 1$, pues los divisores canónicos tienen grado cero (de hecho, $\omega_C = \mathscr{O}_C$). Por tanto, $D + x$ es linealmente equivalente a un divisor efectivo de grado 1, digamos y, luego D es linealmente equivalente a $y - x$. □

[1] El factor 2^8 se introduce, a pesar de lo que pueda parecer, para que en característica 2 todo vaya bien.

Dado que $\mathrm{Pic}^0(C)$ tiene estructura de grupo abeliano, tenemos que el conjunto de los puntos cerrados de C tiene estructura de grupo abeliano con la siguiente operación $+'$: $y +' y' := y''$, siendo y'' tal que $y'' - x$ es linealmente equivalente a $(y-x)+(y'-x)$, es decir, tal que $y + y' - y'' - x = Df$ es un divisor principal.

Por el corolario 14.9.17, C es isomorfa a una cúbica proyectiva plana de ecuación $y^2 - x\cdot(x-1)\cdot(x-\lambda) = 0$, para cierta $\lambda \in k\setminus\{1,0\}$. Sea r la ecuación de la recta que pasa por y e y', sea x' el tercer punto de corte dicha recta con la cúbica, y sea r' la ecuación de la recta que pasa por x y x'. Si x'' es el tercer punto de corte de la recta r' con la cúbica, se verifica que $D(\frac{r}{r'}) = y + y' - x - x''$. Por tanto, $D(\frac{r}{r'}\cdot f^{-1}) = y'' - x''$ y como el género de C no es cero $y'' = x''$. En conclusión, si denotamos $\phi\colon C\times C \to C$ el morfismo que asigna a cada pareja (y,y') el tercer punto de corte de la recta que pasa por y e y' con C, tenemos que el morfismo

$$C\times C \to C,\ (y,y') \mapsto \phi(\phi(y,y'),x)$$

coincide, sobre los puntos racionales, con la ley de grupo definida anteriormente en C.

14.9.4. Curvas en $\mathbb{P}^3$

Supondremos que C es una curva completa no singular sobre un cuerpo algebraicamente cerrado.

24. Definición: Se dice que un divisor D es especial si $h^0(C,\mathscr{L}_{K-D}) > 0$. En caso contrario, se dice que D es no especial. El número $h^0(C,\mathscr{L}_{K-D})$ se denomina índice de especialidad de D.

El teorema de Riemann-Roch da un cálculo exacto de $h^0(C,\mathscr{L}_D)$ si D es no especial. El teorema de Clifford nos dará una acotación del mismo cuando D es especial.

25. Lema: *Si D, D' son divisores efectivos de una curva C, entonces*

$$h^0(C,\mathscr{L}_D) + h^0(C,\mathscr{L}_{D'}) \le h^0(C,\mathscr{L}_{D+D'}) + 1$$

Demostración. Consideremos el morfismo

$$\mathbb{P}(H^0(C,\mathscr{L}_D))\times\mathbb{P}(H^0(C,\mathscr{L}_{D'})) \xrightarrow{\Phi} \mathbb{P}(H^0(C,\mathscr{L}_{D+D'}))$$

$$(E,E') \longmapsto E+E'$$

donde E y E' son divisores efectivos linealmente equivalentes a D y D' respectivamente. Φ es el morfismo inducido por la aplicación bilineal

$$H^0(C,\mathscr{L}_D)\times H^0(C,\mathscr{L}_{D'}) \to H^0(C,\mathscr{L}_{D+D'}),\ (f,g)\mapsto f\cdot g$$

Obsérvese que las fibras de Φ son finitas, porque todo divisor efectivo se escribe como suma de divisores efectivos de un número finito de modos. Por tanto, la dimensión de $\operatorname{Im}\Phi$ coincide con la dimensión de la variedad inicial y se obtiene el lema. □

26. Teorema de Clifford: *Si D es un divisor especial de una curva C, entonces*

$$h^0(C,\mathscr{L}_D) \leq \frac{1}{2}\operatorname{gr} D + 1.$$

Supongamos que C es hiperelíptica. La igualdad se cumple si y solo si D es linealmente equivalente a $2r\cdot x$, donde x es un punto hiperelíptico.

Demostración. Por el lema anterior, $h^0(C,\mathscr{L}_D)+h^0(C,\mathscr{L}_{K-D}) \leq h^0(C,\mathscr{L}_K)+1 = g+1$. Por Riemann-Roch, $h^0(C,\mathscr{L}_D)-h^0(C,\mathscr{L}_{K-D}) = \operatorname{gr} D + 1 - g$. Sumando estas dos expresiones obtenemos

$$h^0(C,\mathscr{L}_D) \leq \frac{1}{2}\operatorname{gr} D + 1.$$

Demostremos la segunda afirmación del teorema. Si $x \in C$ es hiperelíptico, entonces $h^0(C,\mathscr{L}_{2x}) = 2$. Escribamos $H^0(C,\mathscr{L}_{2x}) = \langle 1, f\rangle$, con $v_x(f) = -2$. Entonces $\{1, f, \ldots, f^r\}$ son linealmente independientes y pertenecen a $\Gamma(C,\mathscr{L}_{2r\cdot x})$. Por la desigualdad anterior, $h^0(C,\mathscr{L}_{2r\cdot x}) = \frac{1}{2}\operatorname{gr}(2r\cdot x)+1$.

Recíprocamente, sea D un divisor especial que cumpla la igualdad, y que por tanto tiene grado par $2r$. Se cumple que $h^0(C,\mathscr{L}_{D-y}) < h^0(C,\mathscr{L}_D)$: por Riemann-Roch si $D-y$ no es especial, y por la desigualdad del teorema si $D-y$ es especial. Por tanto, $\mathscr{L}_D$ define un morfismo $\pi\colon C \to \mathbb{P}^r$. Como $H^0(C,\mathscr{L}_D) \subseteq H^0(C,\mathscr{L}_K)$, y el morfismo canónico factoriza vía una proyección por un morfismo de grado 2 a $\mathbb{P}^1$, lo mismo le sucede a π. Tenemos $C \xrightarrow{\pi_1} \mathbb{P}^1 \xrightarrow{\pi_2} \mathbb{P}^r$, con $\pi = \pi_2\circ\pi_1$, $\operatorname{gr}\pi_1 = 2$ y $\operatorname{gr}\pi_2 = r$. Sea $p \in \mathbb{P}^1$ un punto rama, luego $\pi^{-1}(p) = 2\cdot x$, donde x es un punto hiperelíptico. El morfismo π_2 es el morfismo definido por la serie lineal completa de un haz de línea asociado a un divisor de grado r, que es equivalente a $r\cdot p$. Es decir, existe un hiperplano $H \subset \mathbb{P}^r$ tal que $\pi_2^{-1}(H) = r\cdot p$. Por tanto, D es linealmente equivalente a $\pi^{-1}(H) = \pi_1^{-1}(\pi_2^{-1}(H)) = 2r\cdot x$. □

Sea C una curva de $\mathbb{P}^3$, de cuerpo de funciones Σ, $x_0,\ldots,x_3$ coordenadas homogéneas de $\mathbb{P}^3$ y $y_i = x_i/x_0$ coordenadas afines. Entonces $\Omega_{\Sigma/k} = \langle dy_1, dy_2, dy_3\rangle$. Supongamos que $\Omega_{\Sigma/k} = \langle dy_1\rangle$. Entonces el morfismo $k(y_1) \hookrightarrow \Sigma$ es separable. Sea $\mathbb{P}^1$ el haz de hiperplanos que pasan por la recta $x_0 = 0, x_1 = 0$ y consideremos morfismo $C \to \mathbb{P}^1$ que asigna a cada punto de C el hiperplano del haz que pasa por ese punto. Este morfismo coincide con el inducido por la inclusión $k(y_1) \hookrightarrow \Sigma$, y ramifica en los hiperplanos del haz tangentes a la curva. Por el teorema de Hurwitz, casi todos los hiperplanos del haz no son tangentes a la curva.

27. Definición: Diremos que una recta es una secante de la curva $C \hookrightarrow \mathbb{P}^3$ si corta a la curva en dos puntos distintos. Se dice que una recta es una multisecante de la curva C si corta a la curva en más de dos puntos (contando multiplicidades).

Veamos que si la curva es alabeada, existen secantes que no son multisecantes. Probemos primero que si todas las secantes son multisecantes, entonces todas las tangentes a la curva pasan por un mismo punto. Sea $p \in C$ y H un hiperplano que no contenga a p. Sea $\phi\colon C \to H$ la proyección de C desde p en H. Sea $C' = \operatorname{Im}\phi$ y $r \geq 2$ el grado del morfismo $\phi\colon C \to C'$. Sea R una secante no tangente a C que pase por p, que existe sin más que considerar cualquier secante incluida en cualquier plano no tangente a C que pase por p. Todas las secantes que pasan por p cortan a C en $r+1$ puntos distintos (contando p), salvo un número finito de secantes, las correspondientes a los puntos singulares de C' que cortan en más puntos (contando multiplicidades) y las secantes tangentes. Es fácil deducir que todas las secantes que pasan por cualquier punto de C cortan a C en $r+1$ puntos, salvo número finito de secantes que cortan en más puntos. Dado $q \in R \cap C$, ϕ proyecta la tangente en q a C en la tangente a C' en $\phi(q)$ (supongamos $\phi(q)$ no singular). Lo que implica que todas las tangentes en los puntos de $R \cap C \setminus p$ son coplanarias. Proyectando desde otro punto de $R \cap C$ llegamos a la conclusión de que todas las tangentes de los puntos $R \cap C$, incluido p, son coplanarias. Ahora bien, como la condición de que la tangente en un punto sea coplanaria con la tangente en p es cerrada, variando R obtenemos que todos los puntos de C tienen tangentes coplanarias con la de p. Variando p, obtenemos que todas las tangentes son coplanarias. Si $p' \in C$ es un punto que no yace en el plano que contiene a p, q y sus tangentes, entonces la tangente a p' corta a la tangente en p y a la tangente en q en un mismo punto. En conclusión, todas las tangentes a C pasan por un mismo punto.

Sea H un hiperplano no tangente a C. Proyectemos C en un hiperplano desde un punto de H que no yazca en las tangentes a C y no yazca en ninguna de las secantes de C que están en el hiperplano H. La proyección es un morfismo de grado 1, de imagen una curva plana $\bar{C}$ no singular, cuyas tangentes pasan todas por un punto p. Sea $q \notin \bar{C}$, distinto de p. La proyección desde q, $\pi\colon \bar{C} \to \mathbb{P}^1 = R$, en una recta, solo ramifica en los puntos de la recta R' que une p y q, es decir, en $R' \cap \bar{C}$.

En coordenadas afines, supongamos que $p = (0,0)$, q el punto del infinito de la recta $x = 0$ (luego R' es $x = 0$) y $\bar{C}$ de ecuación afín $p(x,y) = 0$. La ecuación de la recta tangente en $c = (\alpha, \beta)$ de $\bar{C}$ es $\frac{\partial p}{\partial x}(\alpha,\beta)(x-\alpha) + \frac{\partial p}{\partial y}(\alpha,\beta)(y-\beta) = 0$ y como pasa por p, $\frac{\partial p}{\partial x}(\alpha,\beta)\alpha + \frac{\partial p}{\partial y}(\alpha,\beta)\beta = 0$, es decir, $\frac{\partial p(x,y)}{\partial x}x + \frac{\partial p(x,y)}{\partial y}y = 0$ en $k[x,y]/(p(x,y))$. Ahora bien si c es un punto de ramificación entonces su tangente es $x = 0$, luego $\frac{\partial p(x,y)}{\partial x}(c) \neq 0$, luego $\frac{\partial p(x,y)}{\partial x}$ es invertible localmente en $c \in \bar{C}$ y x es múltiplo de $\frac{\partial p(x,y)}{\partial y}$ en $(k[x,y]/(p(x,y)))_c$.

Por tanto el número de ramificación,

$$h^0(\bar{C},\Omega_{\bar{C}/\mathbb{P}^1}) = \dim_k k[x,y]/(p(x,y),\frac{\partial p(x,y)}{\partial y}) \leq \dim_k k[x,y]/(p(x,y),x).$$

Por el teorema de Hurwitz,

$$2g_{\bar{C}} - 2 \leq -n,$$

luego $g_{\bar{C}} = 0$ y n es 1 ó 2. Por tanto, el grado de C, que coincide con el de $\bar{C}$, es 1 ó 2, y C no es alabeada (además $g_C = g_{\bar{C}} = 0$).

28. Teorema de Castelnuovo: *Si $C \hookrightarrow \mathbb{P}^3$ es una curva alabeada de grado d y género g, entonces $d \geq 3$ y*

$$g \leq \begin{cases} \frac{1}{4}d^2 - d + 1, & \text{si } d \text{ es par} \\ \frac{1}{4}(d^2-1) - d + 1, & \text{si } d \text{ es impar} \end{cases}$$

Además, si una curva verifica la igualdad, entonces yace sobre una cuádrica (la igualdad se alcanza por ciertas curvas para todo $d \geq 3$).

Demostración. Veamos en primer lugar que existe un hiperplano H de $\mathbb{P}^3$ que corta a la curva en puntos $\{p_1,\ldots,p_d\}$, de modo que tres cualesquiera de ellos no son colineales. Sea X el "conjunto" de las rectas de $\mathbb{P}^3$. Sea $Y = \{(a,b,c,r) \in C\times C\times C\times X : a \neq b \neq c$ y $a,b,c \in r\}$ y $\pi\colon Y \to C$ la primera proyección. Sea $p \in C$ un punto por el que pase alguna cuerda que no sea multicuerda. Proyectando C desde p, por Hurwitz obtendremos que por p solo pasa un número finito de multicuerdas[2] Los puntos de C que no yacen en estas multicuerdas cumplen, como p, que por ellos solo pasan un número finito de multicuerdas. Ahora es fácil probar que las fibras de π son de dimensión cero, salvo quizás para un número finito de puntos para los que es de dimensión 1. Por tanto, $\dim Y = 1$. Proyectando Y en X, tenemos que el "conjunto" de rectas que son multicuerdas es de dimensión 1. Por tanto, el "conjunto" de hiperplanos que contienen a alguna multicuerda es de dimensión 2, luego existe un hiperplano que no contiene multicuerdas.

Sea $D = p_1 + \ldots + p_d$. Entonces $\mathscr{L}_D = \mathscr{O}_{\mathbb{P}^3}(1)_{|C}$. Para cada $i = 1,2,\ldots,\text{mín}(d,2n+1)$, p_i no es un punto base de $\Gamma(C,\mathscr{L}_{nD-p_1-\ldots-p_{i-1}})$: en efecto, sea H_1 un plano que pase por p_1 y p_2 y no pase por ningún otro p_j. Sea H_2 un hiperplano que pase por p_3 y p_4 y no pase por ningún otro p_j. Así sucesivamente hasta $r = [\frac{i-1}{2}]$ (si $i-1$ es impar, consideramos H_r, que pasa solo por p_{i-1}). Para $r < j \leq n$, consideramos planos H_j que

[2] Si el número de multicuerdas que pasan por p fuese cero, entonces la curva proyectada $\tilde{C}$ sería no singular. $\tilde{C}$ sería una curva plana (isomorfa a C) de grado $d-1$ de género geométrico $\frac{(d-2)(d-3)}{2}$. Si proyectamos desde otro punto q de la curva C, obtendremos una curva birracional a C de grado $d-1$ y de género aritmético $\frac{(d-2)(d-3)}{2}$, luego ha de ser no singular y el número de multicuerdas que pasan por q es cero.

no pasen por p_i. La unión de todos los planos corta a C en un divisor linealmente equivalente a nD que pasa por $p_1,\dots,p_{i-1}$ y no por p_i.

Tenemos entonces mín$(d,2n+1)$ desigualdades

$$h^0(C,\mathscr{L}_{nD-p_1-\dots-p_{i-1}}) > h^0(C,\mathscr{L}_{nD-p_1-\dots-p_i}).$$

Luego,

$$h^0(C,\mathscr{L}_{nD}) - h^0(C,\mathscr{L}_{(n-1)D}) \geq \text{mín}(d,2n+1) \qquad (*)$$

Sumando estas desigualdades desde 1 hasta $n >> 0$, obtenemos

$$h^0(C,\mathscr{L}_{nD}) \geq s(s+2)+(n-s)d+1$$

con $s = [\frac{1}{2}(d-1)]$. Por otra parte, para $n >> 0$, nD es no especial, luego por Riemann-Roch

$$h^0(C,\mathscr{L}_{nD}) = nd - g + 1$$

Combinando las dos fórmulas, obtenemos

$$g \leq sd - s(s+2)$$

que es la fórmula del teorema, escrita de modo conciso.

Si se cumple la igualdad, entonces las inecuaciones de $(*)$ son igualdades. En particular, tendremos que $h^0(C,\mathscr{L}_{2D}) = 9$. De la sucesión exacta

$$0 \to \mathfrak{p}_C \to \mathscr{O}_{\mathbb{P}^3} \to \mathscr{O}_C \to 0$$

obtenemos la sucesión exacta

$$0 \to H^0(C,\mathfrak{p}_C(2)) \to H^0(\mathbb{P}^3,\mathscr{O}_{\mathbb{P}^3}(2)) \to H^0(C,\mathscr{L}_{2D})$$

que nos dice que existe una cuádrica que pasa por C. □

14.9.5. Integración por funciones elementales

Juan Antonio Navarro

29. Definición: Llamaremos cuerpo diferencial a un cuerpo K, con una (ley de) derivación $K \to K$, $a \overset{Not}{\mapsto} a'$. Diremos que $a \in K$ es una constante si $a' = 0$. Diremos que $i: K \to L$ es una extensión diferencial si L es un cuerpo diferencial e i es un morfismo de anillos que conmuta con las derivaciones.

Supondremos que los números complejos $\mathbb{C}$ es el cuerpo de constantes de todos los cuerpos diferenciales que vamos a considerar.

Se cumple que:

1. $\frac{(uv)'}{uv} = \frac{u'}{u} + \frac{v'}{v}$.

2. $\frac{u'}{u} = \frac{v'}{v} \Leftrightarrow v = cu$ para alguna constante $c \in \mathbb{C}$, ya que $\frac{u'}{u} = \frac{v'}{v} \Leftrightarrow u'v - v'u = 0 \Leftrightarrow (u/v)' = 0$.

30. Definición: Si $v' = u'/u$, diremos que $v = \ln u$ es el *logaritmo* de u, ó que $u = e^v$ es la *exponencial* de v.

31. Definición: Diremos que una extensión diferencial $K \to L$ es una extensión por *funciones elementales* si $L = K(u_1, \ldots, u_n)$ donde cada función u_i verifica una de las siguientes condiciones:

1. u_i es algebraico sobre $K(u_1, \ldots, u_{i-1})$.

2. u_i es la exponencial de algún elemento de $K(u_1, \ldots, u_{i-1})$.

3. u_i es el logaritmo de algún elemento de $K(u_1, \ldots, u_{i-1})$.

y diremos que $f \in K$ es *integrable por funciones elementales* si existe alguna extensión $K \to L$ por funciones elementales y un elemento $u \in L$ tal que $u' = f$.

Nota: Las funciones elementales de una variable en sentido clásico son los elementos de las extensiones por funciones elementales del cuerpo de funciones racionales $\mathbb{C}(x)$, contenidas en el cuerpo de funciones meromorfas en un abierto del plano complejo (que jugaría el papel de un cierre algebraico). Las funciones trigonométricas (incluso hiperbólicas) y sus inversas son elementales: se expresan con exponenciales y logaritmos.

En principio, la integración con funciones elementales en sentido clásico sería un concepto más restrictivo (pues no hemos probado que toda extensión de $\mathbb{C}(x)$ por funciones elementales pueda sumergirse en un cuerpo de funciones meromorfas), pero el teorema de Liouville mostrará que las funciones integrables con funciones elementales también lo son en el sentido clásico, por lo que ambos coinciden.

32. Teorema de Liouville: *Si una función $f \in K$ es integrable con funciones elementales, entonces existen funciones $h, g_1, \ldots, g_n \in K$ y constantes $c_1, \ldots, c_n \in \mathbb{C}$ tales que*

$$\int f\,dx = h + c_1 \ln g_1 + \ldots + c_n \ln g_n$$

Demostración. Si f admite una primitiva elemental en $K(u,u_2,\dots,u_r)$, por inducción sobre r y considerando la extensión diferencial

$$K(u)\to K(u,u_2,\dots,u_r)$$

podemos suponer que existen $q(u),p_1(u),\dots,p_n(u)\in K(u)$ tales que

$$f=q(u)'+c_1\frac{p_1(u)'}{p_1(u)}+\ldots+c_n\frac{p_n(u)'}{p_n(u)}$$

y hemos de hallar una descomposición similar en K.

Caso u algebraico: La derivación de K se extiende de modo *único* a cada extensión finita L (como $L=K[z]/(p(z))$ siendo $p(z)\in K[z]$ separable, es fácil probar que $\Omega_{L/\mathbb{C}}=\Omega_{K/\mathbb{C}}\otimes_K L$ y que $\mathrm{Der}_{\mathbb{C}}(K,L)=\mathrm{Der}_{\mathbb{C}}(L,L)$), luego tal extensión es compatible con cualquier morfismo de K-álgebras y, por tanto, con trazas y normas. Además $\mathrm{tr}(p'/p)=N(p)'/N(p)$, luego

$$(\dim_K K(u))\cdot f=\mathrm{tr}(f)=(\mathrm{tr}\,q)'+c_1\frac{N(p_1)'}{N(p_1)}+\ldots+c_n\frac{N(p_n)'}{N(p_n)}.$$

Caso u trascendente:

(1) Si u es una exponencial: $u'=g'u$.

El cuerpo de fracciones de $K[[u]]$ es de modo natural un cuerpo diferencial que contiene a $K(u)$. Observemos que $(hu^n)'=(h'+hng')u^n$, así que disponemos de una "traza", $\mathrm{tr}(\sum f_iu^i):=f_0$ $(\sum f_iu^i\in K((u)))$, que también es compatible con las derivaciones de K y $K(u)$, y se concluye de igual modo que en el caso algebraico, ya que si $v=f_nu^n+f_{n+1}u^{n+1}+\ldots$, entonces

$$\mathrm{tr}\frac{v'}{v}=(ng)'+\frac{f_n'}{f_n}.$$

(2) Si u es un logaritmo: $u'=g'/g$.

Descomponiendo las funciones racionales $p_i(u)$ en factores irreducibles podemos suponer que son polinomios mónicos irreducibles o constantes. Descomponiendo $q(u)$ en fracciones simples tenemos:

$$(*)\qquad f=\sum\left(\frac{s_j(u)}{t_j(u)^r}\right)'+c_1\frac{p_1(u)'}{p_1(u)}+\ldots+c_n\frac{p_n(u)'}{p_n(u)}$$

Según el lema 14.9.33, la derivada $p(u)'$ de un polinomio es otro polinomio de igual grado, ó baja en una unidad si el coeficiente de mayor grado es constante. Por tanto, las fracciones $p_i(u)'/p_i(u)$ son simples. Por otra parte

$$\left(\frac{s(u)}{t(u)^r}\right)' = -r\frac{s(u)\cdot t(u)'}{t(u)^{r+1}} + \dots$$

y $t(u)$ no divide a $s(u)\cdot t(u)'$. Como $f \in K$, entonces $r = 0$, los polinomios $p_i(u) \in K$ y $q(u)$ es un polinomio tal que $q(u)' \in K$; por el lema 14.9.33, $q(u) = cu + h$, con $c \in \mathbb{C}$, $h \in K$, y concluimos que $f = h' + c(g'/g) + c_1(p_1'/p_1) + \dots + c_n(p_n'/p_n)$. □

33. Lema: *Si u es trascendente y $u' = g \in K$, el grado de $p(u)'$ coincide con el de $p(u)$, salvo que el primer coeficiente sea constante, caso en que el grado baja en una unidad, además, $p(u)$ no divide a $p(u)'$.*

Demostración. $(f_0u^n + f_1u^{n-1} + \dots)' = f_0'u^n + (nf_0g + f_1')u^{n-1} + \dots$ solo baja de grado cuando $f_0' = 0$. En este caso, si $0 = nf_0g + f_1' = (nf_0u + f_1)'$, se contradice el carácter trascendente de u.

Veamos que $p(u)$ no divide a $p(u)'$: Multiplicando por una función $h \in K$ podemos suponer que $p(u)$ es mónico. En tal caso el grado de $p(u)'$ es menor que el de $p(u)$ y éste no divide a aquel. □

Para averiguar cuándo una función es integrable por funciones elementales nos falta averiguar cuándo satisface la condición del Teorema de Liouville. Cuando al cuerpo de funciones racionales $\mathbb{C}(x)$ se le adjunta una exponencial o un logaritmo (trascendentes) sí puede decidirse (véase ejemplo), descomponiendo f en fracciones simples y usando el lema 14.9.33 en el caso de un logaritmo y el lema 14.9.34 en el de una exponencial.

34. Lema: *Si u es trascendente y $u' = gu$, con $g \in K$, entonces la derivada de cualquier monomio $h_nu^n \neq 0$ es un monomio no nulo de igual grado, y la derivada de un polinomio $p(u)$ solo es múltiplo de $p(u)$ cuando éste es un monomio.*

Demostración. $(h_nu^n)' = (h_n' + nh_ng)u^n$, y su anulación implica que h_nu^n es constante y contradice el carácter trascendente de u. Si $p(u) = \sum_i h_iu^i$ no es un monomio y su derivada es múltiplo suyo, entonces existe un par de índices n, m, con $h_n, h_m \neq 0$ y

$$\frac{h_n' + nh_ng}{h_n} = \frac{h_m' + mh_mg}{h_m}$$

Entonces $(n-m)(u'/u) = (n-m)g = (h'_m/h_m) - (h'_n/h_n)$, luego

$$(u^{n-m})'/u^{n-m} = (h_m/h_n)'/(h_m/h_n)$$

y $u^{n-m} = c\cdot(h_m/h_n)$, lo que vuelve a contradecir el carácter trascendente de u. □

35. Ejemplo: Vamos a estudiar si la integral $\int f(x)e^{g(x)}dx$ es elemental, donde $f(x)$ y $g(x)$ son funciones racionales. Sea $K := \mathbb{C}(x, e^g)$ y $u := e^g$ (luego $u' = g'u$). Si $g(x)$ no es constante, entonces u es trascendente sobre $\mathbb{C}(x)$ pues e^g tiene una singularidad esencial en cualquier polo de g. Si la integral $\int f(x)e^{g(x)}dx$ es elemental, entonces

$$fu = q(u)' + c_1\frac{p_1(u)'}{p_1(u)} + \ldots + c_n\frac{p_n(u)'}{p_n(u)}$$

Podemos suponer que los p_i son irreducibles y mónicos o están en $\mathbb{C}(x)$. Descomponiendo $q(u)$ en fracciones simples y derivando, por el lema 14.9.34, $p_i(u) = u$ ó está en $\mathbb{C}(x)$, y $q(u) = \sum_i h_i(x)u^i$. Luego $q(u) = z(x)u$ para alguna función racional $z(x)$, y concluimos que $fu = (z' + g'z)u$. Es decir, la ecuación diferencial

$$z' + g'z = f$$

tiene alguna solución racional $z(x) \in \mathbb{C}(x)$. Recíprocamente, si $z(x)$ es una de tales soluciones, la integral $\int fe^g dx = ze^g$ es elemental. La existencia de soluciones racionales de esta ecuación puede decidirse descomponiendo en fracciones simples. Veamos algunos ejemplos: $\int e^{x^2}dx$ origina la ecuación $z' + 2xz = 1$, cuya solución ha de ser un polinomio, lo que es imposible. Tal integral no es una función elemental. $\int x^{-1}e^x dx$ origina la ecuación $z' + z = x^{-1}$, que claramente no tiene solución racional. No es una función elemental.

Con el cambio $y = e^x$ obtenemos que $\int \frac{dy}{\ln y}$ no es una función elemental. Como esta integral se obtiene al integrar por partes $\int \ln(\ln x)dx$, ésta tampoco es una función elemental.

36. Ejercicio: $\int x^{-1}\operatorname{sen} x\,dx$ no es una función elemental.

Veamos ahora el **caso algebraico**.

Sea $K = \mathbb{C}(x,y)$ donde y es algebraico sobre $\mathbb{C}(x)$. Dada una 1-forma diferencial $\omega = f(x,y)dx$, consideramos una $\mathbb{Z}$-base $\{r_1,\ldots,r_s\}$ del subgrupo aditivo de $\mathbb{C}$ generado por los residuos de w en los distintos puntos de la variedad de Riemann de K. Sean $D_1,\ldots,D_s$ los divisores, donde el coeficiente de D_i en un punto p es el coeficiente del residuo de ω en p en r_i.

Si la integral $\int\omega$ es elemental, entonces: los divisores $D_1,\ldots,D_s$ definen elementos de torsión en la variedad jacobiana, $m_iD_i = D(g_i)$, y existe una función meromorfa $h\in K$ tal que

$$\omega = dh + \sum_{i=1}^{s} \frac{r_i}{m_i}\frac{dg_i}{g_i}$$

En efecto, de acuerdo con el Teorema de Liouville tenemos

$$\omega = dh + \sum_j c_j \frac{dh_j}{h_j} \quad , \quad c_j\in\mathbb{C}$$

y considerando una base $\{r_1,\ldots,r_s,a_1,\ldots\}$ del $\mathbb{Q}$-espacio vectorial que generan los residuos y las constantes c_j tendremos:

$$\begin{aligned} c_j &= \Big(\sum_i \frac{m_{ij}}{m_i}r_i\Big) + \frac{n_{1j}}{n_1}a_1 + \ldots \\ \omega &= dh + \sum_i r_i\Big(\sum_j \frac{m_{ij}}{m_i}\frac{dh_j}{h_j}\Big) + a_1\Big(\sum_j \frac{n_{1j}}{n_1}\frac{dh_j}{h_j}\Big) + \ldots \\ &= dh + \sum_i \frac{r_i}{m_i}\frac{dg_i}{g_i} + \frac{a_1}{n_1}\frac{dv_1}{v_1} + \ldots \end{aligned}$$

donde $g_i = \prod_j h_j^{m_{ij}}$ y $v_1 = \prod_j h_j^{n_{1j}}$. Considerando el residuo de ω en cualquier cero de v_1 vemos que éstos no existen. Luego,

$$\omega = dh + \sum_{i=1}^{s} \frac{r_i}{m_i}\frac{dg_i}{g_i}$$

y al observar que el residuo de $(df)/f$ en un punto p es precisamente el coeficiente en p del divisor $D(f)$, concluimos que

$$D_i = \frac{D(g_i)}{m_i}.$$

Si existen otros $\bar{m}_i$ y $\bar{g}_i$ de modo que $\bar{m}_iD_i = D(\bar{g}_i)$ entonces $\frac{D(g_i)}{m_i} = \frac{D(\bar{g}_i)}{\bar{m}_i}$. Por tanto, $g_i^{\bar{m}_i} = \lambda\cdot\bar{g}_i^{m_i}$, para cierto $\lambda\in\mathbb{C}$, luego $\frac{r_i}{\bar{m}_i}\frac{d\bar{g}_i}{\bar{g}_i} = \frac{r_i}{m_i}\frac{dg_i}{g_i}$ y

$$\omega = dh + \sum_{i=1}^{s} \frac{r_i}{\bar{m}_i}\frac{d\bar{g}_i}{\bar{g}_i}.$$

Nota: Aunque aparentemente este resultado solo sea una condición necesaria para que una integral $\int\omega$ sea elemental, realmente es una caracterización, y permite averiguar el carácter elemental de $\int\omega$ (siempre que se sepa decidir cuándo un elemento de la jacobiana es de torsión):

Primero se calculan los residuos de ω y los correspondientes divisores D_i. Si alguno no es de torsión, la integral no es elemental. Si todos son de torsión, $m_i D_i = D(g_i)$, consideramos la forma diferencial

$$\theta := \omega - \sum_{i=1}^{s} \frac{r_i}{m_i} \frac{dg_i}{g_i}$$

y el resultado anterior afirma que θ es exacta precisamente cuando la integral $\int \omega$ es elemental. Esta forma diferencial θ ya tiene residuo nulo en todo punto así que las partes principales de sus polos pueden integrarse y obtenemos unos desarrollos de Laurent δ_p. Podemos decidir si tales desarrollos de Laurent son los de alguna función meromorfa $h \in K$ (pues tal condición equivale a que $\sum_p \mathrm{res}_p(\delta_p \omega_i) = 0$ para toda forma diferencial regular ω_i). Si no existe tal función h, la integral no es elemental. Si existe, es única salvo la adición de una constante, y la integral $\int \omega$ es elemental si y solo si $\theta = dh$.

37. Ejemplo: Si ω es regular, ya tiene residuo nulo en todo punto. En tal caso $\theta = \omega$; luego los desarrollos de Laurent δ_p son idénticamente nulos y $h = 0$. Concluimos que la integral $\int \omega$ es elemental si y solo si $\omega = 0$. *Ninguna forma diferencial regular no nula tiene integral elemental.*

En particular, las integrales elípticas

$$\int \frac{dx}{\sqrt{x(x-1)(x-c)}} \quad , \quad c \neq 0, 1$$

no son elementales.

14.10. Problemas

Supondremos siempre que el cuerpo base es algebraicamente cerrado y que las curvas consideradas son completas y no singulares, salvo mención expresa contraria.

1. Sea k de característica cero. Sea C una curva proyectiva plana no singular de grado n. Probar que el número de tangentes que se pueden trazar desde un punto $p \notin C$ del plano proyectivo a la curva es $2n + 2g - 2$, siendo n el grado de la curva y g el género de la curva. Calcular el número de tangentes que se pueden trazar desde un punto $p \in C$.

2. En el ejercicio anterior admitamos que C tenga puntos singulares de multiplicidad 2 que desingularizan con la primera explosión. Entonces el número de tangentes es $2n + 2g - 2 - K$, siendo K el número de cúspides de C.

3. Sea $C \subset \mathbb{P}^2$ una curva proyectiva plana no singular de grado d, sobre un cuerpo algebraicamente cerrado de característica cero. Para cada punto $x \in C$, sea T_xC la recta tangente a C en x. Consideremos T_pC como un punto del plano proyectivo dual $\mathbb{P}^{2^*}$. El morfismo $\phi\colon C \to \mathbb{P}^{2^*}$, $\phi(x) = T_xC$, define un morfismo de C en su *curva dual* C^*. *Calcular el grado de* C^*. *Calcular el número de puntos de inflexión de* C, *considérese para ello el morfismo* $C \to R$, $x \mapsto T_xC \cap R$, *donde* R *es cualquier recta de* $\mathbb{P}^2$.

4. *Sea* C *una curva no singular y* $p_1, \cdots, p_n \in C$ *puntos cerrados. Probar que el abierto* $C \setminus \{p_1, \cdots, p_n\}$ *es una curva afín.*

5. *Sea* C *una curva completa no singular y* $C \setminus \{p_1, \cdots, p_n\} = \operatorname{Spec} A$.

   a) *Probar que* A *es un dominio de ideales principales* $\iff$ *Para todo* $p \in C$ *entonces* $p \sim \sum n_i p_i \iff \operatorname{Pic} C = \sum_i \mathbb{Z} p_i$.

   b) *Probar que* A *es un dominio de ideales principales si y solo si* C *tiene género cero.*

6. *Sea* $\pi\colon C \to C'$ *un revestimiento de Galois entre curvas, sobre un cuerpo de característica cero. Sea* G *el grupo de Galois de* π *y* $n = \#G$. *Sean* $p_1, \ldots, p_s$ *un conjunto maximal de puntos de ramificación de* C *cuyas imágenes por* π *sean distintas. Sean* $r_i = e_{p_i}$ *los índices de ramificación de los* p_i. *Probar que*

$$\frac{2g_C - 2}{n} = 2g_{C'} - 2 + \sum_{i=1}^{s} (1 - \frac{1}{r_i})$$

   Probar que si $g_C \geq 2$ *el valor mínimo de* $2g_{C'} - 2 + \sum_{i=1}^{s} (1 - \frac{1}{r_i})$ *es* $\frac{1}{42}$ *y concluir que* $n \leq 84(g_C - 1)$. *Probar que el orden del grupo de automorfismos de una curva de género* g *mayor o igual que dos es menor igual que* $84(g_C - 1)$.

7. *Probar que la condición necesaria y suficiente para que una curva tenga estructura de grupo es que sea de género* 1 *(sobre un cuerpo de característica cero).*

8. *Sea* k *un cuerpo algebraicamente cerrado de característica cero. Sea* C *una cúbica proyectiva plana no singular. Probar que cada par de puntos de* C *es un par de los tres puntos de contacto de cuatro cónicas tritangentes a* C.

9. *Sea* C *una cónica irreducible del plano proyectivo. Probar que todo automorfismo de* C *levanta a un automorfismo del plano proyectivo.*

10. *Probar que la inclusión de una curva no singular plana proyectiva de grado* 4 *en el plano proyectivo es la inmersión canónica.*

11. *Sea* C *la curva hiperelíptica birracional a* $y^2 = \prod_{i}^{2g+1} (x-\alpha_i)$. *Probar que* $\Gamma(C, \Omega_{C/k}) = \{\sum_{i=0}^{g-1} \lambda_i \frac{x^i dx}{y}\}$. *Expresar en coordenadas el morfismo canónico de* C.

12. *Sea* C *una cúbica proyectiva compleja plana. Probar que desde un punto* p *(que no sea de inflexión) de la cúbica se pueden trazar cuatro tangentes. Demostrar que la cónica que pasa por los cuatro puntos de tangencia y* p, *es tangente a la cúbica en* p.

13. *Sea* C *una curva completa no singular sobre un cuerpo algebraicamente cerrado de característica cero. Probar que si existe una función* $f \in \Sigma_C$, *de modo que* f *y* df *solo tienen un único polo y un único cero en lo mismos puntos, entonces puntos, entonces* $C = \mathbb{P}^1$.

14. *Sea* C *una curva de género* g *y* $x \in C$. *Probar que existen exactamente* g *números naturales* $0 \leq n_1 < \ldots < n_g < 2g$ *de modo que no existe una función meromorfa con un único polo, de orden* n_i *en* x. *Se dice que* x *es de Weierstrass si y solo si* $n_g \neq g$. *Demostrar que* x *es de Weierstrass si y solo si existe una diferencial holomorfa con un cero de orden* g *en* x.

15. *Probar que toda curva se puede meter como una curva cerrada en un espacio proyectivo* $\mathbb{P}^3$.

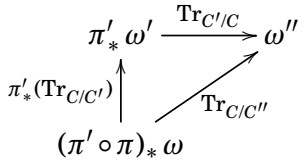
16. *Sea* C *una cúbica alabeada de* $\mathbb{P}^3$. *Sea* C' *otra curva y* $\phi\colon C \to C'$ *un morfismo de grado* 3. *Demostrar que cada fibra de* ϕ *es la intersección de* C *con cada uno de los planos de un haz de planos.*

17. *Sea* C *una curva plana de ecuación* $x^4 + y^4 - 1 = 0$. *Demostrar que* 4 *puntos de la curva son el divisor de ceros de una diferencial holomorfa si y solo si están alineados.* ($\operatorname{car} k \neq 2$).

18. *Sea* C *la desingularización de* $y^5+3x^4y+x^2+xy = 0$. *Dados* 4 *puntos arbitrarios de la curva existe una diferencial holomorfa que tiene ceros en esos cuatro puntos. Existe una diferencial holomorfa con ceros en* 8 *puntos si y solo si los* 8 *puntos yacen en una cónica que pasa por el origen.*

19. *Toda cuártica de género* 1 *en* $\mathbb{P}^3$ *es intersección de dos cuádricas.*

20. Sean $C \xrightarrow{\pi} C' \xrightarrow{\pi'} C''$ morfismos finitos entre curvas completas. Con las notaciones obvias, se cumple que el siguiente diagrama es conmutativo



Resolución: Con las notaciones obvias, se verifica que

$$\mathrm{Tr}^*_{C/C''}(\mathrm{res}'') = \mathrm{res} \quad y \quad (\mathrm{Tr}_{C'/C''} \circ \pi'_*(\mathrm{Tr}_{C/C'}))^*(\mathrm{res}'') = (\pi'_*(\mathrm{Tr}_{C/C'}))^*(\mathrm{res}') = \mathrm{res}$$

y se concluye por dualidad.

Capítulo 15

Teoría de la dualidad

15.1. Introducción

Sea X una variedad proyectiva de dimensión n sobre un cuerpo k. Consideremos los espacios vectoriales finito generados $H^i(X,\mathscr{O}_X)^*$. El objetivo de la teoría de la dualidad es ver que estos espacios vectoriales vuelven a ser de naturaleza cohomológica, es decir, son la cohomología de un haz. Con más precisión, existe un haz quasi-coherente ω_X tal que $H^i(X,\mathscr{O}_X)^* = H^{n-i}(X,\omega_X)$. Con más generalidad, para todo módulo quasi-coherente $\mathscr{M}$, se cumple que

$$H^i(X,\mathscr{M})^* = \mathrm{Ext}^{n-i}_{\mathscr{O}_X}(\mathscr{M},\omega_X)$$

de modo funtorial en $\mathscr{M}$. El problema es demostrar la existencia de ω_X y dar su estructura.

Dado que los grupos de cohomología y los extens se obtiene tomando H^i en ciertos complejos, es natural plantear el problema de la dualidad a nivel de complejos, antes de tomar cohomología: dado $\mathscr{M}$, lo resolveremos funtorialmente por un complejo de módulos acíclicos $C^{\cdot}\mathscr{M}$, (recordemos que $H^i(\Gamma(X,C^{\cdot}\mathscr{M})) = H^i(X,\mathscr{M})$) y plantearemos la representabilidad del funtor

$$\mathscr{M} \rightsquigarrow \mathrm{Hom}_k(\Gamma(X,C^{\cdot}\mathscr{M}),k).$$

El representante de este funtor será un complejo D_X denominado complejo dualizante. El módulo ω_X se obtendrá tomando homología en dicho complejo. De hecho, se probará que si la variedad es Cohen-Macaulay, entonces $D_X[-n] \equiv \omega_X$, donde $\equiv$ quiere decir cuasi-isomorfismo.

Para determinar la estructura del dualizante será necesario ponerse en un marco más general y natural: construir el complejo dualizante $D_{X/S}$ para un morfismo propio

$X \to S$ y no sólo restringirse al caso en que S es un cuerpo. La estructura del complejo dualizante será consecuencia de su comportamiento respecto a dos tipos de morfismos básicos: los morfismos finitos y los cambios de base planos. Se seguirá la siguiente línea argumental: Dada la variedad X, consideremos un punto cerrado $x \hookrightarrow X$. Es elemental que $D_x \equiv k$. De la definición del dualizante se obtendrá fácilmente la relación del dualizante de X con el dualizante de x y el dualizante de la inmersión cerrada $x \hookrightarrow X$ (que es un morfismo finito). Así por ejemplo, si X es una variedad lisa, obtendremos que $\omega_{x/X} \otimes_{\mathscr{O}_X} \omega_X \simeq \omega_x = k$ y que $\omega_{x/X} \simeq \Lambda^n(\mathfrak{m}_x/\mathfrak{m}_x^2)^*$. Por tanto, $\omega_X \otimes_{\mathscr{O}_X} \mathscr{O}_X/\mathfrak{m}_x \simeq \Lambda^n(\mathfrak{m}_x/\mathfrak{m}_x^2)$. Es decir, la fibra de ω_X en x coincide con el álgebra exterior máxima del módulo de las diferenciales de Kähler en x. Para demostrar que el dualizante de una variedad lisa coincide con el álgebra exterior máxima del módulo de las diferenciales de Kähler tendremos que pasar del punto particular x a un punto general. Precisando algo más, en vez de considerar la inmersión $x \hookrightarrow X$ tendremos que considerar la inmersión diagonal $X \hookrightarrow X \times X$, y en vez de considerar la variedad $X \to \operatorname{Spec} k$, deberemos considerar el morfismo $X \times X \to X$.

15.2. Preliminares

En esta sección probamos algunos resultados de carácter técnico que serán utilizados más adelante. Recomendamos al lector que pase directamente a la sección siguiente y vuelva a ésta cuando sea necesario.

Cuando hablemos de $\mathscr{O}_X$-módulos coherentes supondremos que X es un esquema noetheriano.

1. Proposición: *Sea $K^\cdot$ un complejo superiormente acotado de haces de $\mathscr{O}_X$-módulos cuasi-coherentes de homología coherente. Existe un subcomplejo de haces coherentes $K'^\cdot \hookrightarrow K^\cdot$ cuasi-isomorfo a $K^\cdot$.*

Demostración. Procedamos recurrentemente. Basta ver que si K^i es coherente para $i > s$ podemos construir un subcomplejo $K'^\cdot$, con $K'^i = K^i$ para $i > s$ y K'^s coherente, cuasi-isomorfo a $K^\cdot$.

Consideremos el diagrama

$$\cdots \to K^{s-1} \xrightarrow{d_{s-1}} K^s \xrightarrow{d_s} K^{s+1} \to \cdots$$

Sea $\mathscr{M} \subseteq K^s$ un módulo coherente tal que $d_s(\mathscr{M}) = d_s(K_s)$ y sea $\mathscr{M}' \subseteq \operatorname{Ker} d_s \subseteq K^s$ un módulo coherente tal que $\overline{\mathscr{M}}' = \operatorname{Ker} d_s / \operatorname{Im} d_{s-1}$. Sea

$$K'^s := \mathscr{M} + \mathscr{M}', K'^{s-1} := d_{s-1}^{-1}(\mathscr{M} + \mathscr{M}') \text{ y } K'^i = K^i, \text{ para } i \neq s, s-1.$$

$K'^\cdot$ es el subcomplejo buscado (compruébese). □

2. Proposición: *Se cumple:*

1. Si $f: K^\cdot \to L^\cdot$ es un cuasi-isomorfismo entre complejos inferiormente acotados de haces flascos, entonces $f(U): K^\cdot(U) \to L^\cdot(U)$ es un cuasi-isomorfismo, para todo abierto U. Lo mismo es cierto si f es un cuasi-isomorfismo entre complejos inferiormente acotados de módulos cuasi-coherentes sobre un esquema y U es un abierto afín.

2. Si $f: K^\cdot \to L^\cdot$ es un cuasi-isomorfismo entre complejos superiormente acotados e $I^\cdot$ es un complejo inferiormente acotado de inyectivos, entonces los morfismos inducidos

$$\underline{\mathrm{Hom}}^\cdot(L^\cdot, I^\cdot) \to \underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot)$$
$$\mathrm{Hom}^\cdot(L^\cdot, I^\cdot) \to \mathrm{Hom}^\cdot(K^\cdot, I^\cdot)$$

son cuasi-isomorfismos. Análogamente, si $f: K^\cdot \to L^\cdot$ es un cuasi-isomorfismo entre complejos inferiormente acotados y $P^\cdot$ es un complejo superiormente acotado de localmente libres, entonces el morfismo inducido

$$\underline{\mathrm{Hom}}^\cdot(P^\cdot, L^\cdot) \to \underline{\mathrm{Hom}}^\cdot(P^\cdot, K^\cdot)$$

es un cuasi-isomorfismo.

3. Si $K^\cdot$ es un complejo superiormente acotado de haces quasi-coherentes de homología coherente e $I^\cdot$ es un complejo inferiormente acotado de haces quasi-coherentes inyectivos, entonces $\underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot)$ es un complejo de haces de homología quasi-coherente. Además, si $\phi: X \to Y$ es un morfismo plano y $J^\cdot$ es una resolución inyectiva de $\phi^* I^\cdot$, entonces el morfismo

$$\phi^* \underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot) \to \underline{\mathrm{Hom}}^\cdot(\phi^* K^\cdot, J^\cdot)$$

es un cuasi-isomorfismo.

Demostración. 1. El cono de f es un complejo acíclico inferiormente acotado de haces flascos. Por tanto $\Gamma(U, \mathrm{Cono}(f))$ es acíclico. De la igualdad $\Gamma(U, \mathrm{Cono}(f)) = \mathrm{Cono}(f(U))$, se concluye. Análogamente para la segunda parte.

2. $\underline{\mathrm{Hom}}^\cdot(L^\cdot, I^\cdot)$ y $\underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot)$ son bicomplejos. Por ser $I^\cdot$ un complejo de inyectivos, tenemos que

$$H_{d_1}(\underline{\mathrm{Hom}}^\cdot(L^\cdot, I^\cdot)) = \underline{\mathrm{Hom}}^\cdot(H_d(L^\cdot), I^\cdot) = \underline{\mathrm{Hom}}^\cdot(H_d(K^\cdot), I^\cdot) = H_{d_1}(\underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot))$$

luego por 7.2.17, $\underline{\mathrm{Hom}}^\cdot(L^\cdot, I^\cdot) \to \underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot)$ es un cuasi-isomorfismo. Para los demás cuasi-isomorfismos se argumenta del mismo modo.

3. Por la proposición anterior, existe un subcomplejo de haces coherentes $K'^\cdot \hookrightarrow K^\cdot$ cuasi-isomorfo a $K^\cdot$. Igual que en 2.

$$\underline{\mathrm{Hom}}^\cdot(K^\cdot, I^\cdot) \to \underline{\mathrm{Hom}}^\cdot(K'^\cdot, I^\cdot)$$

es cuasi-isomorfismo, luego $\underline{\mathrm{Hom}}^{\cdot}(K^{\cdot}, I^{\cdot})$ tiene homología quasi-coherente.

Para la segunda parte, observemos que la cuestión es local, luego podemos suponer que tenemos una resolución $P^{\cdot} \to K'^{\cdot}$ por libres. Ahora, por ser ϕ plano, $I^{\cdot}$ y $J^{\cdot}$ inyectivos, $\phi^* P^{\cdot}$ proyectivo y por 7.2.17 tenemos los cuasi-isomorfismos

$$\begin{aligned}\phi^* \underline{\mathrm{Hom}}^{\cdot}(K^{\cdot}, I^{\cdot}) \equiv \phi^* \underline{\mathrm{Hom}}^{\cdot}(K'^{\cdot}, I^{\cdot}) \equiv \phi^* \underline{\mathrm{Hom}}^{\cdot}(P^{\cdot}, I^{\cdot}) = \underline{\mathrm{Hom}}^{\cdot}(\phi^* P^{\cdot}, \phi^* I^{\cdot}) \\ \equiv \underline{\mathrm{Hom}}^{\cdot}(\phi^* P^{\cdot}, J^{\cdot}) \equiv \underline{\mathrm{Hom}}^{\cdot}(\phi^* K^{\cdot}, J^{\cdot}).\end{aligned}$$

□

3. Observación: El apartado 2. es igualmente cierto si los complejos considerados son de haces quasi-coherentes, en el primer cuasisomorfismo debemos suponer que el esquema es noetheriano para poder afirmar que los módulos quasi-coherentes inyectivos son localmente inyectivos (ver 12.1.29).

En el apartado 3., si $I^{\cdot}$ es una resolución por inyectivos de un haz quasi-coherente $\mathscr{M}$, entonces $J^{\cdot}$ es una resolución por inyectivos de $\phi^* \mathscr{M}$. Este será el caso que utilizaremos más adelante.

4. Proposición: *Sea X un esquema noetheriano semiseparado, U un abierto afín de X y $\mathfrak{p}$ el ideal coherente de las funciones que se anulan en $X - U$. Si $K^{\cdot}$ es un complejo superiormente acotado de haces quasi-coherentes y homología coherente e $I^{\cdot}$ es un complejo inferiormente acotado de haces quasi-coherentes inyectivos, entonces el morfismo natural*

$$\varinjlim_i \mathrm{Hom}_X(\mathfrak{p}^i, \underline{\mathrm{Hom}}^{\cdot}(K^{\cdot}, I^{\cdot})) \to \mathrm{Hom}^{\cdot}(K^{\cdot}_{|U}, I^{\cdot}_{|U})$$

es un cuasi-isomorfismo.

Demostración. Denotemos $R^{\cdot} = \underline{\mathrm{Hom}}^{\cdot}(K^{\cdot}, I^{\cdot})$. Tenemos que ver que el morfismo natural

$$\varinjlim_i \mathrm{Hom}_X(\mathfrak{p}^i, R^{\cdot}) \to \Gamma(U, R^{\cdot})$$

es un cuasi-isomorfismo. Sea $K' \hookrightarrow K$ un subcomplejo coherente cuasi-isomorfo a $K^{\cdot}$ y $R'^{\cdot} = \underline{\mathrm{Hom}}^{\cdot}(K'^{\cdot}, I^{\cdot})$). Se tiene un diagrama conmutativo

$$\begin{array}{ccc} \varinjlim_i \mathrm{Hom}_X(\mathfrak{p}^i, R^{\cdot}) & \longrightarrow & \Gamma(U, R^{\cdot}) \\ \downarrow & & \downarrow \text{cuasi} \\ \varinjlim_i \mathrm{Hom}_X(\mathfrak{p}^i, R'^{\cdot}) & \xrightarrow[12.1.27]{\sim} & \Gamma(U, R'^{\cdot}) \end{array}$$

donde el "cuasi" se debe a que $R^{\cdot} \to R'^{\cdot}$ es un cuasi-isomorfismo entre complejos de haces flascos (ver la proposición 12.1.28). Basta probar que el morfismo

$$\varinjlim_i \operatorname{Hom}_X(\mathfrak{p}^i, R^{\cdot}) \to \varinjlim_i \operatorname{Hom}_X(\mathfrak{p}^i, R'^{\cdot})$$

es cuasi-isomorfismo.

1) Si X es afín, el cuasi-isomorfismo $R^{\cdot}(X) \to R'^{\cdot}(X)$ induce un cuasi-isomorfismo (por 1. de 15.2.2)

$$\begin{aligned}\varinjlim_i \operatorname{Hom}_X(\mathfrak{p}^i, R^{\cdot}) &= \varinjlim_i \operatorname{Hom}_X(\mathfrak{p}^i, \widetilde{R^{\cdot}(X)}) = \Gamma(U, \widetilde{R^{\cdot}(X)}) \xrightarrow{\text{cuasi}} \Gamma(U, \widetilde{R'^{\cdot}(X)}) \\ &= \varinjlim_i \operatorname{Hom}_X(\mathfrak{p}^i, R'^{\cdot}).\end{aligned}$$

2) Caso general. El morfismo natural $\varinjlim_i \underline{\operatorname{Hom}}_X(\mathfrak{p}^i, R^{\cdot}) \to \varinjlim_i \underline{\operatorname{Hom}}_X(\mathfrak{p}^i, R'^{\cdot})$ es cuasi-isomorfismo, pues lo es al tomar secciones en todo abierto afín (por 1)). Además ambos complejos son de haces flascos (pruébese). Tomando secciones globales se concluye. □

5. Proposición: *Sea X un esquema noetheriano y $f : K^{\cdot} \to L^{\cdot}$ un morfismo de complejos de $\mathcal{O}_X$-módulos quasi-coherentes. Si para todo $\mathcal{O}_X$-módulo coherente $\mathcal{M}$ el morfismo inducido $\operatorname{Hom}_X(\mathcal{M}, K^{\cdot}) \to \operatorname{Hom}_X(\mathcal{M}, L^{\cdot})$ es un cuasi-isomorfismo, entonces f es un cuasi-isomorfismo.*

Demostración. Sea U un abierto de X y $\mathfrak{p}$ el haz de ideales coherente de las funciones que se anulan en $X - U$. Tomando $\mathcal{M} = \mathfrak{p}^n$ y límite inductivo se tiene un cuasi-isomorfismo

$$\Gamma(U, K^{\cdot}) \to \Gamma(U, L^{\cdot})$$

luego $K^{\cdot} \to L^{\cdot}$ es un cuasi-isomorfismo. □

15.3. Dualizante

Sea S un esquema noetheriano semiseparado y $f : X \to S$ un morfismo propio. Sea $\{U_i\}$ un recubrimiento finito de X por abiertos afines sobre S. Denotaremos por $C^{\cdot}\mathcal{M}$ el complejo de haces de Cech del módulo quasi-coherente $\mathcal{M}$ asociado al recubrimiento $\{U_i\}$. El funtor sobre la categoría de módulos quasi-coherentes sobre X que asocia a cada módulo quasi-coherente $\mathcal{M}$ el i-ésimo módulo quasi-coherente de Cech, $C^i\mathcal{M}$, es

un funtor exacto y conmuta con límites inductivos. Por la aciclicidad de los módulos quasi-coherentes en los esquemas afines y la conmutación de las secciones con límite inductivo, obtenemos que el funtor $\mathscr{M} \rightsquigarrow f_*(C^i\mathscr{M})$ es exacto y conmuta con límites inductivos.

1. Existencia del complejo dualizante: *Para cada complejo inferiormente acotado $I^\cdot$ de $\mathscr{O}_S$-módulos inyectivos quasi-coherentes, existe un complejo inferiormente acotado $f^!I^\cdot$ de $\mathscr{O}_X$-módulos inyectivos quasi-coherentes tal que, para todo $\mathscr{O}_X$-módulo quasi-coherente $\mathscr{M}$, se cumple que*

$$\mathrm{Hom}^\cdot_X(\mathscr{M}, f^!I^\cdot) = \mathrm{Hom}^\cdot_S(f_*(C^\cdot\mathscr{M}), I^\cdot).$$

funtorialmente en $\mathscr{M}$.

Demostración. Sea $I^\cdot$ un complejo inferiormente acotado de $\mathscr{O}_S$-módulos quasi-coherentes inyectivos. Dado que $C^\cdot\mathscr{M}$ es un complejo acotado, el complejo de homomorfismos $\mathrm{Hom}^\cdot_S(f_*(C^\cdot\mathscr{M}), I^\cdot)$ vale, en grado n,

$$\mathrm{Hom}^n_S(f_*(C^\cdot\mathscr{M}), I^\cdot) = \bigoplus_p \mathrm{Hom}_S(f_*(C^p\mathscr{M}), I^{p+n})$$

El funtor $\mathscr{M} \rightsquigarrow \mathrm{Hom}^n_S(f_*(C^\cdot\mathscr{M}), I^\cdot)$ es contravariante, exacto y conmuta con límites inductivos. Por tanto, es representable por un $\mathscr{O}_X$-módulo quasi-coherente inyectivo, que denotamos $f^nI^\cdot$. La diferencial del complejo de homomorfismos

$$d\colon \mathrm{Hom}^n_S(f_*(C^\cdot\mathscr{M}), I^\cdot) \to \mathrm{Hom}^{n+1}_S(f_*(C^\cdot\mathscr{M}), I^\cdot)$$

induce una diferencial $d\colon f^nI^\cdot \to f^{n+1}I^\cdot$. Se tiene por tanto un complejo de $\mathscr{O}_X$-módulos quasi-coherentes inyectivos que denotamos $f^!I^\cdot$ y un isomorfismo de complejos

$$\mathrm{Hom}^\cdot_X(\mathscr{M}, f^!I^\cdot) = \mathrm{Hom}^\cdot_S(f_*(C^\cdot\mathscr{M}), I^\cdot)$$

funtorial en $\mathscr{M}$. □

2. Observación: Evidentemente, $f^!I^\cdot$ depende del recubrimiento $\mathscr{U} = \{U_i\}$ escogido. Deberíamos denotarlo $f^!_{\mathscr{U}}I^\cdot$. Ahora bien, es fácil probar por la proposición 15.2.5 que si $\mathscr{U}, \mathscr{V}$ son dos recubrimientos y $\mathscr{W} = \mathscr{U} \cup \mathscr{V}$, se tienen cuasi-isomorfismos

$$f^!_{\mathscr{U}}I^\cdot \to f^!_{\mathscr{W}}I^\cdot \leftarrow f^!_{\mathscr{V}}I^\cdot$$

En particular, los haces de homología de $f^!_{\mathscr{U}}I^\cdot$ no dependen del recubrimiento. Para hacer el complejo independiente del recubrimiento es necesario pasar a la categoría derivada, es decir, a la categoría donde los cuasi-isomorfismos son isomorfismos. Sin

embargo, para evitar esta complicación técnica, será más sencillo fijar un recubrimiento de X y no introducir la categoría derivada. Si $S' \to S$ es un cambio de base y $X' = X \underset{S}{\times} S'$, entonces el recubrimiento escogido en X por abiertos S-afines induce otro en X' por abiertos S'-afines. Supondremos esta elección sin más comentarios en lo que resta del capítulo.

3. Definición: Llamaremos complejo dualizante de X sobre S , y lo denotaremos $D_{X/S}$, al complejo $f^! I^\cdot$, donde $I^\cdot$ es una resolución de $\mathcal{O}_S$ por $\mathcal{O}_S$-módulos quasi-coherentes inyectivos.

Evidentemente, $D_{X/S}$ depende de la resolución inyectiva de $\mathcal{O}_S$ escogida. Si $I^\cdot$, $J^\cdot$ son dos resoluciones inyectivas de $\mathcal{O}_S$, existe un cuasi-isomorfismo (único módulo homotopías) $I^\cdot \to J^\cdot$, que induce un cuasi-isomorfismo $f^! I^\cdot \to f^! J^\cdot$. Así pues, los haces de homología no dependen de la resolución inyectiva.

La igualdad $\dot{\mathrm{Hom}}_X(\mathcal{M}, D_{X/S}) = \dot{\mathrm{Hom}}_S(f_*(C^\cdot \mathcal{M}), I^\cdot)$ se denomina isomorfismo de dualidad.

4. Ejemplo: Si $S = \mathrm{Spec}\, k$ es un cuerpo, entonces $\mathcal{O}_S$ es inyectivo y

$$\Gamma(X, C^\cdot \mathcal{M})^* = \mathrm{Hom}_X(\mathcal{M}, D_{X/k}).$$

Tomando $\mathcal{M} = \mathcal{O}_X$ y homología, se obtiene $H^i(X, \mathcal{O}_X)^* = H^{-i}(\Gamma(X, D_{X/k}))$.

5. Teorema: *Si las fibras de f tienen dimensión menor o igual que n, entonces el funtor sobre la categoría de $\mathcal{O}_X$-módulos quasi-coherentes definido por*

$$F(\mathcal{M}) = \mathrm{Hom}_S(R^n f_* \mathcal{M}, \mathcal{O}_S)$$

es representable por el $\mathcal{O}_X$-módulo quasi-coherente $H^{-n}(D_{X/S})$. En particular, se cumple que $H^{-n-i}(D_{X/S}) = 0$, para $i > 0$

Demostración. La representabilidad de F es obvia, ya que el funtor $R^n f_*$ es exacto por la derecha y conmuta con límites inductivos, luego F es exacto por la izquierda y transforma límites inductivos en proyectivos.

Sea $K^\cdot \mathcal{M}$ el complejo $f_* C^\cdot \mathcal{M}$ truncado en grado n, es decir,

$$K^i \mathcal{M} := \begin{cases} f_* C^i \mathcal{M}, & \text{para } i < n \\ \mathrm{Ker}(d_n : f_* C^n \mathcal{M} \to f_* C^{n+1} \mathcal{M}), & \text{para } i = n \\ 0 & \text{para } i > n \end{cases}$$

Por construcción, $K^\cdot \mathcal{M} \to f_* C^\cdot \mathcal{M}$ es un cuasi-isomorfismo. El funtor $\mathcal{M} \rightsquigarrow K^\cdot \mathcal{M}$ es exacto y conmuta con límites inductivos. Repitiendo la construcción de $D_{X/S}$, pero sustituyendo $f_* C^\cdot \mathcal{M}$ por $K^\cdot \mathcal{M}$, se tiene que existe un complejo $D'_{X/S}$ de $\mathcal{O}_X$-módulos

inyectivos y una igualdad $\mathrm{Hom}_X(\mathscr{M}, D'_{X/S}) = \mathrm{Hom}^{\cdot}_S(K^{\cdot}\mathscr{M}, I^{\cdot})$. Tomando grados, se concluye que $D'_{X/S}$ es nulo en grado menor que $-n$.

El cuasi-isomorfismo $K^{\cdot}\mathscr{M} \to f_*(C^{\cdot}\mathscr{M})$ induce un cuasi-isomorfismo $D_{X/S} \to D'_{X/S}$, luego un isomorfismo $H^{-n}(D_{X/S}) \simeq H^{-n}(D'_{X/S})$.

El complejo $K^{\cdot}\mathscr{M}$ es nulo en grado mayor que n y el complejo $I^{\cdot}$ es nulo en grados negativos, luego se deduce fácilmente que

$$H^{-n}\,\mathrm{Hom}^{\cdot}_S(K^{\cdot}\mathscr{M}, I^{\cdot}) = \mathrm{Hom}_S(H^n[K^{\cdot}\mathscr{M}], H^0(I^{\cdot})) = \mathrm{Hom}_S(R^n f_*\mathscr{M}, \mathscr{O}_S).$$

Por otra parte,

$$H^{-n}\,\mathrm{Hom}^{\cdot}_S(K^{\cdot}\mathscr{M}, I^{\cdot}) = H^{-n}\,\mathrm{Hom}_X(\mathscr{M}, D'_{X/S}) = \mathrm{Hom}_X(\mathscr{M}, H^{-n}(D'_{X_S}))$$

ya que $D'_{X/S}$ es un complejo nulo en grado menor que $-n$. En conclusión,

$$\mathrm{Hom}_S(R^n f_*\mathscr{M}, \mathscr{O}_S) = \mathrm{Hom}_X(\mathscr{M}, H^{-n}(D'_{X_S})) = \mathrm{Hom}_X(\mathscr{M}, H^{-n}(D_{X_S})).$$

□

6. Observación: Hasta aquí no hemos necesitado la hipótesis de que el morfismo $f: X \to S$ sea un morfismo propio, nos ha bastado con que sea separado y cuasicompacto. En lo que sigue sí será necesario, pues tendremos que utilizar que el complejo $f_*C^{\cdot}\mathscr{M}$ es de homología coherente.

7. Forma local de la dualidad: *Para todo $\mathscr{O}_X$-módulo coherente $\mathscr{M}$ se tiene un cuasi-isomorfismo*

$$f_*\,\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S}) \to \underline{\mathrm{Hom}}^{\cdot}_S(f_*(C^{\cdot}\mathscr{M}), I^{\cdot})$$

que al tomar secciones globales es el isomorfismo de dualidad. Si $U \hookrightarrow S$ es un abierto, existe un cuasi-isomorfismo $D_{X/S\,|f^{-1}(U)} \to D_{f^{-1}(U)/U}$.

Demostración. Sea U un abierto afín de S y $\mathfrak{p}$ el ideal coherente de las funciones que se anulan en $S - U$.

Como el recubrimiento considerado en X es afín sobre S, se tiene que

$$f_*(C^{\cdot}(f^*\mathfrak{p}^n \otimes \mathscr{M})) = \mathfrak{p}^n \otimes f_*(C^{\cdot}\mathscr{M}),$$

pues se reduce a ver que dado un morfismo $f: \mathrm{Spec}B \to \mathrm{Spec}A$, un ideal $I \subset A$ y un B-módulo N, entonces $(I \otimes_A B) \otimes_B N = I \otimes_A N$. Entonces

$$\begin{aligned}
\Gamma(U, f_*\,\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S})) &= \varinjlim_n \mathrm{Hom}_X(\mathfrak{p}^n, f_*\,\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S})) \\
&= \varinjlim_n \mathrm{Hom}_X(f^*\mathfrak{p}^n \otimes \mathscr{M}, D_{X/S}) = \varinjlim_n \mathrm{Hom}_S(f_*(C^{\cdot}(f^*\mathfrak{p}^n \otimes \mathscr{M})), I^{\cdot}) \\
&= \varinjlim_n \mathrm{Hom}_S(\mathfrak{p}^n \otimes f_*(C^{\cdot}\mathscr{M}), I^{\cdot}) \xrightarrow{\text{cuasi}} \Gamma(U, \underline{\mathrm{Hom}}_S(f_*(C^{\cdot}\mathscr{M}), I^{\cdot}))
\end{aligned}$$

donde el último morfismo es cuasi-isomorfismo por 15.2.4. Por tanto, se tiene un cuasi-isomorfismo $f_*\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S}) \to \underline{\mathrm{Hom}}^{\cdot}_S(f_*(C^{\cdot}\mathscr{M}), I^{\cdot})$.

Para la segunda parte, sea $V = f^{-1}(U)$. Tomando secciones en U en el cuasi-isomorfismo anterior obtenemos (por 1. de 15.2.2) un cuasi-isomorfismo

$$\mathrm{Hom}_V(\mathscr{M}_{|V}, (D_{X/S})_{|V}) \to \mathrm{Hom}^{\cdot}_U(f_{|V\,*}(C^{\cdot}\mathscr{M}_{|V}), I^{\cdot}_{|U}) = \mathrm{Hom}_V(\mathscr{M}_{|V}, D_{V/U})$$

la igualdad se debe a que $I^{\cdot}_{|U}$ es una resolución inyectiva de $\mathscr{O}_U$. Por 15.2.5 tenemos un cuasi-isomorfismo

$$D_{X/S\,|V} \to D_{V/U}.$$

□

8. Teorema: *Si las fibras de f tienen dimensión menor o igual que n, entonces*

$$f_*\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M}, H^{-n}D_{X/S}) = \underline{\mathrm{Hom}}_{\mathscr{O}_S}(R^n f_*\mathscr{M}, \mathscr{O}_S)$$

es para todo $\mathscr{O}_X$-módulo coherente $\mathscr{M}$ plano sobre S.

Demostración. Para todo ideal coherente $\mathfrak{p} \subseteq \mathscr{O}_S$, $R^n f_*(f^*\mathfrak{p} \otimes \mathscr{M}) = \mathfrak{p} \otimes R^n f_*\mathscr{M}$, por el teorema 13.11.10. Cópiese ahora la demostración del teorema anterior. □

9. Cambio de base plano: *Sea $\phi\colon S' \to S$ un cambio de base plano. Denotemos $X' = X \times_S S'$ y $\phi'\colon X' \to X$, $f'\colon X' \to S'$ las proyecciones naturales. Existe un morfismo natural $\phi'^* D_{X/S} \to D_{X'/S'}$ que es un cuasi-isomorfismo.*

Demostración. Sea $\mathscr{O}_S \to I^{\cdot}$ una resolución por $\mathscr{O}_S$-módulos quasi-coherentes inyectivos y $\phi^* I^{\cdot} \to J^{\cdot}$ una resolución inyectiva por $\mathscr{O}_{S'}$-módulos quasi-coherentes inyectivos. Entonces $J^{\cdot}$ es resolución de $\mathscr{O}_{S'}$. Para cada $\mathscr{O}_X$-módulo coherente $\mathscr{M}$ se tiene

$$\begin{aligned} f'_*\underline{\mathrm{Hom}}_{X'}(\phi'^*\mathscr{M}, \phi'^* D_{X/S}) &= f'_*\phi'^*\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S}) = \phi^* f_*\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S}) \\ &\xrightarrow{\text{cuasi}} \phi^*\underline{\mathrm{Hom}}_S(f_*(C^{\cdot}\mathscr{M}), I^{\cdot}) \xrightarrow{\text{cuasi}} \underline{\mathrm{Hom}}_{S'}(\phi^* f_*(C^{\cdot}\mathscr{M}), J^{\cdot}) = \underline{\mathrm{Hom}}_{S'}(f'_*\phi'^*(C^{\cdot}\mathscr{M}), J^{\cdot}) \\ &= \underline{\mathrm{Hom}}_{S'}(f'_*(C^{\cdot}(\phi'^*\mathscr{M})), J^{\cdot}) \xleftarrow{\text{cuasi}} f'_*\underline{\mathrm{Hom}}_{X'}(\phi'^*\mathscr{M}, D_{X'/S'}) \end{aligned}$$

donde el primer cuasi-isomorfismo es por 15.3.7, el segundo por 15.2.2 y el último por 15.3.7. Tomando secciones globales se obtiene un morfismo

$$(*) \qquad \mathrm{Hom}_{X'}(\phi'^*\mathscr{M}, \phi'^* D_{X/S}) \to \mathrm{Hom}_{X'}(\phi'^*\mathscr{M}, D_{X'/S'})$$

y por tanto un morfismo $\phi'^* D_{X/S} \to D_{X'/S'}$, que define el cuasi-isomorfismo del diagrama previo $f'_*\underline{\mathrm{Hom}}_{X'}(\phi'^*\mathscr{M}, \phi'^* D_{X/S}) \to f'_*\underline{\mathrm{Hom}}_{X'}(\phi'^*\mathscr{M}, D_{X'/S'})$. Para ver que el

morfismo $\phi'^* D_{X/S} \to D_{X'/S'}$ es cuasi-isomorfismo, podemos suponer que S y S' son afines, por 15.3.7. En este caso, el morfismo (*) es un cuasi-isomorfismo. Por adjunción, y por 15.2.5 se obtiene que $\phi'_* \phi'^* D_{X/S} \to \phi'_* D_{X'/S'}$ es un cuasi-isomorfismo. Se concluye porque ϕ' es afín. □

15.4. Cálculo del dualizante

1. Definición: Si $D_{X/S}$ tiene un único haz de homología (digamos en grado d), denotaremos

$$\omega_{X/S} = H^d(D_{X/S})$$

y diremos que es el haz dualizante de X sobre S.

2. Teorema: *Sea $Y \hookrightarrow X$ una inmersión cerrada regular de codimensión r, definida por un ideal $\mathfrak{p}_Y$. Entonces,*

$$\underline{\mathrm{Ext}}^i_{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_X) = \begin{cases} 0 & i \neq r. \\ \Lambda^r(\mathfrak{p}_Y/\mathfrak{p}_Y^2)^* & i = r. \end{cases}$$

Demostración. Procedamos localmente. Sea A un anillo, $\{a_1, \ldots, a_r\}$ una sucesión regular, $I = (a_1, \ldots, a_r)$ y L el módulo libre de base $x_1, \ldots, x_r$. Recordemos que el complejo de Koszul asociado $K(a_1, \ldots, a_r, A) = \bigoplus_i \Lambda^i L$ es acíclico y $H^0(K(a_1, \ldots, a_r, A)) = A/I$. Por tanto es una resolución de A/I por módulos libres. Recordemos además que I/I^2 es un A/I-módulo libre, por 7.4.5. Es fácil comprobar que el complejo dual $K(a_1, \ldots, a_r, A)^*$ es isomorfo a $K(a_1, \ldots, a_r, A) \otimes_A \Lambda^r L^*[r]$ y que $H^r(K(a_1, \ldots, a_r, A)^*) \simeq \Lambda^r(I/I^2)^*$. Por tanto

$$\mathrm{Ext}^i_A(A/I, A) \simeq \begin{cases} 0 & i \neq r. \\ \Lambda^r(I/I^2)^* & i = r. \end{cases}$$

Además el isomorfismo $\mathrm{Ext}^r_A(A/I, A) \simeq \Lambda^r(I/I^2)^*$ no depende de la elección de la sucesión regular, como se puede comprobar sin dificultad. Por tanto globaliza, dando el isomorfismo buscado. □

El módulo $(\mathfrak{p}_Y/\mathfrak{p}_Y^2)^*$ se denomina módulo normal de Y sobre X y se denota $\mathscr{N}_{Y/X}$.

3. Dualidad para morfismos finitos: *Sea $\pi\colon X \to X'$ un morfismo finito. Entonces*

$$\pi_* D_{X/S} = \underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, D_{X'/S}).$$

Además,

(a) $\pi_* D_{X/X'} = \underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, I^{\cdot})$*, siendo* $I^{\cdot}$ *una resolución de* $\mathscr{O}_{X'}$ *por inyectivos, luego*

$$\pi_* H^p(D_{X/X'}) = \underline{\mathrm{Ext}}^p_{\mathscr{O}_{X'}}(\pi_* \mathscr{O}_X, \mathscr{O}_{X'}).$$

(b) Si π *es una inmersión cerrada regular de codimensión* d*, entonces* $D_{X/X'}$ *tiene un único haz de homología en grado* d *y* $\omega_{X/X'} = \Lambda^d_{\mathscr{O}_X} \mathscr{N}_{X/X'}$*, siendo* $\mathscr{N}_{X/X'}$ *el módulo normal de* X *sobre* X'*.*

(c) Si π *es plano, entonces* $D_{X/X'}$ *tiene un único haz de homología en grado cero y* $\pi_* \omega_{X/X'} = \underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, \mathscr{O}_{X'})$*.*

(d) Si $D_{X'/S}$ *tiene un único haz de homología (en grado* n*),* $\omega_{X'/S}$*, y es un* $\mathscr{O}_{X'}$*-módulo plano, entonces*

$$\pi_* H^{p+n}(D_{X/S}) = \pi_* H^p(D_{X/X'}) \otimes_{\mathscr{O}_{X'}} \omega_{X'/S}\,.$$

Demostración. El morfismo π es afín, $\pi_* \pi^* \mathscr{M} = \mathscr{M} \otimes \pi_* \mathscr{O}_X$ y $\pi_* C^{\cdot}(\pi^* \mathscr{M}) = C^{\cdot}(\pi_* \pi^* \mathscr{M})$ (consideramos en X el recubrimiento obtenido tomando π^{-1} del recubrimiento de X'). Sean $f : X \to S$ y $f' : X' \to S$ los morfismo considerados. Entonces,

$$\begin{aligned}
\mathrm{Hom}_{X'}(\mathscr{M}, \pi_* D_{X/S}) &= \mathrm{Hom}_X(\pi^* \mathscr{M}, D_{X/S}) = \mathrm{Hom}_S(f_* C^{\cdot}(\pi^* \mathscr{M}), I^{\cdot}) \\
&= \mathrm{Hom}_S(f'_* \pi_* C^{\cdot}(\pi^* \mathscr{M}), I^{\cdot}) = \mathrm{Hom}_S(f'_* C^{\cdot}(\pi_* \pi^* \mathscr{M}), I^{\cdot}) \\
&= \mathrm{Hom}_{X'}(\pi_* \pi^* \mathscr{M}, D_{X'/S}) = \mathrm{Hom}_{X'}(\mathscr{M}, \underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, D_{X'/S}))
\end{aligned}$$

y hemos obtenido que $\pi_* D_{X/S} = \underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, D_{X'/S})$.

Ahora (a) es inmediato tomando $S = X'$, (b) es consecuencia del teorema anterior y (c) es inmediato. Para probar (d), basta verlo localmente en X', porque basta probar que el morfismo natural

$$\underline{\mathrm{Ext}}^p_{X'}(\pi_* \mathscr{O}_X, \mathscr{O}_{X'}) \otimes_{\mathscr{O}_{X'}} \omega_{X'/S} \to H^{p+n}(\underline{\mathrm{Hom}}_{X'}(\pi_* \mathscr{O}_X, D_{X'/S}))$$

es un isomorfismo. Sea $P_{\cdot} \to \pi_* \mathscr{O}_X$ una resolución por módulos localmente libres (existe localmente en X'), y sea $B := \underline{\mathrm{Hom}}^{\cdot}_{X'}(P_{\cdot}, D^{\cdot}_{X'/S}) = \underline{\mathrm{Hom}}_{X'}(P_{\cdot}, \mathscr{O}_{X'}) \otimes_{\mathscr{O}_{X'}} D^{\cdot}_{X'/S}$. Se tiene un cuasi-isomorfismo $\pi_* D_{X/S} \to B$. Por hipótesis, $H^q(B^{p,\cdot}) = 0$ para $q \neq n$ y $H^n(B^{p,\cdot}) = \underline{\mathrm{Hom}}_{X'}(P_p, \mathscr{O}_{X'}) \otimes_{\mathscr{O}_{X'}} \omega_{X'/S}$, luego

$$H^{p+n}(\pi_* D_{X/S}) = H^{p+n}(B) \underset{7.2.17}{=} \underline{\mathrm{Ext}}^p_{\mathscr{O}_{X'}}(\pi_* \mathscr{O}_X, \mathscr{O}_{X'}) \otimes_{\mathscr{O}_{X'}} \omega_{X'/S} = H^p(\pi_* D_{X/X'}) \otimes_{\mathscr{O}_{X'}} \omega_{X'/S}\,.$$

□

4. Teorema llave (Método de la gráfica): *Consideremos un diagrama:*

$$\begin{array}{ccc} T & \xrightarrow{\delta} & Z \xrightarrow{\phi_X} X \\ & & \downarrow \qquad \downarrow f \\ & & Y \xrightarrow{\phi} S \end{array}$$

donde el cuadrado es cartesiano ($Z = Y \underset{S}{\times} X$)*, f es propio, ϕ plano y δ es una inmersión cerrada. Si $Z \to X$ es de Gorenstein y $T \to X$ es Cohen-Macaulay (con T conexo), entonces $D_{T/Z}$ tiene un único haz de homología (en grado $n = \dim \mathscr{O}_{Z,t} - \dim \mathscr{O}_{T,t}$, para todo $t \in T$) $\omega_{T/Z} = \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z)$, que es plano, y se cumple que*

$$H^{i+n}(D_{T/Y}) = \omega_{T/Z} \otimes_{\mathscr{O}_T} \phi_T^* H^i(D_{X/S}), \qquad \phi_T := \phi_X \circ \delta.$$

Si además T es una intersección completa en Z, entonces

$$H^{i+n}(D_{T/Y}) = \phi_T^* H^i(D_{X/S}).$$

Demostración. Por (a) del teorema anterior y por las hipótesis, $H^i(D_{T/Z}) = 0$ para $i \neq n$ y $H^n(D_{T/Z}) = \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z)$ es plano sobre T (e isomorfo a $\mathscr{O}_T$ en el caso de que T sea una intersección completa en Z, ver 15.4.2) y para todo $\mathscr{O}_X$-módulo coherente $\mathscr{M}$, $\underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \phi_X^* \mathscr{M}) = \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z) \otimes_{\mathscr{O}_Z} \phi_X^* \mathscr{M}$ (véase la demostración de 13.11.17).

Por otra parte, por el teorema anterior y el teorema de cambio de base plano,

$$\delta_* D_{T/Y} = \underline{\mathrm{Hom}}_Z(\mathscr{O}_T, D_{Z/Y}), \quad D_{Z/Y} \overset{\text{cuasi}}{\longleftarrow} \phi_X^* D_{X/S}$$

Para concluir, basta ver que localmente en Z existe un isomorfismo natural

$$\underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z) \otimes_{\mathscr{O}_T} \phi_T^* H^p(D_{X/S}) \xrightarrow{\sim} H^{p+n}(\underline{\mathrm{Hom}}_{\mathscr{O}_Z}(\mathscr{O}_T, D_{Z/Y}))$$

Sea $P_\cdot \to \mathscr{O}_T$ una resolución por $\mathscr{O}_Z$-módulos localmente libres (existe localmente en Z), y sea $B = \underline{\mathrm{Hom}}^{\cdot}_{\mathscr{O}_Z}(P_\cdot, \phi_X^* D_{X/S})$, que coincide con el complejo simple asociado al bicomplejo $B^{p,q} = \underline{\mathrm{Hom}}(P_p, \phi_X^* D^q_{X/S})$. Se cumple que $H^i(\underline{\mathrm{Hom}}_{\mathscr{O}_Z}(\mathscr{O}_T, D_{Z/Y})) = H^i(B)$, como se deduce de los cuasi-isomorfismos (por cambio de base plano y 15.2.2)

$$\underline{\mathrm{Hom}}_{\mathscr{O}_Z}(\mathscr{O}_T, D_{Z/Y}) \to \underline{\mathrm{Hom}}^{\cdot}_{\mathscr{O}_Z}(P_\cdot, D_{Z/Y}) \leftarrow \underline{\mathrm{Hom}}^{\cdot}_{\mathscr{O}_Z}(P_\cdot, \phi_X^* D_{X/S}) = B.$$

$H^i(B^{\cdot,q}) = 0$ para $i \neq n$ y $H^n(B^{\cdot,q}) = \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z) \otimes_{\mathscr{O}_T} f_T^* D^q_{X/S}$, por lo dicho en el primer párrafo. Luego,

$$H^{q+n}(\underline{\mathrm{Hom}}_{\mathscr{O}_Z}(\mathscr{O}_T, D_{Z/Y})) = H^{q+n}(B) \underset{7.2.17}{=} \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_T, \mathscr{O}_Z) \otimes_{\mathscr{O}_T} \phi_T^* H^q(D_{X/S})$$

□

5. Estructura local del complejo dualizante: *Sea U un abierto de un S-esquema propio X, de modo que U es un subesquema cerrado del espacio afín $\mathbb{A}^r_S$. Entonces,*

$$H^i(D_{X/S})_{|U} \simeq \underline{\mathrm{Ext}}^{i+r}_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S}).$$

En particular, si U es un abierto de dos S-esquemas propios X, X', entonces $D_{X/S|U}$ es cuasi-isomorfo a $D_{X'/S|U}$.

Demostración. Sea $Z = X \underset{S}{\times} \mathbb{A}^r_S$ y $\delta\colon U \to Z$, $\delta(x) = (x,x)$ que es una inmersión cerrada, porque es la composición de las inmersiones cerradas $U \hookrightarrow X \times_S U \hookrightarrow X \times_S \mathbb{A}^r_S$. Consideremos el diagrama

$$\begin{array}{ccccc} U & \xrightarrow{\delta} & Z & \xrightarrow{\pi} & X \\ & & \downarrow & & \downarrow f \\ & & \mathbb{A}^r_S & \longrightarrow & S \end{array}$$

Como $U \hookrightarrow Z$ es una intersección completa, por el Teorema 15.4.4:

$$H^i(D_{X/S})_{|U} \simeq H^{i+r}(D_{U/\mathbb{A}^r_S})$$

$H^i(D_{U/\mathbb{A}^r_S}) \simeq \underline{\mathrm{Ext}}^i_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S})$, por el Teorema 15.4.3 (a), lo cual termina la demostración. □

6. Caracterización de los morfismos de Cohen-Macaulay y Gorenstein: *Sea $f\colon X \to S$ un morfismo propio y plano de fibras de dimensión n.*

1) f es Cohen-Macaulay si y sólo si $D_{X/S}$ tiene un único haz de homología $\omega_{X/S}$ en grado $-n$, que es un $\mathscr{O}_X$-módulo coherente y es plano sobre S.

En este caso, $\omega_{X/S}$ es estable por cambio de la base S: Dado un morfismo $\phi\colon S' \in S$, sea $\phi'\colon X \times_S S' \to S'$ el morfismo inducido, se tiene

$$\phi'^{*}\omega_{X/S|X_s} \simeq \omega_{X\times_S S'/S'}$$

Además, si f es de fibras íntegras, $\omega_{X/S}$ en fibras es de rango 1, sin torsión y Cohen-Macaulay. En particular, si X es íntegro, el dualizante $\omega_{X/S}$ es un módulo sin torsión de rango 1.

2) f es Gorenstein si y sólo si $D_{X/S}$ tiene un único haz de homología $\omega_{X/S}$ en grado $-n$ y es un haz de línea. En este caso, si denotamos $Z = X \times_S X$ y $X \hookrightarrow Z$ el morfismo diagonal, entonces

$$\omega_{X/S} \simeq \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_X, \mathscr{O}_Z)^*$$

En particular, si $X \to S$ es liso, entonces $\omega_{X/S} \simeq \Omega^n_{X/S}$.

Demostración. 1) Por el teorema anterior, es suficiente probar que si U es un subesquema cerrado de $\mathbb{A}^r_S$ de codimensión $d = r - n$ y plano sobre S, entonces U es Cohen-Macaulay sobre S si y sólo si $\underline{\mathrm{Ext}}^i_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S}) = 0$ para $i \neq d$ y $\underline{\mathrm{Ext}}^d_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S})$ es plano sobre S. Esto es bien conocido por 13.11.17. Además, si $\underline{\mathrm{Ext}}^d_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S})$ es plano sobre S, entonces es estable por cambio de base $S' \to S$, es decir,

$$\underline{\mathrm{Ext}}^d_{\mathscr{O}_{\mathbb{A}^r_S}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^r_S}) \otimes_{\mathscr{O}_U} \mathscr{O}_{U\times_S S'} = \underline{\mathrm{Ext}}^d_{\mathscr{O}_{\mathbb{A}^r_{S'}}}(\mathscr{O}_{U\times_S S'}, \mathscr{O}_{\mathbb{A}^r_{S'}})$$

(véase la demostración de 13.11.17), luego $\omega_{X/S}$ también.

Para el resto, podemos suponer que $S = \mathrm{Spec}\, k$, con k un cuerpo. Sea $U = \mathrm{Spec}\, B$ un abierto afín de X, con B una k-álgebra de tipo finito. Consideremos un morfismo finito (luego plano) $\pi\colon U \to \mathbb{A}^n_k$. La gráfica $\delta\colon U \hookrightarrow X \times \mathbb{A}^n_k$ es una intersección completa. Por el Teorema 15.4.4, (con $Z = X \times \mathbb{A}^n_k$)

$$\omega_{U/\mathbb{A}^n_k} = \omega_{X/k|U}$$

Ahora, por el Teorema 15.4.3 (c), $\omega_{U/\mathbb{A}^n_k} = \underline{\mathrm{Hom}}_{\mathscr{O}_{\mathbb{A}^n_k}}(\mathscr{O}_U, \mathscr{O}_{\mathbb{A}^n_k})$. Se concluye porque $\mathscr{O}_U$ es finito y plano sobre $\mathscr{O}_{\mathbb{A}^n_k}$.

2) Consideremos el diagrama (con morfismos obvios)

$$\begin{array}{ccccc} X & \xrightarrow{\delta} & Z & \xrightarrow{\pi_2} & X \\ & & \downarrow{\scriptstyle \pi_1} & & \downarrow \\ & & X & \longrightarrow & S \end{array}$$

Como f es Gorenstein, por el Teorema 15.4.4

$$H^{n+q}(D_{X/X}) \simeq \underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_X, \mathscr{O}_Z) \underset{\mathscr{O}_X}{\otimes} H^q(D_{X/S})$$

y se concluye porque $D_{X/X}$ es una resolución inyectiva de $\mathscr{O}_X$.

Recíprocamente, supongamos que $D_{X/S}$ tiene un único haz de homología $\omega_{X/S}$ en grado $-n$ y que es de línea. Por 15.4.3 (d),

$$H^{p-n}(D_{X/X}) \simeq \underline{\mathrm{Ext}}^p_{\mathscr{O}_Z}(\mathscr{O}_X, \mathscr{O}_Z) \underset{\mathscr{O}_X}{\otimes} \omega_{X/S}$$

luego

$$\underline{\mathrm{Ext}}^p_{\mathscr{O}_Z}(\mathscr{O}_X, \mathscr{O}_Z) = \begin{cases} 0 & p \neq n \\ \omega^*_{X/S} & p = n \end{cases}$$

y esta igualdad se mantiene por paso a fibras sobre S, luego $X \to S$ es un morfismo de Gorenstein. Por último, si $X \to S$ es liso, entonces $X \hookrightarrow Z$ es una inmersión cerrada regular de codimensión n. Por el Teorema 15.4.2, $\underline{\mathrm{Ext}}^n_{\mathscr{O}_Z}(\mathscr{O}_X, \mathscr{O}_Z) \simeq \Omega^n_{X/S}$, ya que el módulo normal de X sobre Z coincide con el módulo de diferenciales de X sobre S.

□

7. Observación : Sea $f : X \to S$ un morfismo propio, de Cohen-Macaulay y de dimensión n. Si para cada $\mathscr{O}_X$-módulo $\mathscr{M}$ sustituimos el complejo $C^{\cdot}\mathscr{M}$ por su truncado en la etapa n-ésima (como hacíamos en la demostración de 15.3.5) construimos otro complejo dualizante $D'_{X/S}$ cuasi-isomorfo a $D_{X/S}$. Ahora bien, $D'_{X/S}$ es nulo en grados menores que $-n$. Corriendo el grado en $-n$, y por el teorema anterior, se obtiene que $D'_{X/S}[-n]$ es una resolución inyectiva del haz dualizante $\omega_{X/S}$. Por tanto,

$$H^i(\mathrm{Hom}_X(\mathscr{M}, D_{X/S})) = \mathrm{Ext}^{i-n}_{\mathscr{O}_X}(\mathscr{M}, \omega_{X/S})$$
$$H^i(\underline{\mathrm{Hom}}_X(\mathscr{M}, D_{X/S})) = \underline{\mathrm{Ext}}^{i-n}_{\mathscr{O}_X}(\mathscr{M}, \omega_{X/S})$$

8. Corolario : *Sea X una variedad propia de dimensión n y Cohen-Macaulay sobre un cuerpo k. Existe un haz quasi-coherente ω_X, llamado haz dualizante, tal que para todo módulo quasi-coherente $\mathscr{M}$ tenemos isomorfismos naturales*

$$\mathrm{Ext}^i_{\mathscr{O}_X}(\mathscr{M}, \omega_X) = H^{n-i}(X, \mathscr{M})^*$$

Si $\mathscr{M}$ es coherente localmente libre, tenemos isomorfismos naturales

$$H^i(X, \mathscr{M}) = H^{n-i}(X, \mathscr{M}^* \otimes \omega_X)^*$$

Por último, X es Gorenstein si y sólo si ω_X es un haz de línea.

Demostración. Por dualidad, $\Gamma(X, C^{\cdot}\mathscr{M})^* = \mathrm{Hom}_X(\mathscr{M}, D_{X/k})$. Tomando homología se concluye por la observación 15.4.7. Si además $\mathscr{M}$ es localmente libre, entonces

$$H^i(X, \mathscr{M}) = \mathrm{Ext}^{n-i}_{\mathscr{O}_X}(\mathscr{M}, \omega_X)^* = \mathrm{Ext}^{n-i}_{\mathscr{O}_X}(\mathscr{O}_X, \mathscr{M}^* \otimes \omega_X)^* = H^{n-i}(X, \mathscr{M}^* \otimes \omega_X)^*$$

y hemos terminado.

□

9. Corolario : *Sea X una variedad propia y lisa de dimensión n. Para cualesquiera $0 \leq p, q \leq n$ se verifica*

$$H^p(X, \Omega^q_{X/k}) = H^{n-p}(X, \Omega^{n-q}_{X/k})^*$$

Demostración. Se deduce del isomorfismo $\Omega^q_{X/k} = (\Omega^{n-q}_{X/k})^* \underset{\mathscr{O}_X}{\otimes} \Omega^n_{X/k}$, y del corolario anterior. □

10. Transitividad del dualizante: *Sea $f: Y \to S$ un morfismo propio de Gorenstein de dimensión n. Para todo morfismo propio $h: X \to Y$, se verifica*

$$H^i(D_{X/Y}) \underset{\mathscr{O}_X}{\otimes} h^* \omega_{Y/S} \simeq H^{i-n}(D_{X/S})$$

Por tanto, $D_{X/Y}$ tiene un único haz de homología (en grado d) si y sólo si $D_{X/S}$ tiene un único haz de homología (en grado $d-n$), y en este caso

$$\omega_{X/Y} \underset{\mathscr{O}_X}{\otimes} h^* \omega_{Y/S} \simeq \omega_{X/S}$$

Demostración. Sea $Z = X \times_S Y$ y $\delta: X \hookrightarrow Z$ la gráfica de h. Del diagrama

$$\begin{array}{ccccc} X & \xrightarrow{\delta} & Z & \longrightarrow & X \\ & & \downarrow & & \downarrow \\ & & Y & \longrightarrow & S \end{array}$$

y del Teorema 15.4.4 obtenemos $H^i(D_{X/Y}) = \omega_{X/Z} \otimes H^{i-n}(D_{X/S})$. Del morfismo de X-esquemas $X \to Z$ y del Teorema 15.4.3 (d), se deduce que $\omega^{-1}_{X/Z} = (\omega_{Z/X} \otimes_{\mathscr{O}_Z} \mathscr{O}_X) = h^* \omega_{Y/S}$, con lo que se concluye. □

11. Teorema: *Sea $X \to S$ propio y Gorenstein, y $j: Y \hookrightarrow X$ una inmersión regular de codimensión d. Entonces,*

$$\omega_{Y/S} \simeq \Lambda^d_{\mathscr{O}_Y} \mathscr{N}_{Y/X} \underset{\mathscr{O}_Y}{\otimes} j^* \omega_{X/S}$$

y si Y es plano sobre S entonces es de Gorenstein.

Demostración. Se sigue del Teorema 15.4.10 y del Teorema 15.4.3 (b). □

12. Fórmula de Residuos: *Sea $f: X \to S$ propio y Gorenstein, y $j: D \hookrightarrow X$ una inmersión regular de codimensión 1. Entonces,*

$$\omega_{D/S} \simeq j^* \omega_{X/S}(D) \simeq \omega_{X/S}(D)/\omega_{X/S}$$

y si D es plano sobre S es de Gorenstein. En particular, si $X \to S$ es liso, entonces

$$\omega_{D/S} \simeq \Omega^n_{X/S}(D)/\Omega^n_{X/S}$$

Esto es, el dualizante del divisor $D \to S$ de $X \to S$ son las n-formas con polo a lo largo del divisor módulo las n-formas regulares.

13. Teorema: *Sea $g: Y \to S$ propio y Cohen-Macaulay de dimensión n, $\pi: X \to Y$ un morfismo finito y $f = g \circ \pi: X \to S$ Cohen-Macaulay. Entonces*

$$\pi_* \omega_{X/S} \simeq \underline{\mathrm{Hom}}_{\mathscr{O}_Y}(\pi_* \mathscr{O}_X, \omega_{Y/S})$$

Si además $Y \to S$ es Gorenstein, entonces

$$\pi_* \omega_{X/S} \simeq \underline{\mathrm{Hom}}_{\mathscr{O}_Y}(\pi_* \mathscr{O}_X, \mathscr{O}_Y) \underset{\mathscr{O}_Y}{\otimes} \omega_{Y/S}$$

Demostración. Por dualidad para morfismos finitos, $\pi_* D_{X/S} = \underline{\mathrm{Hom}}_{\mathscr{O}_Y}(\pi_* \mathscr{O}_X, D_{Y/S})$, (ver 15.4.3). Tomando homología se obtiene

$$\pi_* H^{-n}(D_{X/S}) = H^{-n}(\underline{\mathrm{Hom}}_{\mathscr{O}_Y}(\pi_* \mathscr{O}_X, D_{Y/S})) = \underline{\mathrm{Hom}}_{\mathscr{O}_Y}(\pi_* \mathscr{O}_X, \omega_{X/S})$$

donde la última igualdad se debe a la observación 15.4.7.

□

14. Dualidad para un morfismo birracional: *Sea $f: X \to Y$ un morfismo propio y birracional de S-esquemas íntegros. Si Y es Gorenstein sobre S y X es Cohen-Macaulay sobre S, entonces el complejo dualizante $D_{X/Y}$ tiene un único haz de homología situado en grado 0, y*

$$\omega_{X/Y} \otimes f^* \omega_{Y/S} \simeq \omega_{X/S}$$

Si además $X \to Y$ es finito, entonces $f_* \omega_{X/Y} \simeq \zeta$, donde ζ es el conductor de $X \to Y$ (es decir, el anulador de $f_* \mathscr{O}_X / \mathscr{O}_Y$).

Demostración. La primera parte es el Teorema 15.4.10. La segunda parte se deduce del Teorema 15.4.3 (a), y del isomorfismo $\underline{\mathrm{Hom}}_{\mathscr{O}_Y}(f_* \mathscr{O}_X, \mathscr{O}_Y) \simeq \zeta$. □

15. Dualidad para un morfismo normal de Cohen-Macaulay: *Sea $f: X \to S$ un morfismo propio, de Cohen-Macaulay y geométricamente normal (es decir, de fibras normales) de dimensión n. El dualizante relativo es naturalmente isomorfo al haz de las n-diferenciales de Zariski relativas*

$$\omega_{X/S} = (\Omega^n_{X/S})^{**}$$

Demostración. Sea el abierto $U = \{x \in X : (\Omega_{X/S})_x \simeq \mathscr{O}^n_{X,x}\}$, que es el abierto donde f es liso, y no es vacío porque contiene al punto genérico de cada fibra de S. Por la dualidad para morfismos lisos, $\omega_{X/S|U} \simeq \Omega_{X/S|U}$. Denotemos $i: U \hookrightarrow X$ la inclusión natural. Para terminar, veamos que se tienen isomorfismos

$$\omega_{X/S} \underset{(1)}{\xrightarrow{\sim}} i_*(\omega_{X/S|U}) \simeq i_*(\Omega^n_{X/S|U}) \simeq i_*(\Omega^{n\,**}_{X/S|U}) \underset{(2)}{\xleftarrow{\sim}} (\Omega^n_{X/S})^{**}$$

Los isomorfismos (1) y (2) se deducen de los siguientes lemas:

16. Lema: *Se tiene un isomorfismo*

$$\mathscr{O}_X \xrightarrow{\sim} i_*\mathscr{O}_U$$

Por tanto, para todo $\mathscr{O}_X$-módulo coherente plano $\mathscr{N}$ el morfismo $\mathscr{N} \to i_*(\mathscr{N}_{|U})$ es isomorfismo. Además, para todo $\mathscr{O}_X$-módulo cuasi-coherente $\mathscr{M}$, tomando $\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathscr{M},-)$ en el isomorfismo $\mathscr{O}_X \xrightarrow{\sim} i_*\mathscr{O}_U$, se tiene un isomorfismo $\mathscr{M}^* \xrightarrow{\sim} i_*(\mathscr{M}^*_{|U})$ y por tanto

$$\mathscr{M}^{**} \xrightarrow{\sim} i_*(\mathscr{M}^{**}_{|U})$$

Demostración. En primer lugar veamos que el enunciado es cierto si lo es en fibra. Tenemos que probar la epiyectividad del morfismo $\mathscr{O}_X \to i_*\mathscr{O}_U = \varinjlim_n \underline{\mathrm{Hom}}(\mathfrak{p}^n, \mathscr{O}_X)$ (siendo $\mathfrak{p}$ el ideal que define el cerrado $X-U$). Basta ver que $\mathscr{O}_X \to \underline{\mathrm{Hom}}(\mathfrak{p}^n, \mathscr{O}_X)$ es epiyectivo, que equivale a probar que $\underline{\mathrm{Ext}}^1_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}^n, \mathscr{O}_X)$ es nulo. Puede suponerse que S es el espectro de un anillo local $\mathscr{O}$. Definimos el funtor sobre los $\mathscr{O}$-módulos finito generados $F(N) = \underline{\mathrm{Ext}}^1_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}^n, \pi^*N)$. Es un funtor semiexacto, luego basta ver que $F(\mathscr{O}/\mathfrak{m}) = 0$. Por definición, $F(\mathscr{O}/\mathfrak{m}) = \underline{\mathrm{Ext}}^1_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}^n, \mathscr{O}_{X_s})$, siendo X_s la fibra del punto cerrado de S. A partir de la sucesión exacta $0 \to \mathfrak{p}^n \to \mathscr{O}_X \to \mathscr{O}_X/\mathfrak{p}^n \to 0$, se obtiene que $\underline{\mathrm{Ext}}^1_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{p}^n, \mathscr{O}_{X_s})$ es el conúcleo de $\mathscr{O}_{X_s} \to \underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathfrak{p}^n, \mathscr{O}_{X_s})$. Pero este morfismo es epiyectivo, pues $\mathscr{O}_{X_s} = i_{s*}\mathscr{O}_{U_s}$, donde i_s y U_s son respectivamente i y U en fibra sobre s, y $\{\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\mathfrak{p}^n, \mathscr{O}_{X_s})\}$ es un sistema inductivo de morfismos inyectivos (porque $\mathscr{O}_{X_s}$ es íntegro) de límite inductivo $i_{s*}\mathscr{O}_{U_s}$. En conclusión, $F(\mathscr{O}/\mathfrak{m}) = 0$.

Supongamos por tanto que X es una variedad normal sobre un cuerpo. Si $x \in X$ es un punto de codimensión 1, entonces, por ser X normal, $\mathscr{O}_{X,x}$ es un anillo local de ideales principales. En este punto $(\Omega_{X/k})_x$ es un $\mathscr{O}_{X,x}$-módulo localmente libre, pues completando podemos suponer que $\mathscr{O}_{X,x} = K[[x]]$, por el teorema de Cohen. En conclusión, $X-U$ es un cerrado que es unión de cerrados irreducibles de codimensión mayor que 1 y por 5.3.13 el morfismo $\mathscr{O}_X \to i_*\mathscr{O}_U$ es isomorfismo. □

17. Lema: *El morfismo natural $\omega_{X/S} \to i_*(\omega_{X/S|U})$ es isomorfismo.*

Demostración. Como antes, el problema se reduce a probarlo en fibra, luego podemos suponer $S = \mathrm{Spec}\, k$. Ahora, basta probar el isomorfismo al restringir a un recubrimiento afín. Sea V un abierto afín de X y $\pi\colon V \to \mathbb{A}^n$ una proyección finita y plana. Basta ver que el enunciado se verifica para el módulo $\pi_*(\omega_{X/S|V})$ y el abierto $U' = \pi(U \cap V)$. Ahora bien, como ya vimos en la demostración de 15.4.6, $\omega_{X/S|V} \simeq \omega_{V/\mathbb{A}^n}$, y por tanto $\pi_*(\omega_{X/S|V}) \simeq \underline{\mathrm{Hom}}_{\mathscr{O}_{\mathbb{A}^n}}(\mathscr{O}_V, \mathscr{O}_{\mathbb{A}^n})$, que es plano sobre $\mathbb{A}^n$, luego se concluye por el lema anterior. □

Con estos lemas queda terminada la demostración del teorema. □

15.5. Residuo

Sea X una variedad algebraica propia lisa de dimensión n sobre un cuerpo algebraicamente cerrado. Sea $\Omega_X^n = \Lambda^n \Omega_{X/k}$ el haz dualizante de X. Dado un punto cerrado $x \in X$, consideremos la sucesión exacta $0 \to \mathfrak{m}_x \to \mathscr{O}_X \to \mathscr{O}_X/\mathfrak{m}_x \to 0$ y la sucesión exacta larga de extens asociada al tomar $\mathrm{Hom}_{\mathscr{O}_X}(-, \Omega_X^n)$

$$\mathrm{Ext}^n_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{m}_x, \Omega_X^n) \to \mathrm{Ext}^n_{\mathscr{O}_X}(\mathscr{O}_X, \Omega_X^n) \to \mathrm{Ext}^n_{\mathscr{O}_X}(\mathfrak{m}_x, \Omega_X^n).$$

Por teoría de dualidad $\mathrm{Ext}^n_{\mathscr{O}_X}(\mathfrak{m}_x, \Omega_X^n) = H^0(X, \mathfrak{m}_x)^* = 0$. Además,

$$\mathrm{Ext}^n_{\mathscr{O}_X}(\mathscr{O}_X, \Omega_X^n) = H^0(X, \mathscr{O}_X)^* \simeq k,$$

y por 15.4.2, $\mathrm{Ext}^n_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{m}_x, \Omega_X^n) = \mathrm{Hom}_{\mathscr{O}_X}(\Lambda^n(\mathfrak{m}_x/\mathfrak{m}_x^2), \Omega_X^n/\mathfrak{m}_x\Omega_X^n) \simeq k$. Con todo, tenemos

$$\mathrm{Hom}_{\mathscr{O}_X}(\Lambda^n(\mathfrak{m}_x/\mathfrak{m}_x^2), \Omega_X^n/\mathfrak{m}_x\Omega_X^n) = \mathrm{Ext}^n_{\mathscr{O}_X}(\mathscr{O}_X/\mathfrak{m}_x, \Omega_X^n) = H^n(X, \Omega_X^n) \qquad (*)$$

Así pues, el morfismo $\mathrm{Id} \in \mathrm{Hom}_{\mathscr{O}_X}(\Lambda^n(\mathfrak{m}_x/\mathfrak{m}_x^2), \Omega_X^n/\mathfrak{m}_x\Omega_X^n)$, define un elemento canónico $\xi_X \in H^n(X, \Omega_X^n)$. Veamos que este elemento no depende del x escogido tomando un "punto x general". Consideremos la proyección $\pi_2 \colon X \times X \to X$ y el morfismo diagonal ("punto general") $X \hookrightarrow X \times X$. Consideremos el funtor derivado n-ésimo de $\pi_{2,*}\,\underline{\mathrm{Hom}}_{\mathscr{O}_{X\times X}}(\mathscr{O}_{X\times X}/\Delta, -)$. Tenemos que

$$R^n\pi_{2,*}\,\underline{\mathrm{Hom}}_{\mathscr{O}_{X\times X}}(\mathscr{O}_{X\times X}/\Delta, \Omega_X^n \otimes_k \mathscr{O}_X) = \underline{\mathrm{Hom}}_{\mathscr{O}_X}(\Omega_X^n, \Omega_X^n)$$

Consideremos el funtor derivado n-ésimo de $\pi_{2,*}\,\underline{\mathrm{Hom}}_{\mathscr{O}_{X\times X}}(\mathscr{O}_{X\times X}, -)$. Tenemos que

$$R^n\pi_{2,*}\,\underline{\mathrm{Hom}}_{\mathscr{O}_{X\times X}}(\mathscr{O}_{X\times X}, \Omega_X^n \otimes_k \mathscr{O}_X) = H^n(X, \Omega_X^n) \otimes_k \mathscr{O}_X$$

Luego tenemos un morfismo natural $\underline{\mathrm{Hom}}_{\mathscr{O}_X}(\Omega_X^n, \Omega_X^n) \to H^n(X, \Omega_X^n) \otimes_k \mathscr{O}_X$, que en fibras es el isomorfismo $(*)$ anterior, por tanto, es un isomorfismo. Tomando secciones globales, obtenemos la igualdad

$$\mathrm{Hom}_{\mathscr{O}_X}(\Omega_X^n, \Omega_X^n) = H^n(X, \Omega_X^n)$$

que aplica Id en ξ_X.

1. Definición: Diremos que la aplicación k-lineal $\mathrm{Res} \colon H^n(X, \Omega_X^n) \to k$, que verifica $\mathrm{Res}(\xi_X) = 1$ es el residuo de X.

Tomando duales en la igualdad anterior obtenemos $\mathrm{Hom}_{\mathscr{O}_X}(\Omega_X^n, \Omega_X^n) = H^n(X, \Omega_X^n)^*$ e Id se aplica en Res. Por 15.3.5, el par $(\Omega_X^n, \mathrm{Res})$ representa al funtor $H^n(X, -)^*$.

2. Definición: Dado un punto cerrado $x \in X$, la composición de los morfismos

$$H^n_x(X,\Omega^n_X) \to H^n(X,\Omega^n_X) \overset{\text{Res}}{\to} k,$$

la denotaremos Res_x y diremos que es el residuo local en x.

3. Definición: Sea $Y \subset X$ una subvariedad de codimensión r localmente intersección completa, e I el haz de ideales de funciones de X que se anulan en Y. La imagen de $d\colon \Lambda^r(I/I^2) \to \Omega^r_X/I\Omega^r_X$, $d(\bar{f}_1 \wedge \cdots \wedge \bar{f}_r) = \overline{df_1 \wedge \cdots \wedge df_r}$ en el morfismo

$$\text{Hom}_{\mathcal{O}_X}(\Lambda^r(I/I^2),\Omega^r_X/I\Omega^r_X) = \text{Ext}^r_{\mathcal{O}_X}(\mathcal{O}_X/I,\Omega^r_X) \hookrightarrow H^r_Y(X,\Omega^r_X)$$

se denota $\rho_X(Y)$ y se denomina la clase de cohomología de Y en X.

La imagen de la clase de cohomología $\rho_X(x)$ en $H^n(X,\Omega_X)$ es ξ_X, luego

$$\text{Res}_x(\rho_X(x)) = 1$$

15.6. Cálculo del residuo

Denotemos $\mathcal{O} = \mathcal{O}_{X,x}$ y $\Omega^n = \Omega^n_{\mathcal{O}/k}$, es claro que $H^n_x(X,\Omega^n_X) = H^n_x(\text{Spec}\mathcal{O},\Omega^n)$. Sean $(f_1)_0,\ldots,(f_n)_0$ hipersuperficies de $\text{Spec}\mathcal{O}$, cuya intersección sea x. Sea $U_i = \text{Spec}\mathcal{O} - (f_i)_0$ y $U = \text{Spec}\mathcal{O} - x = \cup_i U_i$. Toda n-forma meromorfa, $w \in H^0(U_1 \cap \ldots \cap U_n,\Omega^n)$, define, por cohomología Cech, una clase de cohomología en $H^{n-1}(U,\Omega^n)$[1]

$$[w] \in H^{n-1}(U,\Omega^n)$$

y por tanto en $H^n_x(\text{Spec}\mathcal{O},\Omega^n)$, vía el connecting $H^{n-1}(U,\Omega^n) \to H^n_x(\text{Spec}\mathcal{O},\Omega^n)$, de la sucesión exacta de la cohomología local.

1. Definición: Definimos $\text{Res}_x(w)$ como $\text{Res}_x([w])$.

Sean ahora $D_1,\ldots,D_n$ divisores efectivos irreducibles de X, cuya intersección $D_1 \cap \cdots \cap D_n$ sea un número finito de puntos. Denotemos $D = D_1 + \ldots + D_n$ y sea θ una n-forma meromorfa con polos eventualmente en los D_i. Para cada punto $x \in D_1 \cap \ldots \cap D_n$, pasando al anillo local podemos definir $\text{Res}_x\,\theta$

2. Teorema: *En las hipótesis anteriores, se verifica*

$$\sum_{x \in X} \text{Res}_x\,\theta = 0$$

[1] Observemos que si w no tiene polos en algún $(f_i)_0$ entonces $w \in H^0(U_1 \cap \ldots \cap \widehat{U_i} \cap \ldots \cap U_n,\Omega^n)$ y su clase en $H^{n-1}(U,,\Omega^n)$ sería nula

Demostración. Sea $U_i = X - D_i$ y $U = \cup_i U_i = X - \cap_i D_i$. La n-forma θ pertenece a $H^0(U_1 \cap \ldots \cap U_n, \Omega^n_X)$, luego define por cohomología Cech un elemento en $H^{n-1}(U, \Omega^n_X)$. Ahora la sucesión exacta de cohomología local

$$H^{n-1}(U, \Omega^n_X) \to \underset{x}{\oplus} H^n_x(X, \Omega^n_X) \to H^n(X, \Omega^n_X) \overset{\text{Res}}{=} k$$

y la compatibilidad del residuo local y el global (por definición) permiten concluir. □

3. Definición: Sea $w \in \Omega^r$, $f_1, \ldots, f_r$ una sucesión regular, $I = (f_1, \ldots, f_r)$ e $Y = (I)_0$. Consideremos la igualdad

$$\text{Hom}_{\mathscr{O}}(\Lambda^r(I/I^2), \Omega^r/I\Omega^r) = \text{Ext}^r_{\mathscr{O}_X}(\mathscr{O}_X/I, \Omega^r_X)$$

Sea $\left[\begin{smallmatrix} w \\ f_1,\ldots,f_r \end{smallmatrix}\right]$ el elemento de $\text{Ext}^r_{\mathscr{O}}(\mathscr{O}/I, \Omega^r)$ que se corresponde con el morfismo

$$\Lambda^r(I/I^2) \to \Omega^r/I\Omega^r,\ \bar{f}_1 \wedge \cdots \wedge \bar{f}_r \mapsto \bar{w}$$

Seguiremos denotando $\left[\begin{smallmatrix} w \\ f_1,\ldots,f_r \end{smallmatrix}\right]$ a la imagen de este elemento en $H^r_Y(X, \Omega^r_X)$, que llamaremos símbolo de Grothendieck.

4. Proposición: *Se verifica que* $\frac{w}{f_1 \cdots f_r} = \left[\begin{smallmatrix} w \\ f_1,\ldots,f_r \end{smallmatrix}\right]$.

Demostración. $K^m_\cdot$ el complejo de Koszul asociado a $\{f_1^m, \ldots, f_r^m\}$. Sea $\bar{K}^m_\cdot$ el complejo definido por $\bar{K}^m_0 = 0$ y $\bar{K}^m_i = K^m_i$ para todo $i \neq 0$, que es una resolución del ideal $I_m = (f_1^m, \ldots, f_r^m)$. Denotemos $U_i = X \backslash (f_i)_0$, $U = \cup_i U_i$ e $Y = X \backslash U$. Conviene identificar cada sumando $\mathscr{O} \cdot \mathbf{f}^{\mathbf{m}}_{\mathbf{i_1}} \wedge \cdots \wedge \mathbf{f}^{\mathbf{m}}_{\mathbf{i_j}}$ con el ideal $(f^m_{i_1} \cdots f^m_{i_j})$, pues a través de esta identificación se tiene que

$$\varinjlim_r \text{Hom}_{\mathscr{O}}(\bar{K}^m_\cdot[1], \Omega^r) = \Gamma(U, \check{C}^\cdot \Omega^r)$$

porque para todo ideal $\mathfrak{p} \subset \mathscr{O}$ y $\mathscr{O}$-módulo M, $\varinjlim_m \text{Hom}_{\mathscr{O}}(\mathfrak{p}^m, M) = \Gamma(V, M)$, con $V = X \backslash (\mathfrak{p})_0$. La proposición se sigue del diagrama conmutativo

$$\begin{array}{ccccc}
\text{Hom}_{\mathscr{O}}(\bar{K}^m_r, \Omega^r) & \longrightarrow & \text{Ext}^{r-1}_{\mathscr{O}}(I_m, \Omega^r) & \xrightarrow{\delta} & \text{Ext}^r_{\mathscr{O}}(\mathscr{O}/I_m, \Omega^r) \\
\downarrow \varinjlim & & \downarrow \varinjlim & & \downarrow \varinjlim \\
H^0(U_1 \cap \cdots \cap U_r, \Omega^r) & \longrightarrow & H^{r-1}(U, \Omega^r) & \xrightarrow{\delta} & H^r_Y(\Omega^r)
\end{array}$$

□

5. Propiedades del símbolo de Grothendieck: *1. Si $Y = (f_1,\dots,f_r)_0 \subset X$, entonces*

$$\rho_X(Y) = \left[\begin{smallmatrix} df_1\wedge\cdots\wedge df_n \\ f_1,\dots,f_r \end{smallmatrix}\right]$$

2. Sea $(f_1,\dots,f_n)\subseteq(g_1,\dots,g_n)$, con lo cual $f_i = \sum a_{ij}g_j$ y supongamos que definen el mismo cerrado. Entonces,

$$\left[\begin{smallmatrix} w \\ g_1,\dots,g_n \end{smallmatrix}\right] = \left[\begin{smallmatrix} \det(a_{ij})w \\ f_1,\dots,f_n \end{smallmatrix}\right]$$

3. Sea $I = (f_1,\dots,f_n)$. Si $w \in I\Omega^n$, entonces

$$\left[\begin{smallmatrix} w \\ f_1,\dots,f_n \end{smallmatrix}\right] = 0$$

Demostración. Son inmediatas. □

6. Cálculo explícito del residuo: *Sea X una variedad propia lisa de dimensión n, $x \in X$ un punto racional y $x_1,\dots,x_n$ un sistema de parámetros en x que generan el ideal maximal de gérmenes de las funciones que se anulan en x.*

1. Se verifica que $\operatorname{Res}_x(\frac{dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}) = \begin{cases} 1 \text{ si } m_1 = \ldots = m_n = 1 \\ 0 \text{ en cualquier otro caso} \end{cases}$

2. Sea $w = g\,dx_1\wedge\cdots\wedge dx_n$ una forma regular en x y $f_1,\dots,f_n$ una sucesión regular en x. Para cada i existe un m_i tal que $x_i^{m_i} \in (f_1,\dots,f_n)$, luego $x_i^{m_i} = \sum a_{ij}f_j$. Entonces, $\operatorname{Res}_x(\frac{w}{f_1\cdots f_n})$ *es el coeficiente en $x_1^{m_1-1}\cdots x_n^{m_n-1}$ del desarrollo de potencias de $g\cdot\det(a_{ij})$.*

Demostración. $\frac{dx_1\wedge\cdots\wedge dx_n}{x_1\cdots x_n}$ coincide con la clase de cohomología de x luego

$$\operatorname{Res}_x(\frac{dx_1\wedge\cdots\wedge dx_n}{x_1\cdots x_n}) = 1$$

Si algún $m_i \le 0$ entonces $\operatorname{Res}_x(\frac{dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}) = 0$ por 15.6.5 3.

Vamos a deformar $\frac{dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}$, cuando algún $m_i \neq 1$, a n-formas proporcionales, conservando el residuo a lo largo de la deformación. Consideremos la deformación de X al cono normal (véase la subsección 17.3.2). Sean pues $\tilde{Z}$ la explosión de $X\times\mathbb{P}^1$ en el punto $(x,\infty)\in X\times\mathbb{P}^1$, $\pi\colon\tilde{Z}\to\mathbb{P}^1$ la proyección (plana) natural, $\tilde{X}$ la explosión de

X en x y la sección $s\colon \mathbb{P}^1 \hookrightarrow \tilde{Z}$, $s(\lambda) = (x, \lambda)$ (denotemos $s(\infty) = 0_\infty$). Observemos que $s(\mathbb{P}^1) \cap (\tilde{X} \times \infty) = \emptyset$. Sea $\mathbb{A}^1 = \mathbb{P}^1 - \infty = \operatorname{Spec} k[t]$, observemos que $\pi^{-1}(\mathbb{A}^1) = X \times \mathbb{A}^1$.

Por 15.4.10, $\omega_{\tilde{Z}/\mathbb{P}^1} = \omega_{\tilde{Z}} \otimes (\pi^* \omega_{\mathbb{P}^1})^*$. El morfismo π es liso fuera de $\tilde{X} \times \infty$, luego en este abierto $\omega_{\tilde{Z}/\mathbb{P}^1} = \Omega^n_{\tilde{Z}/\mathbb{P}^1}$.

Sea Δ_s el haz de ideales de funciones de $\tilde{Z}$ que se anulan en $s(\mathbb{P}^1)$ y sea $X_t = \pi^{-1}(t)$. Como este cerrado no corta con $\tilde{X} \times \infty$, tenemos el isomorfismo $d\colon \Lambda^n(\Delta_s/\Delta_s^2) = \omega_{\tilde{Z}/\mathbb{P}^1}/\Delta_s \omega_{\tilde{Z}/\mathbb{P}^1}$, en fibras sobre cada $t \in \mathbb{A}^1$ coincide con $d_{x_t}\colon \Lambda^n(\mathfrak{m}_{x_t}/\mathfrak{m}_{x_t}^2) = \Omega^n_{X_t}/\mathfrak{m}_{x_t}\Omega^n_{X_t}$. $R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}/\Delta_s, \omega_{\tilde{Z}/\mathbb{P}^1})$ y $R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}, \omega_{\tilde{Z}/\mathbb{P}^1})$ en fibras sobre cada $t \in \mathbb{A}^1$ coinciden con $\underline{\operatorname{Ext}}_{\mathscr{O}_{X_t}}(\mathscr{O}_{X_t}/\mathfrak{m}_{x_t}, \omega_{X_t})$ y $\underline{\operatorname{Ext}}^n_{\mathscr{O}_{X_t}}(\mathscr{O}_{X_t}, \Omega^n_{X_t})$. Sea $\rho_{\tilde{Z}}(s(\mathbb{P}^1))$ la imagen de d en las secciones globales de $R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}, \omega_{\tilde{Z}/\mathbb{P}^1})$. En fibras sobre cada $t \in \mathbb{A}^1$ coincide con $\rho_{X_t}(x_t)$. Sea $\operatorname{Res}_{s(\mathbb{P}^1)}$ la sección global de $(R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}, \omega_{\tilde{Z}/\mathbb{P}^1}))^*$ que por dualidad coincide con $\mathrm{Id} \in \operatorname{Hom}_{\mathscr{O}_{\tilde{Z}}}(\omega_{\tilde{Z}/\mathbb{P}^1}, \omega_{\tilde{Z}/\mathbb{P}^1})$. La restricción de $\operatorname{Res}_{s(\mathbb{P}^1)}$ a $\mathbb{A}^1$ coincide con $\operatorname{Res}_{s(\mathbb{A}^1)}$, que por dualidad coincide con $\mathrm{Id} \in \operatorname{Hom}_{\mathscr{O}_{X\times\mathbb{A}^1}}(\omega_{X\times/\mathbb{A}^1}, \omega_{X\times/\mathbb{A}^1})$. Por tanto $\operatorname{Res}_{s(\mathbb{P}^1)}$ en fibras sobre cada $t \in \mathbb{A}^1$, coinciden con Res_{x_t}.

Denotemos por $\Delta_s^{(m)}$ el ideal de ceros $s(\mathbb{P}^1)$, que localmente en x_t es $(x_1^{m_1}, \ldots, x_n^{m_n})$ si $t \neq \infty$ y en 0_∞ es $((tx_1)^{m_1}, \ldots, (tx_n)^{m_n})$. $R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}/\Delta_s^{(m)}, \omega_{\tilde{Z}/\mathbb{P}^1})$ en fibras sobre $t \in \mathbb{A}^1$ coincide con $\underline{\operatorname{Ext}}^n_{\mathscr{O}_{X_t}}(\mathscr{O}_{X_t}/\mathfrak{m}_{x_t}^{(m)}, \Omega^n_{X_t})$. Como $w = \frac{d(tx_1)\wedge\cdots\wedge d(tx_n)}{(tx_1)^{m_1}\cdots(tx_n)^{m_n}}$ es una sección global de $R^n\pi_* \underline{\operatorname{Hom}}_{\mathscr{O}_{\tilde{Z}}}(\mathscr{O}_{\tilde{Z}}/\Delta_s^{(m)}, \omega_{\tilde{Z}/\mathbb{P}^1})$ y $\operatorname{Res}_{s(\mathbb{P}^1)}(w) \in \mathscr{O}_{\mathbb{P}^1}(\mathbb{P}^1) = k$, tenemos que

$$\operatorname{Res}_{s(\mathbb{P}^1)}(w) = Res_{x_t}\left(\frac{d(tx_1)\wedge\cdots\wedge d(tx_n)}{(tx_1)^{m_1}\cdots(tx_n)^{m_n}}\right) = t^{n-\sum_i m_i} \operatorname{Res}_x\left(\frac{dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}\right)$$

Luego, $\operatorname{Res}_x\left(\frac{dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}\right) = 0$ si algún $m_i > 1$.

Por último,

$$\begin{aligned}\operatorname{Res}_x\left(\frac{w}{f_1\cdots f_n}\right) &= \operatorname{Res}_x\left(\frac{\det(a_{ij})w}{x_1^{m_1}\cdots x_n^{m_n}}\right) = \operatorname{Res}_x\left(\frac{a\cdot dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}\right) + \operatorname{Res}_x\left(\frac{a'\cdot dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}\right)\\ &= \operatorname{Res}_x\left(\frac{a\cdot dx_1\wedge\cdots\wedge dx_n}{x_1^{m_1}\cdots x_n^{m_n}}\right)\end{aligned}$$

donde a es el desarrollo de Taylor de $\det(a_{ij})g$ hasta el orden $m_1 + \ldots + m_n$ y $a' = \det(a_{ij})g - a$, y la última igualdad se debe a 15.6.5 3. Por el resultado obtenido en el párrafo anterior concluimos. □

Capítulo 16

Sucesión Espectral

16.1. Introducción

Sea M un objeto de una categoría abeliana y una filtración

$$M \supset \cdots \supset M_p \supset M_{p+1} \supset \cdots \supset 0, \quad (p \in \mathbb{Z})$$

Sea d una diferencial en M compatible con la filtración, es decir, $dM_p \subseteq M_p$. El graduado $GM = \oplus_p M_p/M_{p+1}$ tiene una diferencial inducida por d. El problema que va a tratarse es computar la homología de M, $H(M)$, en términos de la homología del graduado, $H(GM)$.

La técnica de la sucesión espectral proporciona un método de aproximar, si no $H(M)$, sí su graduado por las imágenes $\operatorname{Im} i_p^\infty$ de las flechas

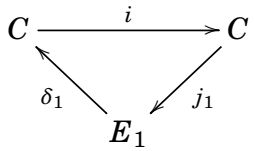
$$i_p^\infty : H(M_p) \to H(M)$$

inducidas por las inmersiones $M_p \hookrightarrow M$.

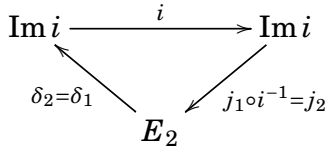
Así pues, el problema de la sucesión espectral es aproximar el graduado de la homología, $GH(M)$, por la homología del graduado, $H(GM)$, en el sentido que se explicará en lo que sigue.

16.2. Triángulos exactos

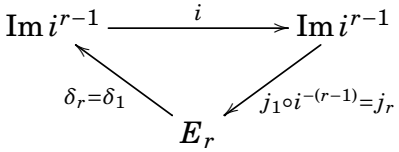
Sea un triángulo exacto de una categoría abeliana



Sea la diferencial $d_1 = j_1 \circ \delta_1$ en E_1. Entonces, $H_{d_1}(E_1) = [\delta_1^{-1}(\operatorname{Im} i)]/[j_1(\operatorname{Ker} i)]$ y lo denotaremos E_2. Los morfismos $\delta_2 \colon E_2 \to \operatorname{Im} i$, $\delta_2(\bar{a}) = \overline{\delta_1(a)}$ y $j_2 \colon \operatorname{Im} i \to E_2$, $j_2(i(a)) = \overline{j_1(a)}$ están bien definidos y verifican el triángulo exacto



Recurrentemente tendremos los triángulos exactos



con $E_r = H_{d_{r-1}}(E^{r-1})$.

Los objetos E_r pueden manejarse fácilmente en términos del triángulo inicial, como muestra el siguiente teorema:

1. Teorema: *Se verifica que* $E_r = \delta_1^{-1}(\operatorname{Im} i^{r-1})/j_1(\operatorname{Ker} i^{r-1})$

Demostración. Por hipótesis de inducción $E_{r-1} = \delta_1^{-1}(\operatorname{Im} i^{r-2})/j_1(\operatorname{Ker} i^{r-2})$. Ahora ya

$$\begin{aligned} E_r &= H_{d_{r-1}}(E_{r-1}) = \delta_{r-1}^{-1}(\operatorname{Im} i^{r-1})/(j_1 \circ i^{-(r-2)})(\operatorname{Ker} i_{|\operatorname{Im} i^{r-2}}) \\ &= [\delta_1^{-1}(\operatorname{Im} i^{r-1})/j_1(\operatorname{Ker} i^{r-2})]/[j_1(\operatorname{Ker} i^{r-1})/j_1(\operatorname{Ker} i^{r-2})] = \delta_1^{-1}(\operatorname{Im} i^{r-1})/j_1(\operatorname{Ker} i^{r-1}) \end{aligned}$$

□

16.3. Sucesión espectral de un objeto diferencial filtrado

Sea M un objeto de una categoría abeliana y $M \supset \cdots \supset M_p \supset M_{p+1} \supset \cdots \supset 0$ una filtración ($p \in \mathbb{Z}$). Suponemos que $M_{-\infty} := \underset{p\in\mathbb{Z}}{\cup} M_p = M$. Sea d una diferencial en M compatible con la filtración, es decir, $d(M_p) \subseteq M_p$. Se dice que M es un objeto diferencial y filtrado. Denotemos

$$SM = \underset{p}{\oplus} M_p, \qquad GM = \underset{p}{\oplus} M_p/M_{p+1}$$

Las sucesiones exactas

$$0 \to M_{p+1} \to M_p \to M_p/M_{p+1} \to 0$$

definen la sucesión exacta de módulos diferenciales ($\mathbb{Z}$-graduados)

$$0 \to SM \to SM \to GM \to 0.$$

y por tanto el triángulo exacto de objetos ($\mathbb{Z}$-graduados)

$$\begin{array}{ccc} H(SM) = \oplus H(M_p) & \xrightarrow{\quad i \quad} & H(SM) = \oplus H(M_p) \\ & {\scriptstyle \delta_1} \nwarrow \quad \swarrow {\scriptstyle j_1} & \\ & E_1 = H(GM) = \oplus H(M_p/M_{p+1}) & \end{array}$$

donde i disminuye el grado en 1, j_1 mantiene el grado, δ_1 lo aumenta en 1 y $d_1 = j_1 \circ \delta_1$ lo aumenta en 1.

De aquí se deduce la sucesión de triángulos exactos (de objetos graduados)

$$\begin{array}{ccc} \operatorname{Im} i^{r-1} & \xrightarrow{\quad i \quad} & \operatorname{Im} i^{r-1} \\ & {\scriptstyle \delta_r = \delta_1} \nwarrow \quad \swarrow {\scriptstyle j \circ i^{-(r-1)} = j_r} & \\ & E_r & \end{array}$$

donde i disminuye el grado en 1, j_r aumenta el grado en $r-1$, δ_r lo aumenta en 1 y d_r aumenta en r. La graduación es explícitamente: $(\operatorname{Im} i^{r-1})_p = \operatorname{Im} i^{r-1}_{p+r-1}$, donde

$$i^{r-1}_{p+r-1} : H(M_{p+r-1}) \to H(M_p)$$

es el morfismo inducido por $M_{p+r-1} \hookrightarrow M_p$, $m \mapsto i^{r-1}(m)$; y $E_r = \underset{p}{\oplus} E_r^p$, donde definimos $E_r^p = (\delta_1^{-1} \operatorname{Im} i^{r-1})_p / j_1(\operatorname{Ker} i_p^{r-1})$.

El triángulo exacto da lugar a la sucesión exacta larga

$$\cdots \to E_r^p \xrightarrow{\delta_r} \operatorname{Im} i^{r-1}_{p+r} \xrightarrow{i} \operatorname{Im} i^{r-1}_{p+r-1} \xrightarrow{j_r} E_r^{p+r-1} \to \cdots \qquad (**)$$

1. Definición: Se llama sucesión espectral asociada al objeto diferencial filtrado M a la sucesión de objetos diferenciales

$$(E_1, d_1), (E_2, d_2), \ldots, (E_r, d_r), \ldots$$

donde $E_r = H_{d_{r-1}}(E_{r-1})$.

La homología $H(M)$ está filtrada por las imágenes $\operatorname{Im} i_p^\infty$ de las flechas

$$i_p^\infty : H(M_p) \to H(M)$$

inducidas por las inclusiones $M_p \hookrightarrow M$. Denotaremos $E_\infty = G(H(M))$ y E_∞^p a la componente de grado p de $GH(M)$.

2. Teorema de aproximación: *Sea p fijo. Si existe un índice k tal que δ_k es nula sobre E_k^p, entonces existen morfismos $E_r^p \to E_{r+1}^p$ $(r \geq k)$ y se verifica que $\varprojlim_{r\to\infty} E_r^p = E_\infty^p$.*

Demostración. Si δ_k es nula sobre E_k^p entonces, como $\delta_{k+1}(\bar{m}) = \delta_k(m) = 0$, $\delta_{k+1} = 0$ en E_{k+1}^p. Luego, $\delta_r = 0$ en E_r^p, para $r \geq k$. Si δ_r es nula sobre E_r^p entonces d_r también. Por tanto, como $H_{d_r}(E_r^p) = E_{r+1}^p$, existe un epimorfismo $E_r^p \to E_{r+1}^p$. De la sucesión exacta

$$\operatorname{Im} i_{p+1}^{r-1} \longrightarrow \operatorname{Im} i_p^{r-1} \longrightarrow E_r^p \to \delta_r(E_r^p) = 0 \qquad\qquad (r \geq k)$$

se deduce, tomando límites inductivos

$$0 \to \operatorname{Im} i_{p+1}^\infty \longrightarrow \operatorname{Im} i_p^\infty \longrightarrow \varprojlim_{r\to\infty} E_r^p \to 0$$

pues $\varprojlim_{r\to\infty} \operatorname{Im} i_p^r = \operatorname{Im} i_p^\infty$, con lo que se concluye.

□

3. Definición: Se dice que la sucesión espectral E_r es convergente si para cada p existe un índice $k(p)$ tal que $\delta_{k(p)}$ es nula sobre $E_{k(p)}^p$.

En este caso, existen morfismos $E_r^p \to E_{r+1}^p$ $(r \geq k(p))$ y se tiene la "aproximación"

$$GH(M) = E_\infty = \varprojlim_{r\to\infty} E_r$$

Si M y M' son dos objetos diferenciales filtrados y $\Phi : M \to M'$ es un morfismo diferencial compatible con las filtraciones, entonces induce un morfismo $\Phi_r : E_r(M) \to E_r(M')$, de modo que la asignación $M \rightsquigarrow E_r(M)$ es un functor covariante sobre la categoría de objetos diferenciales filtrados. Se sigue:

4. Corolario: *Si Φ_r es isomorfismo, entonces Φ_{r+k} es isomorfismo para todo $k \geq 0$ y si las sucesiones espectrales convergen,*

$$\Phi_\infty : GH(M) \to GH(M')$$

es un isomorfismo.

5. Corolario: *Si $H(M_i) = 0$ para $i \geq k$, entonces la sucesión espectral E_r^p es convergente y $E_\infty^p = \varprojlim_{r\to\infty} E_r^p$.*

Demostración. Para $r \geq k-p$, la composición $i^{r-1}_{p+r}: H(M_{p+r}) \to H(M_k) \to H(M_{p+1})$ es nula, luego δ_r es nulo sobre E^p_r y concluimos por el teorema anterior. □

6. Definición: Se dice que la filtración $\{M_p\}$ es regular, si existe un índice k de modo que $H(M_p) = 0$, para $p \geq k$.

7. Teorema: *Sea $\Phi: M \to M'$ un morfismo diferencial compatible con las filtraciones. Si las filtraciones de M y M' son regulares y $\Phi_r: E_r \to E'_r$ es isomorfismo para algún r, entonces Φ es un cuasi-isomorfismo.*

Demostración. Como las filtraciones son regulares las sucesiones espectrales convergen y $\Phi_\infty: GH(M) \to GH(M')$ es un isomorfismo. Se tienen así isomorfismos

$$\operatorname{Im} i^\infty_p / \operatorname{Im} i^\infty_{p+1} \simeq \operatorname{Im} i'^\infty_p / \operatorname{Im} i'^\infty_{p+1}$$

y recurrentemente se obtienen isomorfismos $\operatorname{Im} i^\infty_p / \operatorname{Im} i^\infty_{p+r} \simeq \operatorname{Im} i'^\infty_p / \operatorname{Im} i'^\infty_{p+r}$. Por ser las filtraciones regulares, $\operatorname{Im} i_{p+r} = 0 = \operatorname{Im} i'_{p+r}$ para $r >> 0$, luego $\operatorname{Im} i^\infty_p \simeq \operatorname{Im} i'^\infty_p$. Tomando límite inductivo cuando $p \to -\infty$, y teniendo en cuenta que la homología conmuta con límites inductivos, obtenemos $H(M) \simeq H(M')$. □

8. Definición: Se dice que la sucesión espectral asociada a una filtración regular es degenerada, si existe $r > 0$ de modo que $E^i_r = 0$, para todo i distinto de un cierto p.

9. Teorema: *Si la sucesión espectral es degenerada, se tienen isomorfismos canónicos*

$$H(M) \simeq E^p_\infty \simeq E^p_r.$$

Demostración. Es sencillo ver que $E^q_r = E^q_{r+i}$ para $i > 0$ y todo q, luego $\lim_{r\to\infty} E^q_r \simeq E^q_r$. De la igualdad $\lim_{r\to\infty} E^q_r = E^q_\infty$, se deduce $E^q_\infty = 0$ para $q \neq p$. Por tanto,

$$\operatorname{Im} i^\infty_p = \operatorname{Im} i^\infty_{p-r}, \text{ para } r \geq 0$$
$$\operatorname{Im} i^\infty_{p+1} = \operatorname{Im} i^\infty_{p+r}, \text{ para } r > 0$$

Entonces, por ser la filtración regular, $\operatorname{Im} i^\infty_{p+1} = \operatorname{Im} i^\infty_{p+r} = 0$ para $r >> 0$, luego $E^p_\infty = \operatorname{Im} i^\infty_p = \lim_{r\to\infty} \operatorname{Im} i^\infty_{p-r} = H(M)$. □

16.4. Caso bigraduado

Supongamos ahora que M está graduado, $M = \bigoplus_{n\in\mathbb{N}} N^n$, de modo compatible con la diferencial y la filtración, es decir, $d(N^n) \subset N^{n+1}$ y $M_p = \bigoplus_n (M_p \cap N^n)$. Denotaremos $M_{p,n-p} := M_p \cap N^n$.

- $\operatorname{Im} i^r = \bigoplus_{p,n} (\operatorname{Im} i^r)_{p,n-p}$, con $(\operatorname{Im} i^r)_{p,n-p} := \operatorname{Im} i^r_{p+r,n-(p+r)}$, donde

$$i^r_{p+r,n-(p+r)} \colon H^n(M_{p+r}) \to H^n(M_p)$$

es el morfismo inducido por $M_{p+r} \hookrightarrow M_p$.

- E_1 está bigraduado por $E_1^{p,n-p} = H^n(M_p/M_{p+1})$, δ_1 aumenta el exponente cohomológico en 1, i en 0 y j_1 en 0. Los E_r se pueden bigraduar como en el caso anterior por:

$$E_r^{p,n-p} = (\delta_1^{-1} \operatorname{Im} i^{r-1})_{p,n-p})/j_1(\operatorname{Ker} i^{r-1}_{p,n-p})$$

y se tiene la sucesión exacta

$$\cdots \to E_r^{p,n-p} \xrightarrow{\delta_r} \operatorname{Im} i^{r-1}_{p+r,n+1-(p+r)} \xrightarrow{i} \operatorname{Im} i^{r-1}_{p+r-1,n+1-(p+r-1)} \xrightarrow{j_r} E_r^{p+r-1,n+1-(p+r-1)} \to \cdots$$

y la diferencial d_r es de grado $(r, 1-r)$, $d_r \colon E_r^{p,n-p} \to E_r^{p+r,n+1-(p+r)}$.

Igualmente denotamos $i^\infty_{p,n-p} \colon H^n(M_p) \to H^n(M)$ el morfismo obvio y definimos $E_\infty^{p,n-p} = \operatorname{Im} i^\infty_{p,n-p} / \operatorname{Im} i^\infty_{p+1,n-(p+1)}$.

Con las mismas demostraciones obtendremos:

1. Teorema de aproximación: *Sean n y p fijos. Si δ_k es nulo sobre $E_k^{p,n-p}$ para un cierto índice k, existen morfismos $E_r^{p,n-p} \to E_{r+1}^{p,n-p}$ $(r \geq k)$ y se verifica $E_\infty^{p,n-p} = \lim_{r\to\infty} E_r^{p,n-p}$.*

2. Definición: Se dice que la sucesión espectral $E_r^{p,n-p}$ es convergente, si para cada p y n existe un índice $k(p,n)$ tal que $\delta_{k(p,n)}$ es nula sobre $E^{p,n-p}_{k(p,n)}$.

En este caso existen morfismos $E_r^{p,n-p} \to E_{r+1}^{p,n-p}$ $(r \geq k(p,n))$ y se tiene la "aproximación"

$$GH(M) = \lim_{r\to\infty} E_r$$

3. Corolario: *Si $H^{n+1}(M_i) = 0$ para $i \geq k(n)$, entonces la sucesión espectral $E_r^{p,n-p}$ es convergente y $E_\infty^{p,n-p} = \lim_{r\to\infty} E_r^{p,n-p}$.*

4. Definición: Se dice que la filtración $\{M_p\}$ es regular, si para cada n existe un índice $k(n)$ de modo que $H^n(M_p) = 0$, para $p > k(n)$.

5. Teorema: *Sea $\Phi \colon M \to M'$ un morfismo de objetos diferenciales filtrados y graduados. Si las filtraciones de M y M' son regulares y $\Phi_r \colon E_r \to E'_r$ es isomorfismo para algún r, entonces Φ es un cuasi-isomorfismo.*

6. Definición: Se dice que la sucesión espectral $E_r^{p,n-p}$ asociada a una filtración regular $\{M_p\}$ es degenerada, si existe un entero r tal que, para cada n, $E_r^{p,n-p} = 0$, para todo $p \neq p(n)$.

7. Teorema: *Si la sucesión espectral es degenerada, existen isomorfismos canónicos $H^n(M) \simeq E_\infty^{p(n),n-p(n)}$. Si $p(n) = p$ es independiente de n, entonces $H^n(M) = E_r^{p,n-p}$.*

16.5. Sucesión espectral asociada a un bicomplejo

Sea $M = \underset{p,q}{\oplus} M^{p,q}$ un objeto bigraduado con dos diferenciales d_1 y d_2, tales que

$$d_1 : M^{p,q} \to M^{p+1,q}$$
$$d_2 : M^{p,q} \to M^{p,q+1}$$
$$d_1 d_2 = d_2 d_1$$

Si se escribe $N^n = \underset{p+q=n}{\oplus} M^{p,q}$ y $d = d_1 + (-1)^n d_2$, entonces $M = \oplus_n N^n$ y $d : N^n \to N^{n+1}$ es una diferencial. Se definen dos filtraciones sobre M por

$$M_m := \underset{p \geq m}{\oplus} M^{p,\cdot}, \qquad \overline{M}_m := \underset{q \geq m}{\oplus} M^{\cdot,q}$$

siendo $M^{p,\cdot} = \underset{q}{\oplus} M^{p,q}$ y análogamente $M^{\cdot,q}$. Ambas filtraciones son compatibles con d.

1. Teorema: *Los segundos términos de las sucesiones espectrales asociadas a las dos filtraciones anteriores son*

$$E_2^{p,q} = H_{d_1}^p(H_{d_2}^q(M)), \qquad \overline{E}_2^{p,q} = H_{d_2}^q(H_{d_1}^p(M)).$$

Demostración. $E_1^p = H_d(M_p/M_{p+1}) = H_{d_2}(M^{p,\cdot})$, luego $E_1 = H_{d_2}(M)$. Además, es fácil ver que la diferencial de E_1 es la inducida por d_1 y concluimos. □

2. Teorema: *Se tiene:*

a) Si M está acotado inferiormente ($M^{p,q} = 0$ para q menor que cierto s) o acotado por la derecha ($M^{p,q} = 0$ para p mayor que cierto r), la filtración M_m es regular.

b) Si M está acotado superiormente ($M^{p,q} = 0$ para q mayor que cierto s) o acotado por la izquierda ($M^{p,q} = 0$ para p menor que cierto r), la filtración $\overline{M}_m$ es regular.

Demostración. a) Si $M^{p,q} = 0$ para $q < s$, entonces $N^n \cap M_m = 0$ para $m > n - s$. Análogamente, si $M^{p,q} = 0$ para $p > r$, entonces $N^n \cap M_m = 0$ para $m > r$.

b) Se procede de modo equivalente. □

Volvamos a probar el teorema 7.2.17 con las técnicas de la sucesión espectral.

3. Teorema: *Sea M un bicomplejo tal que $M^{p,q} = 0$ si $p < r$ y d_1 exacta (para $p > r$). Sea $P^{s+r} = \operatorname{Ker} d_1 : M^{r,s} \to M^{r+1,s}$, que es un complejo con la diferencial d_2. La inyección natural $P \to M$ es un cuasi-isomorfismo.*

Demostración. $\overline{E}_2(M) = H_{d_2}(H_{d_1}(M)) = H_{d_2}(P) = \overline{E}_2(P)$, luego se concluye por 16.5.2 b) y 16.4.5.

□

16.5.1. Sucesión espectral de hiperfuntores derivados

Estamos en una categoría abeliana con suficientes inyectivos.

4. Lema: *Sea* $0 \to M' \to M \to M'' \to 0$ *una sucesión exacta y* $M' \to I^{\cdot}$, $M'' \to J^{\cdot}$ *resoluciones inyectivas. Entonces puede construirse un diagrama conmutativo de complejos y morfismos de complejos*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow & & \\ 0 & \longrightarrow & I^{\cdot} & \xrightarrow{i} & I^{\cdot} \oplus J^{\cdot} & \xrightarrow{p} & J^{\cdot} & \longrightarrow & 0 \end{array}$$

donde i y p son los morfismos naturales y f es cuasi-isomorfismo. (La diferencial del complejo $I^{\cdot} \oplus J^{\cdot}$ *no es la usual, se construirá en la demostración).*

Demostración. El morfismo $M \hookrightarrow I^0 \oplus J^0$ se construye del modo siguiente: El morfismo $M' \hookrightarrow I^0$ levanta a un morfismo $M \to I^0$ y el morfismo $M'' \hookrightarrow J^0$ define por composición un morfismo $M \to J^0$. En consecuencia tenemos un morfismo $M \hookrightarrow I^0 \oplus J^0$.

Ahora se procede análogamente con la sucesión exacta $0 \to I^0/M' \to (I^0 \oplus J^0)/M \to J^0/M'' \to 0$. Así sucesivamente se construye la diferencial en $I^{\cdot} \oplus J^{\cdot}$ y el diagrama deseado. □

5. Definición: Una resolución de Cartan-Eilenberg de un complejo $M^{\cdot}$ es el complejo simple asociado a un bicomplejo diferencial $R^{\cdot\cdot} = \bigoplus_{p,q \geq 0} R^{p,q}$ de objetos inyectivos, de diferenciales $d_1 : R^{p,q} \to R^{p+1,q}$ y $d_2 : R^{p,q} \to R^{p,q+1}$, tal que para cada p, se verifica

- $R^{p,\cdot}$ es resolución inyectiva de M^p.
- $Z^p_{d_1}(R^{\cdot\cdot})$ $(= \operatorname{Ker} d_1 : R^{p,\cdot} \to R^{p+1,\cdot})$ es resolución inyectiva de $Z^p(M^{\cdot})$.
- $B^p_{d_1}(R^{\cdot\cdot})$ $(= \operatorname{Im} d_1 : R^{p-1,\cdot} \to R^{p,\cdot})$ es resolución inyectiva de $B^p(M^{\cdot})$.
- $H^p_{d_1}(R^{\cdot\cdot})$ es resolución inyectiva de $H^p(M^{\cdot})$.

En particular, una resolución de Cartan-Eilenberg es una resolución inyectiva de $M^{\cdot}$.

6. Teorema: *Si* $M^{\cdot}$ *está acotado inferiormente, admite una resolución de Cartan-Eilenberg, que denotaremos* $I^{\cdot}(M^{\cdot})$.

Demostración. Sea $M^{\cdot} = M^s \to M^{s+1} \to \cdots$ y sean I_s, J_{s+1} resoluciones inyectivas de los ciclos $Z^s(M^{\cdot})$ y bordes $B^{s+1}(M^{\cdot})$ respectivamente. Aplicando el lema anterior a la sucesión exacta

$$0 \to Z^s(M^{\cdot}) \to M^s \to B^{s+1}(M^{\cdot}) \to 0$$

se sigue que $R_s = I_s \oplus J_{s+1}$ es una resolución inyectiva de M^s.

Sea ahora K_{s+1} una resolución inyectiva de $H^{s+1}(M^\cdot)$. De la sucesión exacta

$$0 \to B^{s+1}(M^\cdot) \to Z^{s+1}(M^\cdot) \to H^{s+1}(M^\cdot) \to 0$$

y del lema anterior se sigue que $I_{s+1} = J_{s+1} \oplus K_{s+1}$ es una resolución inyectiva de $Z^{s+1}(M^\cdot)$. Por reiteración se acaba. □

Sea $M^\cdot$ un complejo inferiormente acotado y F un funtor covariante aditivo. Sea $M^\cdot \to I^{\cdot\cdot}$ una resolución de Cartan-Eilenberg de $M^\cdot$. Por la teoría del bicomplejo, el bicomplejo $F(I^{\cdot\cdot})$ tiene una filtración regular (por el teorema 16.5.2) a la que está asociada una sucesión espectral convergente al graduado de $\mathbb{R}^\cdot F(M^\cdot)$ por una filtración conveniente cuyo término $\bar{E}_2^{p,q}$ vale:

$$\bar{E}_2^{p,q} = H^q_{d_2}(H^p_{d_1}(F(I^{\cdot\cdot}))) = H^q_{d_2}(F(H^p_{d_1}(I^{\cdot\cdot}))) = R^q F(H^p(M^\cdot))$$

donde la segunda igualdad se debe a que, por ser F aditivo, transforma sucesiones exactas de inyectivos en sucesiones exactas, y la tercera por ser $H^p_{d_1}(I^{\cdot\cdot})$ resolución inyectiva de $H^p(M^\cdot)$. Esta sucesión espectral se conoce como sucesión espectral de hiperfuntores derivados.

Sea G otro functor aditivo y supongamos que F transforma inyectivos en G-acíclicos. Aplicando la sucesión espectral de los funtores derivados a G y $\mathbb{R}F(M^\cdot)$ se obtiene una sucesión espectral cuyo término $\bar{E}_2^{p,q}$ vale $R^qG(\mathbb{R}^pF(M^\cdot))$ y cuyo término E_∞ es isomorfo al graduado por una filtración adecuada de $\underset{n}{\oplus}\mathbb{R}^n(GF)(M^\cdot)$, por el teorema del functor compuesto de Grothendieck.

La sucesión espectral asociada a $\underset{n,p+q=n}{\oplus}\bar{E}_2^{p,q} = \underset{n,p+q=n}{\oplus}R^qG(\mathbb{R}^pF(M^\cdot))$ que converge a un graduado de $\underset{n}{\oplus}\mathbb{R}^n(GF)(M^\cdot)$ se conoce como *sucesión espectral del funtor compuesto*, que notaremos

$$R^qG(\mathbb{R}^pF(M^\cdot)) \Longrightarrow \mathbb{R}^{p+q}(GF)(M^\cdot)$$

Sucesión que permite aproximar los hiperfuntores derivados de un funtor compuesto en función de los funtores derivados de los factores.

Veamos que la sucesión espectral del funtor compuesto no depende la resolución de Cartan-Eilenberg considerada.

7. Proposición : *Sean $(M^\cdot,d)$, $(N^\cdot,d')$ y $(I^\cdot,d'')$ complejos inferiormente acotados y supongamos que I_n, $\operatorname{Ker}d''_n$ e $\operatorname{Im}d''_n$ son inyectivos, para todo n. Sea $i\colon M^\cdot \hookrightarrow N^\cdot$ un morfismo inyectivo de complejos (los morfismos $M^n \to N^n$ son inyectivos para todo n), inyectivo en homología. Entonces, todo morfismo de complejos $f\colon M^\cdot \to I^\cdot$ extiende a un morfismo de complejos $g\colon N^\cdot \to I^\cdot$.*

Demostración. Dado un complejo diferencial $(P^\cdot,d)$ inferiormente acotado, denotemos $P^{i\leq n} := \oplus_{i<n}P^i \oplus \operatorname{Ker}d_n$ y $P'^{i\leq n} := \oplus_{i<n}P^i \oplus \operatorname{Im}d_{n-1}$. Tenemos la inclusión obvia $P'^{i\leq n} \hookrightarrow$

$P^{i\leq n}$ y la sucesión exacta

$$0 \to \mathrm{Hom}(H^n(P^\cdot), \mathrm{Ker}\, d''_n) \to \mathrm{Hom}^\cdot(P^{i\leq n}, I^{i\leq n}) \to \mathrm{Hom}^\cdot(P'^{i\leq n}, I'^{i\leq n}) \to 0$$

Si todo morfismo $M'^{i\leq n} \to I'^{i\leq n}$ lo sabemos extender a $N'^{i\leq n} \to I'^{i\leq n}$ entonces todo morfismo $M^{i\leq n} \to I^{i\leq n}$ lo sabemos extender a $N^{i\leq n} \to I^{i\leq n}$: En efecto, como las flechas verticales primera y tercera del diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(H^n(N^\cdot), \mathrm{Ker}\, d''_n) & \longrightarrow & \mathrm{Hom}^\cdot(N^{i\leq n}, I^{i\leq n}) & \longrightarrow & \mathrm{Hom}^\cdot(N'^{i\leq n}, I'^{i\leq n}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}(H^n(M^\cdot), \mathrm{Ker}\, d''_n) & \longrightarrow & \mathrm{Hom}^\cdot(M^{i\leq n}, I^{i\leq n}) & \longrightarrow & \mathrm{Hom}^\cdot(M'^{i\leq n}, I'^{i\leq n}) & \longrightarrow & 0
\end{array}$$

son epiyectivas, la segunda flecha vertical es epiyectiva.

Tenemos la inclusión obvia $P^{i\leq n} \hookrightarrow P'^{i\leq n+1}$ y la sucesión exacta

$$0 \to \mathrm{Hom}(\mathrm{Im}\, d_n, \mathrm{Im}\, d''_n) \to \mathrm{Hom}^\cdot(P'^{i\leq n+1}, I'^{i\leq n+1}) \to \mathrm{Hom}^\cdot(P^{i\leq n}, I^{i\leq n}) \to 0$$

Si todo morfismo $M^{i\leq n} \to I^{i\leq n}$ lo sabemos extender a $N^{i\leq n} \to I^{i\leq n}$ entonces todo morfismo $M'^{i\leq n+1} \to I'^{i\leq n+1}$ lo sabemos extender a $N'^{i\leq n+1} \to I'^{i\leq n+1}$: En efecto, como las flechas verticales primera y tercera del diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(\mathrm{Im}\, d'_n, \mathrm{Im}\, d''_n) & \longrightarrow & \mathrm{Hom}^\cdot(N'^{i\leq n+1}, I'^{i\leq n+1}) & \longrightarrow & \mathrm{Hom}^\cdot(N^{i\leq n}, I^{i\leq n}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}(\mathrm{Im}\, d_n, \mathrm{Im}\, d''_n) & \longrightarrow & \mathrm{Hom}^\cdot(M'^{i\leq n+1}, I'^{i\leq n+1}) & \longrightarrow & \mathrm{Hom}^\cdot(M^{i\leq n}, I^{i\leq n}) & \longrightarrow & 0
\end{array}$$

son epiyectivas, la segunda flecha vertical es epiyectiva.

En conclusión, si todo morfismo $M^{i\leq n} \to I^{i\leq n}$ lo sabemos extender a $N^{i\leq n} \to I^{i\leq n}$ entonces todo morfismo $M^{i\leq n+1} \to I^{i\leq n+1}$ lo sabemos extender a $N^{i\leq n+1} \to I^{i\leq n+1}$ y terminamos por recurrencia.

□

8. Proposición: *Sea $M^\cdot$ un complejo inferiormente acotado, $i\colon M^\cdot \to N^{\cdot\cdot}$ una resolución (i.e., $M^n \to N^{n,\cdot}$ es acíclico para todo n) y $f\colon M^\cdot \to I^{\cdot\cdot}$ una resolución de Cartan-Eilenberg. Entonces, existe un morfismo de bicomplejos $g\colon N^{\cdot\cdot} \to I^{\cdot\cdot}$ tal que $f = g \circ i$.*

Demostración. El morfismo $M^\cdot \to I^{\cdot 0}$ extiende a un morfismo $N^{\cdot 0} \to I^{\cdot 0}$. El morfismo $N^{\cdot 0}/M^\cdot \to I^{\cdot 1}$ extiende a un morfismo $N^{\cdot 1} \to I^{\cdot 1}$. Etc. □

Por tanto si tenemos dos resoluciones de Cartan-Eilenberg $M^\cdot \to I^{\cdot\cdot}$, $M^\cdot \to J^{\cdot\cdot}$, existe un morfismo de bicomplejos $F(I^{\cdot\cdot}) \to F(J^{\cdot\cdot})$, cuyos términos $\bar{E}_2^{p,q}$ son iguales, y convergen a un graduado de $\mathbb{R}^\cdot F(M^\cdot)$ por ciertas filtraciones, luego el morfismo identidad inducido en $\mathbb{R}^\cdot F(M^\cdot)$ aplica biyectivamente una filtración en la otra.

9. Ejemplos: Dado un complejo de haces $K^\cdot$ en un espacio topológico X, sea $F = \Gamma(X,-)$. Se tiene la sucesión espectral de hipercohomología, cuyo primer término $E_1^{p,q}$ es $H^q(X,K^p)$ y que converge a un graduado de $\mathbb{H}^\cdot(X,K^\cdot)$.

El funtor $\underline{\mathrm{Hom}}_{\mathscr{O}_X}(M,-)$ transforma inyectivos en flascos, por 10.6.4 y estos son $\Gamma(X,-)$-acíclicos. De la igualdad $\mathrm{Hom}_{\mathscr{O}_X}(M,N) = \Gamma(X,\underline{\mathrm{Hom}}_{\mathscr{O}_X}(M,N))$, se tiene la sucesión espectral convergente del funtor compuesto

$$H^q(X,\underline{\mathrm{Ext}}^p_{\mathscr{O}_X}(M,N)) \Longrightarrow \mathrm{Ext}^{p+q}_{\mathscr{O}_X}(M,N)$$

Sean $X \xrightarrow{f} Y \xrightarrow{g} Z$ aplicaciones continuas. El funtor f_* transforma haces inyectivos en haces g_*-acíclicos (pues la imagen directa de un inyectivo es inyectivo). Por tanto, se tiene una sucesión espectral convergente

$$R^q g_*(R^p f_*(F)) \Longrightarrow R^{p+q}(g\circ f)_*(F)$$

conocida como *sucesión espectral de Leray*.

10. Ejemplo: Supongamos ahora que $\mathscr{C}$ es una categoría abeliana con suficientes proyectivos. El hiperfuntor derivado por la izquierda de un funtor aditivo covariante F lo hemos denotado $\mathbb{L}F(M^\cdot) = F(P^\cdot(M^\cdot))$, y el n-ésimo funtor derivado por la izquierda de F

$$\mathbb{L}_nF(M^\cdot) = H^{-n}(\mathbb{L}F(M^\cdot)).$$

La restricción a $\mathscr{C}$ serán de los funtores derivados por la izquierda n-ésimos de F los denotamos $\mathscr{L}_nF$. Sea G otro funtor aditivo y supongamos que F transforma proyectivos en G-acíclicos, entonces tenemos la sucesión espectral del funtor compuesto

$$\mathscr{L}_qG(\mathbb{L}_pF(M^\cdot)) \longrightarrow \mathbb{L}_{p+q}(GF)(M^\cdot)$$

Sea $A \to B$ un morfismo de anillos, M un B-módulo. Sea $\mathscr{C}$ la categoría de A-módulos, $\mathscr{C}'$ la categoría de B-módulos, $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}'$ el funtor definido por $F(N) = N\otimes_A B$ y $G\colon \mathscr{C}' \rightsquigarrow \mathscr{C}'$ el funtor definido por $G(M') = M'\otimes_B M$. Entonces, $\mathbb{L}_iF(N) = \mathrm{Tor}_i^A(N,B)$ y $\mathbb{L}_jG(M') = \mathrm{Tor}_j^B(M',M)$. Además, $GF(N) = N\otimes_A M$ y $\mathbb{L}_n(FG)(N) = \mathrm{Tor}_n^A(N,M)$. Tenemos la sucesión espectral de los tores

$$\mathrm{Tor}_i^B(\mathrm{Tor}_j^A(N,B),M) \Longrightarrow \mathrm{Tor}_{i+j}^A(N,M)$$

Sea $f\colon Y \to X$ un morfismo de esquemas cuasicompacto, $\mathscr{M}$ un $\mathscr{O}_X$-móulo cuasicoherente y $\mathscr{N}$ un $\mathscr{O}_Y$-módulo cuasicoherente. Tenemos la sucesión espectral de los tores

$$\underline{\mathrm{Tor}}_i^{f_*\mathscr{O}_Y}(\underline{\mathrm{Tor}}_j^{\mathscr{O}_X}(\mathscr{N},f_*\mathscr{O}_Y),f_*\mathscr{M}) \Longrightarrow \underline{\mathrm{Tor}}_{i+j}^{\mathscr{O}_X}(\mathscr{N},f_*\mathscr{M})$$

Capítulo 17

Teoría K y Riemann-Roch

Todos los esquemas considerados serán noetherianos, salvo que se diga lo contrario.

17.1. Introducción

Es claro que el grupo $K(X)$, que es el grupo universal para las funciones aditivas sobre los $\mathcal{O}_X$-módulos coherentes, ha de tener un papel central en la determinación de las funciones aditivas, como es la característica de Euler-Poincaré

$$\chi(\mathcal{M}) = \sum_{i\geq 0}(-1)^i \dim_k H^i(X,\mathcal{M})$$

de los haces coherentes cuando X es propio sobre un cuerpo k. Lo sorprendente es que, al menos cuando X es regular, tal grupo posea muchas de las propiedades de una teoría cohomológica – producto cup, imágenes directas e inversas, fórmula de proyección, Gysin, teorema de periodicidad, (donde ha de entenderse que la clase de cohomología de cada subvariedad Y viene representada por el haz de anillos locales $\mathcal{O}_Y$.) – y permita establecer un cálculo geométrico con los propios módulos, no con ciclos. Así la teoría K fundamenta hasta cierto punto una teoría global de la intersección.

No obstante, este anillo $K(X)$ es demasiado fino para desarrollar una teoría usual de la intersección, porque los anillos locales de subvariedades racionalmente equivalentes pueden no coincidir en teoría K. Por eso se considera el graduado $GK(X)$ de $K(X)$ por la filtración definida por la codimensión del soporte, de modo que cada haz coherente $\mathcal{M}$ con soporte de codimensión d coincide en $GK(X)$ con el ciclo

$$[\mathcal{M}] = \sum_{cod\, x=p} l_{\mathcal{O}_X}(\mathcal{M}_x)[\mathcal{O}_X/\mathfrak{p}_x]$$

Esta filtración es compatible con el producto de $K(X)$, al menos cuando X es liso, y el correspondiente anillo graduado $GK(X)$ ya tiene todas las propiedades razonables

de una teoría global de la intersección, incluyendo una teoría de clases de Chern de haces localmente libres. Esta teoría global es independiente de una teoría local previa basada en números locales de intersección y en su compatibilidad con cierta equivalencia de ciclos, que ha sido siempre el enfoque tradicional, como es el caso de la teoría del anillo de Chow $A(X)$, anillo que coincide con $GK(X)$ salvo elementos de torsión: $GK(X) \otimes \mathbb{Q} = A(X) \otimes \mathbb{Q}$.

17.2. Teoría K

1. Definición: Diremos que una función f, definida sobre la categoría de los $\mathcal{O}_X$-módulos coherentes, y con valores en un grupo abeliano es aditiva, cuando para toda sucesión exacta

$$0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$$

de $\mathcal{O}_X$-módulos coherentes, se cumple que $f(\mathcal{M}) = f(\mathcal{M}') + f(\mathcal{M}'')$.

2. Definición: Llamaremos grupo K de los haces coherentes, que denotaremos por $K_\cdot(X)$, al cociente del grupo abeliano libre de base los $\mathcal{O}_X$-módulos coherentes (módulo isomorfismos) por el subgrupo generado por los elementos $\mathcal{M} - \mathcal{M}' - \mathcal{M}''$, para cada sucesión exacta $0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$.

Si en esta definición se sustituye "$\mathcal{O}_X$-módulo coherente" por "$\mathcal{O}_X$-módulo coherente localmente libre" se obtiene la definición de grupo K de los haces localmente libres, y se denota $K^\cdot(X)$.

Es obvio que dar una función aditiva sobre la categoría de los $\mathcal{O}_X$-módulos coherentes con valores en un grupo abeliano G equivale a dar un morfismo de grupos $K_\cdot(X) \to G$. Análogamente para $K^\cdot(X)$.

Todo haz coherente $\mathcal{M}$ define un elemento de $K_\cdot(X)$, que se denota por $[\mathcal{M}]$, o bien $\mathcal{M}$ si no causa confusión. Igualmente, todo haz $\mathcal{L}$ localmente libre define un elemento de $K_\cdot(X)$, que se denota por $[\mathcal{L}]$, o bien $\mathcal{L}$ si no causa confusión.

3. Proposición: *$K^\cdot(X)$ es un anillo conmutativo con unidad con el producto definido extendiendo bilinealmente la igualdad*

$$[\mathcal{L}] \cdot [\mathcal{L}'] := [\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}']$$

Igualmente, $K_\cdot(X)$ es un $K^\cdot(X)$-módulo, con el producto definido extendiendo bilinealmente la igualdad

$$[\mathcal{L}] \cdot [\mathcal{M}] := [\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{M}]$$

con $\mathcal{M}$ coherente y $\mathcal{L}$ localmente libre.

Demostración. Los productos están bien definidos porque si

$$0 \to \mathscr{M}' \to \mathscr{M} \to \mathscr{M}'' \to 0$$

es una sucesión exacta de $\mathscr{O}_X$-módulos coherentes, entonces $0 \to \mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}' \to \mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M} \to \mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}'' \to 0$ es exacta. Por tanto, si $[\mathscr{M}] = [\mathscr{M}'] + [\mathscr{M}'']$, entonces $[\mathscr{L}] \cdot [\mathscr{M}] = [\mathscr{L}] \cdot [\mathscr{M}'] + [\mathscr{L}] \cdot [\mathscr{M}'']$. Todo lo demás es una sencilla comprobación. □

4. Notación: Dado un subesquema cerrado $Z \subset X$, denotaremos $[Z]$ o simplemente Z, al elemento de $K_\cdot(X)$ definido por el $\mathscr{O}_X$-módulo coherente $\mathscr{O}_Z$, y diremos que es la clase de Z en $K_\cdot(X)$.

5. Definición: Denotaremos $Z_\cdot(X)$ el grupo libre generado por los subesquemas cerrados íntegros de X. Los elementos de $Z_\cdot(X)$ se denominan ciclos de X.

6. Teorema: *El morfismo $\phi\colon Z_\cdot(X) \to K_\cdot(X)$, $\phi(Y) := Y$ es epiyectivo.*

Demostración. Se procede por inducción noetheriana sobre el ideal anulador de los haces coherentes.

Sea $\mathscr{M}$ un haz coherente sobre X. Sea x un punto genérico del soporte de $\mathscr{M}$ y $\mathfrak{p}_x$ el haz de ideales de funciones que se anulan en x. Consideremos la sucesión exacta

$$0 \to \mathfrak{p}_x\mathscr{M} \to \mathscr{M} \to \mathscr{M}/\mathfrak{p}_x\mathscr{M} \to 0$$

Si $\mathfrak{p}_x\mathscr{M} \neq 0$, por inducción, el teorema es cierto para $\mathfrak{p}_x\mathscr{M}$, y para $\mathscr{M}/\mathfrak{p}_x\mathscr{M}$, luego para $\mathscr{M}$.

Si $\mathfrak{p}_x\mathscr{M} = 0$, entonces $\operatorname{Sop}\mathscr{M} = \bar{x}$ y podemos suponer que $X = \bar{x}$, que es un esquema íntegro. Sea $\widetilde{\mathscr{M}_x}$ el haz constante de fibra $\mathscr{M}_x$. Consideremos el morfismo natural $\varphi\colon \mathscr{M} \to \widetilde{\mathscr{M}_x}$. El núcleo $\operatorname{Ker}\varphi \neq \mathscr{M}$ está en las hipótesis de inducción, luego basta demostrar el teorema para $\operatorname{Im}\varphi$. Es decir, podemos suponer que $\mathscr{M}$ no tiene torsión. En este caso, por 14.2.2 2., existe un haz de ideales $I \neq 0$ no nulo y una sucesión exacta

$$0 \to I \to \mathscr{M} \to \mathscr{M}/I \to 0$$

$\mathscr{M}/I$ está en las hipótesis de inducción e I verifica el teorema porque $\mathscr{O}_X/I$ está en la hipótesis de inducción, luego concluimos el teorema para $\mathscr{M}$.

□

Imagen directa e inversa.

7. Definición: Sea $f : X \to Y$ un morfismo de esquemas noetherianos. Si $\mathscr{L}$ es un $\mathscr{O}_Y$-módulo coherente localmente libre, se define $f^!(\mathscr{L}) = f^*\mathscr{L}$. Entonces $f^!$ es una función

aditiva de la categoría de $\mathcal{O}_Y$-módulos coherentes localmente libres en $K^{\cdot}(X)$, luego define un morfismo de grupos

$$f^!: K^{\cdot}(Y) \to K^{\cdot}(X)$$

que se denomina imagen inversa admirable. Es inmediato ver que $f^!$ es un morfismo de anillos. Si $X \xrightarrow{f} Y \xrightarrow{g} Z$ son morfismos de esquemas noetherianos, entonces $(g \circ f)^! = g^! \circ f^!$.

Si f es un morfismo plano, se define igualmente el morfismo $f^!: K_{\cdot}(Y) \to K_{\cdot}(X)$ por extensión lineal de la función aditiva $f^!(\mathcal{M}) = f^*\mathcal{M}$.

Si $i: Y \hookrightarrow X$ es una inmersión cerrada regular, para todo $\mathcal{O}_X$-módulo coherente $\mathcal{M}$ se define $i^!(\mathcal{M}) = \sum(-1)^i \underline{\mathrm{Tor}}_i^{\mathcal{O}_X}(\mathcal{O}_Y, \mathcal{M})$. Esta suma es finita por ser i inmersión regular. Por la sucesión exacta larga de tores, esta función es aditiva, luego define un morfismo de grupos

$$i^!: K_{\cdot}(X) \to K_{\cdot}(Y)$$

8. Ejercicio: Sea $f: X \to Y$ un morfismo plano y $Z \subset Y$ un subesquema cerrado. Probar que $f^!([Z]) = [f^{-1}(Z)]$.

9. Definición: Sea $f: X \to Y$ un morfismo propio. Para todo $\mathcal{O}_X$-módulo coherente $\mathcal{M}$ los haces $R^i f_*(\mathcal{M})$ son $\mathcal{O}_Y$-módulos coherentes y son nulos para $i > \dim X$. Por la sucesión exacta larga de las imágenes directas superiores la función $\mathcal{M} \mapsto \sum_{i \geq 0} (-1)^i R^i f_*(\mathcal{M})$ de la categoría de $\mathcal{O}_X$-módulos coherentes con valores en $K_{\cdot}(Y)$ es aditiva. Por tanto define un morfismo de grupos

$$f_!: K_{\cdot}(X) \to K_{\cdot}(Y)$$

que se denomina imagen directa admirable de Grothendieck.

10. Ejercicio: Sea $i: Y \hookrightarrow X$ una inmersión cerrada. Para todo módulo coherente $\mathcal{M}$ en Y, se verifica que $i_!\mathcal{M} = i_*\mathcal{M}$, en particular si Z es un subesquema cerrado en Y, $i_!(Z) = Z$.

Veamos ahora que la imagen directa admirable es compatible con la composición de morfismos, es decir, $(g \circ f)_! = g_! \circ f_!$. Para ello necesitaremos el siguiente lema.

11. Lema: *Sea $\mathcal{M}$ un complejo filtrado y graduado de $\mathcal{O}_X$-módulos cuasi-coherentes con sólo un número finito de módulos de cohomología no nulos y que son haces coherentes. Supongamos que la sucesión espectral $E_2^{p,q}$ asociada es de $\mathcal{O}_X$-módulos coherentes y convergente. Si $E_2^{p,q}$ es no nulo solamente para un número finito de valores p y q, entonces*

$$\sum_{p,q}(-1)^{p+q}E_2^{p,q} = \sum_n (-1)^n H^n(\mathcal{M})$$

en $K_{\cdot}(X)$

Demostración. Todas las sumas que aparecen tienen sentido, porque sólo hay un número finito de términos no nulos.

Los términos $E_2^{p,q}$ forman un complejo cuya cohomología son los términos $E_3^{p,q}$, luego por la invarianza de la característica de Euler-Poincaré por paso a la cohomología, en $K_\cdot(X)$ se cumple que

$$\sum_{p,q}(-1)^{p+q}E_2^{p,q} = \sum_{p,q}(-1)^{p+q}E_3^{p,q} = \cdots = \sum_{p,q}(-1)^{p+q}E_r^{p,q}$$

Para r suficientemente grande, la diferencial $d_r\colon E_r^{p,q} \to E_r^{p+r,q-r+1}$ es nula, porque $E_r^{p,q}$ tiene un número finito de términos no nulos. Por tanto, $E_r^{p,q} = E_\infty^{p,q}$, para $r >> 0$. Por último, los términos de $E_\infty^{p,q}$ forman el graduado asociado a una filtración de la cohomología de $\mathscr{M}$, luego en $K_\cdot(X)$ se cumple que

$$\sum_{p,q}(-1)^{p+q}E_2^{p,q} = \sum_n(-1)^n H^n(\mathscr{M})$$

□

12. Proposición: *Si $X \xrightarrow{f} Y \xrightarrow{g} Z$ son morfismos propios, entonces $(g\circ f)_! = g_!\circ f_!$.*

Demostración. $R^q g_*(R^p f_*(\mathscr{M}))$ converge a $R^{p+q}(gf)_*(\mathscr{M})$, por la sucesión espectral de Leray. Por tanto,

$$\begin{aligned}(gf)_!(\mathscr{M}) &= \sum_n(-1)^n R^n(gf)_*(\mathscr{M}) = \sum_{p,q}(-1)^{p+q}R^p g_*(R^q f_*(\mathscr{M}))\\ &= \sum_q(-1)^q g_!(R^q f_*(\mathscr{M})) = g_!(f_!(\mathscr{M}))\end{aligned}$$

□

13. Proposición: *Si $Z \xhookrightarrow{i} Y \xhookrightarrow{j} X$ son inmersiones cerradas regulares, entonces $(j\circ i)^! = i^!\circ j^!$.*

Demostración. Se argumenta como en la proposición anterior con la sucesión espectral (del funtor compuesto) $\underline{\mathrm{Tor}}_j^{\mathscr{O}_Y}(\mathscr{O}_Z, \underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{M}))$ que converge a $\underline{\mathrm{Tor}}_{i+j}^{\mathscr{O}_X}(\mathscr{O}_Z, \mathscr{M})$. □

14. Fórmula de proyección: *Si $f\colon X \to Y$ es un morfismo propio, entonces $f_!$ es un morfismo de $K^\cdot(Y)$-módulos. Es decir, para todo $x \in K_\cdot(X)$ y todo $y \in K^\cdot(Y)$ se cumple*

$$f_!(x\cdot f^!(y)) = f_!(x)\cdot y$$

Demostración. $R^i f_*(\mathscr{M})\otimes_{\mathscr{O}_Y}\mathscr{L} = R^i f_*(\mathscr{M}\otimes_{\mathscr{O}_X} f^*\mathscr{L})$ para todo módulo coherente $\mathscr{M}$ sobre X y todo módulo coherente localmente libre $\mathscr{L}$ sobre Y: la cuestión es local en Y, luego puede suponerse que $\mathscr{L}$ es trivial y entonces la igualdad es inmediata. □

15. Proposición: *Sea $f: X \to Y$ un morfismo propio y $g: \overline{Y} \to Y$ un morfismo plano. Consideremos el diagrama cartesiano*

$$\begin{array}{ccc} X \times_Y \overline{Y} & \xrightarrow{\bar{g}} & X \\ {\scriptstyle \bar{f}}\downarrow & & \downarrow{\scriptstyle f} \\ \overline{Y} & \xrightarrow{g} & Y \end{array}$$

Se verifica que $g^!(f_!(x)) = \bar{f}_!(\bar{g}^!(x))$ sobre $K_\cdot(X)$.

Demostración. Es consecuencia del teorema de cambio de base 13.4.6. □

16. Teorema (Gysin): *Sea $j: Y \hookrightarrow X$ un subesquema cerrado y $U \overset{i}{\hookrightarrow} X$ el abierto complementario. Se verifica la sucesión exacta*

$$K_\cdot(Y) \xrightarrow{j_!} K_\cdot(X) \xrightarrow{i^!} K_\cdot(U) \to 0$$

Demostración. Todo módulo coherente en U es restricción de un módulo coherente sobre X, por el Problema 12.1.14 del capítulo 12, luego $i^!$ es epiyectivo. Obviamente $i^! j_! = 0$. Sólo nos falta probar que $\operatorname{Ker} i^! \subseteq \operatorname{Im} j_!$.

Denotemos $K_\cdot^Y(X)$ el grupo K de los $\mathscr{O}_X$-módulos coherentes concentrados en Y. Se tiene un morfismo natural $K_\cdot^Y(X) \to K_\cdot(X)$, cuya imagen está contenida en el núcleo de $i^!$.

Dado un módulo coherente $\mathscr{M}$ en U, dos extensiones coherentes $\tilde{\mathscr{M}}$, $\tilde{\mathscr{M}}'$ a X difieren en teoría K en haces concentrados en Y. En efecto, el núcleo del morfismo natural $\tilde{\mathscr{M}} \to i_* \mathscr{M}$ es un haz coherente concentrado en Y. Lo mismo decimos con $\tilde{\mathscr{M}}'$. La imagen de $\tilde{\mathscr{M}}$ en $i_* \mathscr{M}$ difiere en haces concentrados en Y de la suma de las imágenes de $\tilde{\mathscr{M}}$ y $\tilde{\mathscr{M}}'$ en $i_* \mathscr{M}$. Lo mismo decimos con $\tilde{\mathscr{M}}'$. Con todo se concluye.

Ahora es fácil concluir que $s: K_\cdot(U) \to K_\cdot(X)/K_\cdot^Y(X)$, $\mathscr{M} \mapsto \tilde{\mathscr{M}}$, está bien definido. Así, dado $x \in K_\cdot(X)$, si $i^!(x) = 0$ entonces $0 = s(0) = s(i^!(x)) = \bar{x}$ y $x \in K_\cdot^Y(X)$.

Por último, el morfismo $j_!: K_\cdot(Y) \to K_\cdot^Y(X)$ es epiyectivo (de hecho, es isomorfismo), pues si $\mathscr{N}$ es un haz concentrado en Y, entonces la filtración $\{\mathfrak{p}_Y^n \cdot \mathscr{N}\}_{n \geq 0}$ de $\mathscr{N}$ es finita y su graduado está anulado por $\mathfrak{p}_Y$, es decir, es un $\mathscr{O}_Y$-módulo.

□

17. Teorema: *Sea $\pi: E \to X$ localmente (sobre X) isomorfo a $X \times \mathbb{A}^n$. El morfismo*

$$\pi^!: K_\cdot(X) \to K_\cdot(E)$$

es epimorfismo. Si además existe una sección s de π entonces $\pi^!$ es isomorfismo.

Demostración. La epiyectividad, por inducción noetheriana y Gysin, se reduce al caso $E = X \times \mathbb{A}^n$ y $X = \operatorname{Spec} A$ afín. Factorizando la proyección $X \times \mathbb{A}^n \to X$ en $X \times \mathbb{A}^n \to X \times \mathbb{A}^{n-1} \to X$, se reduce al caso $n = 1$, es decir, $E = X \times \mathbb{A}^1 = \operatorname{Spec} A[t]$. Basta ver la epiyectividad sobre los cerrados íntegros de $X \times \mathbb{A}^1$. Sea Z un tal cerrado y $\mathfrak{q}$ el ideal primo de $A[t]$ que lo define. Sea $\mathfrak{p}$ su antimagen en A por la inclusión $A \to A[t]$. Si $\mathfrak{q} = \mathfrak{p} \cdot A[t]$, entonces $A[t]/\mathfrak{q} = \pi^!(A/\mathfrak{p})$ y hemos concluido. En caso contrario, $\mathfrak{q}$ define un ideal primo no nulo $\bar{\mathfrak{q}}$ de $(A/\mathfrak{p})[t]$. Es claro que, localizando por una función no nula de $A/\mathfrak{p}$, $\bar{\mathfrak{q}}$ es un ideal principal. Por tanto, existe $f \in A$ que no pertenece a $\mathfrak{p}$ tal que $\mathfrak{q} = (\mathfrak{p}, P(t))$ en $A_f[t]$. Denotemos $\bar{A} = A_f/\mathfrak{p}A_f$. Se tiene entonces la sucesión exacta

$$0 \to \bar{A}[t] \xrightarrow{\cdot \bar{P}(t)} \bar{A}[t] \to A_f[t]/\mathfrak{q} \to 0$$

de donde se deduce que $A_f[t]/\mathfrak{q} = 0$ en teoría K. Si denotamos $U = \operatorname{Spec} A_f$, $Y = X - U$, hemos probado que Z se anula en $K_\cdot(U \times \mathbb{A}^1)$, luego por Gysin Z está en la imagen de $K_\cdot(Y \times \mathbb{A}^1) \to K_\cdot(X \times \mathbb{A}^1)$. Por inducción noetheriana, $K_\cdot(Y) \to K_\cdot(Y \times \mathbb{A}^1)$ es epiyectivo, luego hemos concluido.

Observemos que $s\colon X \to E$ es una inmersión regular. Es fácil demostrar que si $\mathscr{M} = \pi^* \mathscr{N}$ entonces $\underline{\operatorname{Tor}}_i^{\mathscr{O}_E}(\mathscr{M}, \mathscr{O}_X) = 0$ para $i > 0$, luego $s^! \circ \pi^! = \mathrm{Id}$ y $\pi^!$ es inyectiva. □

18. Lema: *Sea X un esquema noetheriano, regular y separado. Todo $\mathscr{O}_X$-módulo coherente es cociente de un $\mathscr{O}_X$-módulo localmente libre.*

Demostración. Sea $X = \operatorname{Spec} A$ un esquema afín regular de cuerpo de funciones Σ y de dimensión n. Recordemos que A es un dominio localmente de factorización única. Si $Y \subset X$ es un cerrado tal que alguna de sus componentes sea de dimensión menor que $n-1$, entonces $X \backslash Y$ no es un esquema afín. En efecto, restringiéndonos a un abierto básico, podemos suponer que $\dim Y < n-1$. Se verifica

$$\Gamma(X \backslash Y, \mathscr{O}_X) = \bigcap_{\substack{x \in X \backslash Y \\ \text{alt.} \mathfrak{p}_x = 1}} \mathscr{O}_{X,x} = \bigcap_{\substack{x \in X \\ \text{alt.} \mathfrak{p}_x = 1}} \mathscr{O}_{X,x} = A$$

luego $X \backslash Y$ no es afín.

Volvamos a las hipótesis del teorema. Como consecuencia del párrafo anterior, si U es un abierto afín, entonces $X \backslash U$ es unión de subesquemas irreducibles de codimensión 1. Por tanto, el haz de ideales de las funciones que se anulan en $X \backslash U$ es localmente principal.

Sea U_i un recubrimiento finito de X por abiertos afines y $\mathfrak{p}_i$ los haces de ideales de las funciones que se anulan en $X \backslash U_i$. Por el Problema 12.1.27 del capítulo 12, para todo haz coherente $\mathscr{M}$ se cumple que

$$\varinjlim_n \operatorname{Hom}_{\mathscr{O}_X}(\mathfrak{p}_i^n, \mathscr{M}) = \Gamma(U_i, \mathscr{M})$$

Por ser U_i afín y $\mathscr{M}$ coherente, existe un número finito de secciones de $\mathscr{M}$ sobre U_i que generan la fibra de $\mathscr{M}$ en todo punto de U_i. Es decir, para cada índice i, existe una suma directa finita de potencias de $\mathfrak{p}_i$ y un morfismo de esta suma directa en $\mathscr{M}$, que es epiyectivo al restringirlo a U_i. La suma directa sobre i de los haces localmente libres así construidos, se epiyecta sobre $\mathscr{M}$. □

19. Teorema: *Sea X un esquema noetheriano, regular y separado. El morfismo natural $K^{\cdot}(X) \to K_{\cdot}(X)$, $[\mathscr{P}] \mapsto [\mathscr{P}]$ es un isomorfismo.*

Demostración. Construyamos el morfismo inverso. Por el lema anterior y el teorema de Serre 7.5.8, todo módulo coherente $\mathscr{M}$ se resuelve por un número finito de módulos localmente libres, $\mathscr{P}_{\cdot} \to \mathscr{M} \to 0$. Por tanto, $\mathscr{M} = \sum_i (-1)^i \mathscr{P}_i$ en $K_{\cdot}(X)$. Definimos el morfismo inverso $K_{\cdot}(X) \to K^{\cdot}(X)$, por $\mathscr{M} \mapsto \sum_i (-1)^i \mathscr{P}_i$.

Tenemos que ver:

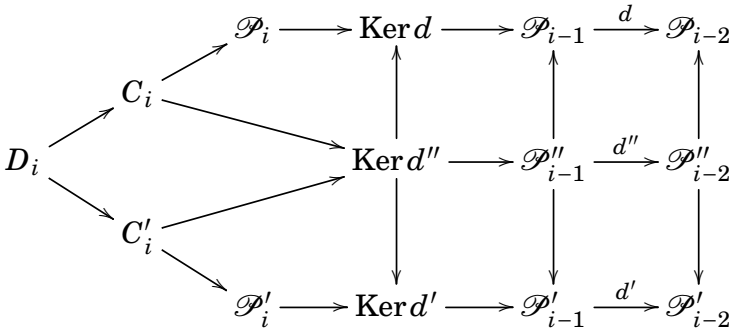
a) Si $\mathscr{P}_{\cdot}$ y $\mathscr{P}'_{\cdot}$ son resoluciones finitas de $\mathscr{M}$ por módulos localmente libres, entonces $\sum_i (-1)^i \mathscr{P}_i = \sum_i (-1)^i \mathscr{P}'_i$ en $K^{\cdot}(X)$.

b) Dada una sucesión exacta de módulos coherentes

$$0 \to \mathscr{M}' \to \mathscr{M} \to \mathscr{M}'' \to 0$$

y resoluciones finitas $\mathscr{P}'_{\cdot}$, $\mathscr{P}_{\cdot}$ y $\mathscr{P}''_{\cdot}$ por módulos localmente libres de $\mathscr{M}'$, $\mathscr{M}$ y $\mathscr{M}''$, se verifica $\sum_i (-1)^i \mathscr{P}'_i + \sum_i (-1)^i \mathscr{P}''_i = \sum_i (-1)^i \mathscr{P}_i$ en $K^{\cdot}(X)$.

Veamos a): Construyamos una resolución $\mathscr{P}''_{\cdot}$ de $\mathscr{M}$ por haces localmente libres que se epiyecte en $\mathscr{P}_{\cdot}$ y $\mathscr{P}'_{\cdot}$. Supuesto construido $\mathscr{P}''_{i-1}$, construyamos $\mathscr{P}''_i$. Consideremos el diagrama



donde hemos supuesto que $\operatorname{Ker} d''$ se epiyecta en $\operatorname{Ker} d$ y $\operatorname{Ker} d'$, sin más que añadirle a $\mathscr{P}''_{i-1}$ un haz localmente libre que se epiyecte en ambos, y donde hemos definido $C_i := \mathscr{P}_i \times_{\operatorname{Ker} d} \operatorname{Ker} d''$, $C'_i := \mathscr{P}'_i \times_{\operatorname{Ker} d'} \operatorname{Ker} d''$, $D_i := C_i \times_{\operatorname{Ker} d''} C'_i$ y $\mathscr{P}''_i$ cualquier haz localmente libre que se epiyecte en D_i.

El núcleo, $N_\cdot$, del epimorfismo y cuasi-isomorfismo $\mathscr{P}''_\cdot \to \mathscr{P}_\cdot$, es un complejo exacto de haces localmente libres. Por tanto, $\sum_i (-1)^i \mathscr{P}''_i = \sum_i (-1)^i N_i + \sum_i (-1)^i \mathscr{P}_i = \sum_i (-1)^i \mathscr{P}_i$. Argumentando igual con $\sum_i (-1)^i \mathscr{P}'_i$, concluimos que $\sum_i (-1)^i \mathscr{P}_i = \sum_i (-1)^i \mathscr{P}'_i$.

Veamos b): Dado un módulo localmente libre $\mathscr{Q}'_0$ y un epimorfismo $\pi' : \mathscr{Q}'_0 \to \mathscr{M}'$, componiendo con la inclusión $\mathscr{M}' \hookrightarrow \mathscr{M}$ tenemos un morfismo $\mathscr{Q}'_0 \to \mathscr{M}$. Dado otro módulo localmente libre $\mathscr{Q}''_0$ y un epimorfismo $\mathscr{Q}''_0 \to \mathscr{M}$, podemos definir un epimorfismo $\pi : \mathscr{Q}_0 := \mathscr{Q}'_0 \oplus \mathscr{Q}''_0 \to \mathscr{M}$ y un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{M}' & \longrightarrow & \mathscr{M} & \longrightarrow & \mathscr{M}'' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \pi'} & & \uparrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \pi''} & & \\ 0 & \longrightarrow & \mathscr{Q}'_0 & \longrightarrow & \mathscr{Q}'_0 \oplus \mathscr{Q}''_0 & \longrightarrow & \mathscr{Q}''_0 & \longrightarrow & 0 \end{array}$$

Argumentando igual con $\operatorname{Ker}\pi'$, $\operatorname{Ker}\pi$ y $\operatorname{Ker}\pi''$, podemos construir resoluciones por módulos localmente libres $\mathscr{Q}'_\cdot, \mathscr{Q}_\cdot, \mathscr{Q}''_\cdot$ de modo que $\mathscr{Q}_i = \mathscr{Q}'_i \oplus \mathscr{Q}''_i$. Ahora ya, por el apartado a) concluimos el apartado b).

□

20. Notación: En las hipótesis del teorema los grupos $K^\cdot(X)$ y $K_\cdot(X)$ son canónicamente isomorfos, y se denotan con el símbolo $K(X)$.

21. Observación: Es importante observar que el isomorfismo $K^\cdot(X) = K_\cdot(X)$ permite definir el producto de dos módulos coherentes:

Sean $\mathscr{M}$ y $\mathscr{M}'$ módulos coherentes sobre X. Si $\mathscr{L}_\cdot$ y $\mathscr{L}'_\cdot$ son sendas resoluciones de $\mathscr{M}$ y $\mathscr{M}'$ por haces localmente libres, por definición, $\mathscr{M} \cdot \mathscr{M}' = (\sum_i (-1)^i \mathscr{L}_i) \cdot (\sum_j (-1)^j \mathscr{L}'_j) = \sum_{i+j} (-1)^{i+j} \mathscr{L}_i \otimes_{\mathscr{O}_X} \mathscr{L}'_j$. Ahora bien, como un complejo es igual a su cohomología en teoría K, tenemos que

$$\mathscr{M} \cdot \mathscr{M}' = \sum_{i \geq 0} (-1)^i \underline{\operatorname{Tor}}_i^{\mathscr{O}_X}(\mathscr{M}, \mathscr{M}')$$

Análogamente, dado un morfismo $f : X \to Y$ entre esquemas regulares separados podemos definir la imagen inversa admirable $f^!$ de un módulo coherente; explícitamente

$$f^!(\mathscr{M}) = \sum_{i \geq 0} (-1)^i \underline{\operatorname{Tor}}_i^{\mathscr{O}_Y}(\mathscr{O}_X, \mathscr{M})$$

22. Proposición: *Si Y, Y' son subvariedades cerradas de una variedad lisa separada X, entonces*

$$Y \cdot Y' = \delta^!(Y \times Y')$$

siendo $\delta : X \hookrightarrow X \times X$ el morfismo diagonal.

Demostración. Si $\mathscr{P}$ y $\mathscr{P}'$ son módulos coherentes localmente libres, entonces (Cap. 0, Problema 87)

$$\delta^*(\mathscr{P}\otimes_k\mathscr{P}') = (\mathscr{P}\otimes_k\mathscr{P}')/\Delta\cdot(\mathscr{P}\otimes_k\mathscr{P}') = \mathscr{P}\otimes_{\mathscr{O}_X}\mathscr{P}'$$

siendo Δ el ideal de la diagonal. Por tanto, $\mathscr{P}\cdot\mathscr{P}' = \delta^!(\mathscr{P}\otimes_k\mathscr{P}')$, en teoría K. Se concluye por linealidad. □

23. Proposición: *Sea $i: Y\hookrightarrow X$ una inmersión cerrada entre esquemas noetherianos regulares y separados. Para todo subesquema cerrado $Z\subset X$ se verifica*

$$i_!(i^!Z) = Y\cdot Z$$

Demostración. Es consecuencia inmediata de la fórmula de la proyección. □

17.2.1. Teoría K de los fibrados proyectivos

Sea E será un $\mathscr{O}_X$-módulo localmente libre de rango $n+1$ y $\pi:\mathbb{P}(E)=\operatorname{Proj}B\to X$ el fibrado proyectivo de rango n asociado.

Los siguientes resultados se utilizarán sin mención previa:

1. Para todo número entero $m\geq 0$, se cumple que

$$R^i\pi_*(\mathscr{O}_{\mathbb{P}(E)}(m)) = 0, \text{ para } i>0$$
$$\pi_*(\mathscr{O}_{\mathbb{P}(E)}(m)) = S^m(E^*)$$

   En particular, $\pi_*(\mathscr{O}_{\mathbb{P}(E)}) = \mathscr{O}_X$ y $R^i\pi_*(\mathscr{O}_{\mathbb{P}(E)}) = 0$ para $i>0$.

   En teoría K, $\pi_!(\mathscr{O}_{\mathbb{P}(E)}(m)) = S^m(E^*)$. En particular, $\pi_!\mathscr{O}_{\mathbb{P}(E)} = 1$.

2. Para todo número natural $0<m<\operatorname{rg}E$, se cumple que $R^i\pi_*(\mathscr{O}_{\mathbb{P}(E)}(-m)) = 0$, para $i\geq 0$. En teoría K, $\pi_!(\mathscr{O}_{\mathbb{P}(E)}(-m)) = 0$.

   Por el teorema de Grauert y 13.11.11, si $\mathscr{N}$ es un $\mathscr{O}_X$-módulo coherente entonces $R^i\pi_*(\pi^*\mathscr{N}\otimes\mathscr{O}_{\mathbb{P}(E)}(n)) = \mathscr{N}\otimes R^i\pi_*(\mathscr{O}_{\mathbb{P}(E)}(n))$, para $i\geq 0$ y $n\in\mathbb{Z}$. En particular, $\pi_!\pi^! = \mathrm{Id}$ y $\pi_!(\mathscr{O}_{\mathbb{P}(E)}(-m)\cdot\pi^!\mathscr{N}) = 0$, para $0<m<\operatorname{rg}E$.

24. Teorema de periodicidad : *Sea X un esquema noetheriano, E un $\mathscr{O}_X$-módulo localmente libre de rango $n+1$ y $\pi:\mathbb{P}(E)\to X$ la proyección natural. Sea x_E el elemento de $K^{\cdot}(\mathbb{P}(E))$ definido como $x_E = 1-\mathscr{O}_{\mathbb{P}(E)}(-1)$. Entonces $1, x_E, \ldots, x_E^n$ forman base de $K_{\cdot}(\mathbb{P}(E))$ sobre $K_{\cdot}(X)$. Es decir, el morfismo*

$$K_{\cdot}(X)\oplus\overset{n+1}{\cdots}\oplus K_{\cdot}(X)\longrightarrow K_{\cdot}(\mathbb{P}(E))$$
$$(a_0,\ldots,a_n)\longmapsto\sum\pi^!(a_i)\cdot x_E^i$$

es isomorfismo. En particular, si X es regular y separado, entonces $K(\mathbb{P}(E))$ es un $K(X)$-módulo libre de base $1, x_E, x_E^2, \ldots, x_E^n$.

Demostración. En primer lugar obsérvese que $\pi^!$ es inyectivo, pues $\pi_! \circ \pi^! = \mathrm{Id}$. Por tanto, seguiremos denotando por $K_\cdot(X)$ a la imagen de $\pi^!$.

Veamos que son linealmente independientes. Sea t la clase de $\mathscr{O}_{\mathbb{P}(E)}(-1)$ en $K^\cdot(\mathbb{P}(E))$. Como $x_E = 1-t$, basta ver que $1, t, \ldots, t^n$ son independientes. Si $a_0 + a_1 \cdot t + \cdots + a_n \cdot t^n = 0$ (con $a_i \in K_\cdot(X)$), aplicando $\pi_!$ se obtiene que $a_0 = 0$. Multiplicando $a_1 \cdot t + \cdots + a_n \cdot t^n = 0$ por t^{-1} y aplicando $\pi_!$ se obtiene que $a_1 = 0$. Así sucesivamente se concluye.

Veamos ahora que son generadores. Sea $U \subseteq X$ un abierto donde E es trivial e Y el cerrado complementario. Por Gysin e inducción noetheriana se reduce a probar el teorema en U, es decir, podemos suponer que E es trivial, en cuyo caso $\mathbb{P}(E) = X \times \mathbb{P}^n$ y x_E es la clase de cualquier hiperplano $X \times \mathbb{P}^{n-1}$. Ahora se procede por inducción sobre n, siendo el caso $n = 0$ trivial. El cerrado $X \times \mathbb{P}^{n-1} \overset{j}{\hookrightarrow} X \times \mathbb{P}^n$ tiene por abierto complementario el fibrado afín trivial $X \times \mathbb{A}^n$. Por Gysin se tiene la sucesión exacta

$$K_\cdot(X \times \mathbb{P}^{n-1}) \xrightarrow{j_!} K_\cdot(X \times \mathbb{P}^n) \to K_\cdot(X \times \mathbb{A}^n) \to 0$$

Si $\bar{x}$ es el elemento de $K^\cdot(X \times \mathbb{P}^{n-1})$ definido como $\bar{x} := 1 - \mathscr{O}_{X \times \mathbb{P}^{n-1}}(-1) = j^! x_E$, se verifica que $j_!(\bar{x}^i) = x_E^{i+1}$, por la fórmula de proyección. Por inducción, $K_\cdot(X \times \mathbb{P}^{n-1})$ está generado por $1, \bar{x}, \ldots, \bar{x}^{n-1}$, luego la imagen de $j_!$ está generada por $x_E, \ldots, x_E^n$. Por otro lado, $K_\cdot(X \times \mathbb{A}^n)$ está generado por 1 (teorema 17.2.17). Por la sucesión exacta concluimos. □

25. Corolario: *Se tiene el isomorfismo de anillos $K(\mathbb{P}^n_k) = \mathbb{Z}[x]/(x^{n+1})$, donde x es la clase de un hiperplano (cualquiera).*

Demostración. Solo hay que ver que $x^{n+1} = 0$, lo cual se deduce de que pueden encontrarse $n+1$ hiperplanos cuya intersección sea vacía. □

Igualmente, se tiene el siguiente corolario.

26. Corolario: $K_\cdot(X \times \mathbb{P}^n) = K_\cdot(X)[x]/(x^{n+1})$.

27. Corolario: *Sea $\pi : E \to X$ un fibrado afín. El morfismo*

$$\pi^! : K_\cdot(X) \to K_\cdot(E)$$

es isomorfismo.

Demostración. E es el complementario de un hiperplano de un espacio proyectivo: Sea F el $\mathscr{O}_X$-módulo localmente libre de las funciones afines de E (si V es el fibrado vectorial que opera sobre E, entonces $F(U) := \{f : \pi^{-1}(U) \to \mathbb{A}^1 : f(e+v) = f(e), \text{ para todo } e, v\}$). Tenemos un morfismo $E \to F^*$, $e(f) := f(e)$ y el hiperplano H formado por aquellas $w \in$

F^* que sobre las funciones afines constantes son nulas. Entonces, $\mathbb{P}(F^*) = E \coprod \mathbb{P}(H)$, denotemos $i : \mathbb{P}(H) \hookrightarrow \mathbb{P}(F^*)$ la inclusión obvia. De la sucesión exacta de Gysin

$$K_\cdot(\mathbb{P}(H)) \to K_\cdot(\mathbb{P}(F)) \to K_\cdot(E) \to 0$$

y por el teorema de periocidad $K_\cdot(\mathbb{P}(F)) = \oplus_{i=0}^{n} K_\cdot(X) \cdot x_{F^*}^i$ y $i_!(K_\cdot(\mathbb{P}(F))) = \oplus_{i=1}^{n} K_\cdot(X) \cdot x_{F^*}^i$. Por tanto, $K_\cdot(E) = K_p oint(X)$.

□

17.3. Graduado de la teoría K

Aunque la teoría K de variedades regulares tiene muchas propiedades típicas de una teoría de la intersección, es difícil construir una tal teoría sobre ella, fundamentalmente porque el anillo $K(X)$ no está graduado, y porque, como hemos dicho en la introducción, los anillos locales de dos subvariedades racionalmente equivalentes no tienen por qué ser iguales en teoría K. Es decir, el anillo $K(X)$ es demasiado fino.

Para solventar estas dificultades, el grupo $K(X)$ se filtra mediante la codimensión del soporte de los haces coherentes, y el graduado, $GK(X)$, es el grupo en el que vamos a trabajar en este capítulo. Las operaciones suma, producto, imagen directa e inversa se construirán a partir de las de la teoría K, viendo que son compatibles con las filtraciones. El punto difícil es probar que el producto y la imagen inversa admirable son compatibles con las filtraciones. Para probar que si y es un ciclo de codimensión p e y' es un ciclo de codimensión p', entonces $y \cdot y'$ es suma de ciclos de codimensión mayor o igual que $p + p'$, observaremos que puede suponerse que uno de los ciclos es regular, porque cortar dos ciclos es lo mismo que cortar su producto directo con la diagonal. A continuación, probaremos que dado un esquema X y un subesquema Y, existe una deformación de X al cono normal de X a lo largo de Y, $C_Y X$, de modo que Y se deforma a la sección cero de $C_Y X$. Reduciremos el problema al corte, en un fibrado, de la sección cero con un ciclo y concluiremos fácilmente. Así, $GK(X)$ tendrá estructura de anillo (cuando X sea liso).

Los esquemas considerados serán siempre variedades algebraicas.

1. Definición: Sea X irreducible de dimensión n. Sea $K_d(X)$ el subgrupo de $K_\cdot(X)$ engendrado por los haces coherentes cuyo soporte es unión de cerrados irreducibles de codimensión mayor o igual que d. Se obtiene una filtración de $K_\cdot(X)$

$$0 = K_{n+1}(X) \subseteq K_n(X) \subseteq K_{n-1}(X) \subseteq \cdots \subseteq K_0(X) = K(X)$$

cuyo graduado asociado se denota $GK(X)$,

$$GK(X) = \underset{d\geq 0}{\oplus} G_d K(X) = \underset{d\geq 0}{\oplus} K_d(X)/K_{d+1}(X)$$

2. Definición: Denotaremos $Z_p(X)$ el subgrupo libre de $Z_\cdot(X)$ generado por los subesquemas cerrados e íntegros de codimensión p y lo denominaremos p-ciclos de X.

3. Observación: El morfismo $Z_p(X) \to K_p(X)/K_{p+1}(X)$, $[Z] \mapsto \overline{[Z]}$ es epiyectivo. Para ello, véase la demostración del teorema 17.2.6.

4. Teorema: *Si $\mathscr{M}$ es un haz coherente sobre X cuyo soporte es unión de cerrados irreducibles de codimensión mayor o igual que d, entonces la clase de $\mathscr{M}$ en $K_d(X)/K_{d+1}(X)$ coincide con la clase de*

$$\sum_{\operatorname{codim} x = d} l_{\mathscr{O}_{X,x}}(\mathscr{M}_x) \cdot \mathscr{O}_X/\mathfrak{p}_x$$

Demostración. Como el sumatorio anterior es aditivo para las sucesiones exactas de módulos coherentes de codimensión mayor o igual que d y nulo sobre $K_{d+1}(X)$, basta demostrar la fórmula en el caso $\mathscr{M} = \mathscr{O}_X/\mathfrak{p}_x$, donde es trivial.

□

5. Proposición: *Sea X una variedad irreducible regular separada e Y, Y' subvariedades irreducibles de codimensión p y q respectivamente. Si Y e Y' se cortan en ciclos de codimensión $p+q$, entonces*

$$Y \cdot Y' = \sum_{\operatorname{codim} x = p+q} \sum_{i \geq 0} (-1)^i l_{\mathscr{O}_{X,x}} \left(\underline{\operatorname{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{Y'})_x \right) \cdot \bar{x} \text{ módulo } K_{p+q+1}$$

Demostración. $Y \cdot Y' = \sum_{i \geq 0} (-1)^i \underline{\operatorname{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{Y'})$. Concluimos al aplicar el teorema anterior a los haces $\underline{\operatorname{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{Y'})$, que están concentrados en codimensión mayor o igual que $p+q$. □

6. Proposición: *Sea $f : X \to Y$ un morfismo propio entre variedades algebraicas irreducibles y sea $d = \dim Y - \dim X$. Si Z es una subvariedad irreducible de X de codimensión p, se verifica*

$$f_!(Z) = f_*(Z) \text{ módulo } K_{p+d+1}$$

donde

$$f_*(Z) = \begin{cases} 0, & si\ \dim f(Z) < Z \\ [Z : f(Z)] \cdot f(Z), & si\ \dim f(Z) = Z \end{cases}$$

siendo $[Z : f(Z)]$ el grado de Z sobre $f(Z)$, es decir, el grado entre sus cuerpos de funciones. Por tanto, $f_!$ es compatible con las filtraciones e induce un morfismo homogéneo de grado d

$$f_* : GK(X) \to GK(Y)$$

Demostración. Distingamos los dos casos:

1. $\dim f(Z) < \dim Z$. En este caso, las imágenes directas superiores $R^i f_* \mathcal{O}_Z$ están concentradas en $f(Z)$ para $i \geq 0$, que es de codimensión mayor o igual que $p+d+1$ en Y, luego $f_!(Z) = 0$ módulo K_{p+d+1}.

2. $\dim f(Z) = \dim Z$. El morfismo $f : Z \to f(Z)$ es, en el punto genérico de $f(Z)$, un morfismo finito de grado $n = [Z : f(Z)]$. Por el teorema de cambio de base 13.4.6, los haces $R^i f_*(\mathcal{O}_Z)$ tienen fibra nula en el punto genérico de $f(Z)$ para $i > 0$, y $f_* \mathcal{O}_Z$ es de longitud n en dicho punto genérico. Se concluye. □

7. Definición: Si $i : Y \hookrightarrow X$ es una inmersión cerrada de codimensión d, el elemento $i_*(1) \in G_d K(X)$ se denomina clase de cohomología de Y en X y se denota por Y.

8. Proposición: *Si $f : X \to Y$ es un morfismo plano, entonces $f^! : K_\cdot(Y) \to K_\cdot(X)$ es compatible con las filtraciones y define un morfismo homogéneo de grado cero*

$$f^* : GK(Y) \to GK(X)$$

Demostración. Por ser f plano, cumple el teorema de de descenso de los iedales (ver 3.3.40). Luego, si Z es un subesquema cerrado de Y de codimensión mayor o igual que d, entonces $f^{-1}(Z)$ es un subesquema cerrado de X de codimensión $\geq d$. Se concluye. □

9. Proposición: *Para todo diagrama cartesiano*

$$\begin{array}{ccc} \overline{X} & \xrightarrow{\overline{f}} & X \\ {\scriptstyle \overline{\pi}}\downarrow & & \downarrow{\scriptstyle \pi} \\ \overline{Y} & \xrightarrow{f} & Y \end{array}$$

con f plano y π propio, se verifica: $f^*(\pi_*(a)) = \overline{\pi}_*(\overline{f}^*(a))$, para todo $a \in GK(X)$.

Demostración. Se deduce de la fórmula análoga en teoría K (prop. 17.2.15). □

10. Teorema (Gysin): *Sea $Y \overset{j}{\hookrightarrow} X$ un cerrado irreducible de codimensión d y sea $U \overset{i}{\hookrightarrow} X$ el abierto complementario. Se verifica una sucesión exacta*

$$GK(Y) \xrightarrow{j_*} GK(X) \xrightarrow{i^*} GK(U) \to 0$$

Demostración. Denotemos $K_\cdot^Y(X)$ el grupo K de los $\mathcal{O}_X$-módulos coherentes concentrados en Y, y también lo filtramos por la codimensión del soporte: $K_p^Y(X)$ es el subgrupo generado por los $\mathcal{O}_X$-módulos coherentes concentrados en Y y cuyo soporte es de codimensión $\geq p$ (en X).

Si $\mathscr{M}$ es un módulo coherente en U cuyo soporte es de codimensión $\geq p$, se puede extender a un módulo coherente en X con soporte de codimensión $\geq p$. En efecto, basta ver que extiende a un módulo coherente con soporte en el cierre en X de $\mathrm{Sop}\mathscr{M}$, Z. Sea $U' = U \cup (X \setminus Z)$ y $\mathscr{M}'$ el módulo coherente en U' que coincide con $\mathscr{M}$ en U y es nulo en $X \setminus Z$. Extendiendo $\mathscr{M}'$ a X se concluye.

Además, si $\mathscr{M}_1, \mathscr{M}_2$ son dos extensiones de $\mathscr{M}$ en las condiciones anteriores, difieren en una suma de módulos concentrados en Y cuyo soporte es de codimensión $\geq p$. Razonando como en 17.2.16 se concluye que el núcleo del epimorfismo $K_p(X) \to K_p(U)$ es $K_p^Y(X)$.

Por otro lado, el morfismo $j_! : K_{p-d}(Y) \to K_p^Y(X)$ es claramente epiyectivo (se prueba igual que en 17.2.16). Por tanto, se tiene la sucesión exacta

$$K_{p-d}(Y) \to K_p(X) \to K_p(U) \to 0$$

y se concluye. □

17.3.1. Graduado K de un fibrado proyectivo

El objetivo de esta subsección es dar el teorema de periodicidad para el graduado K y construir la imagen inversa para una inmersión regular. A partir de ella se podrá probar que, cuando X es lisa, el producto de $K(X)$ es compatible con la filtración y por tanto dota a $GK(X)$ de estructura de anillo.

Intersección con divisores.

11. Proposición: *Sea $\mathscr{L}$ haz de línea en X y denotemos $\delta(\mathscr{L}) = 1 - \mathscr{L}$. Se verifica:*

(a) $\delta(\mathscr{L})$ pertenece a $K_1(X)$.

(b) Si $a \in K_d(X)$, entonces $a \cdot \delta(\mathscr{L})$ pertenece a $K_{d+1}(X)$. Por tanto se tiene un morfismo homogéneo de grado 1

$$\begin{aligned} GK(X) &\xrightarrow{\cdot\delta(\mathscr{L}))} GK(X) \\ a &\mapsto a \cdot \delta(\mathscr{L}) \end{aligned}$$

(c) Fórmula de proyección: Para todo morfismo propio $f : X' \to X$ se verifica

$$f_*(a \cdot \delta(f^*\mathscr{L})) = f_*(a) \cdot \delta(\mathscr{L})$$

para todo $a \in GK(X')$.

(d) Si $f: X' \to X$ es un morfismo plano, entonces

$$f^*(a \cdot \delta(\mathscr{L})) = f^*(a) \cdot \delta(f^*\mathscr{L}),$$

para todo $a \in GK(X)$.

Demostración. (a) y (b) Si un módulo $\mathscr{M} \in K_p(X)$, entonces $\mathscr{M}$ y $\mathscr{M} \otimes \mathscr{L}$ coinciden en $K_p(X)/K_{p+1}(X)$ porque tienen las mismas longitudes en los puntos genéricos de su soporte.

(c) se deduce de la fórmula de proyección en teoría K. (d) es inmediata.

□

12. Definición: Sea $\mathscr{L}$ es un haz de línea sobre X. Seguiremos denotando $\delta(\mathscr{L})$ a la clase de $1-\mathscr{L}$ en $G_1K(X) = K_1(X)/K_2(X)$, y se denomina clase de obstrucción de $\mathscr{L}$.

13. Teorema: *δ: $\mathrm{Pic}(X) \to G_1K(X)$, $\mathscr{L} \mapsto \delta(\mathscr{L})$, es un morfismo de grupos, funtorial para las respectivas imágenes inversas (cuando existan).*

Demostración. La funtorialidad se debe a la igualdad $f^!\delta(\mathscr{L}) = f^!(1-\mathscr{L}) = 1 - f^*\mathscr{L} = \delta(f^*\mathscr{L})$, para todo morfismo $f: X' \to X$. Veamos que δ es un morfismo de grupos: Sean $\mathscr{L}$ y $\mathscr{L}'$ haces de línea sobre X. Hay que probar que $1 - \mathscr{L} \otimes \mathscr{L}' = (1-\mathscr{L}) + (1-\mathscr{L}')$ módulo $K_2(X)$. Efectivamente,

$$1 - \mathscr{L} \otimes \mathscr{L}' - (1-\mathscr{L}) - (1-\mathscr{L}') = \mathscr{L} + \mathscr{L}' - \mathscr{L} \otimes \mathscr{L}' - 1 = -(1-\mathscr{L}) \cdot (1-\mathscr{L}') \in K_2(X)$$

□

14. Proposición: *Si $D \overset{i}{\hookrightarrow} X$ es un divisor efectivo de Cartier, entonces $i^!: K_\cdot(X) \to K_\cdot(D)$ es compatible con la filtración, es decir, $i^!(K_p(X)) \subseteq K_p(D)$, y por tanto induce un morfismo homogéneo de grado cero*

$$i^*: GK(X) \to GK(D)$$

y se verifica $i_* i^*(a) = a \cdot D$ para todo $a \in GK(X)$, donde $D = 1 - \mathscr{L}_{-D}$.

Demostración. Basta ver que si Y es un subesquema cerrado e íntegro de codimensión $\geq p$ de X, entonces $i^!(\mathscr{O}_Y)$ pertenece a $K_p(D)$. Por definición $i^!(\mathscr{O}_Y) = \underline{\mathrm{Tor}}_0^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_D) - \underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_D)$. Si Y no está contenido en D, entonces $i^!(\mathscr{O}_Y) = \mathscr{O}_{Y \cap D}$ y se concluye. Si Y está contenido en D, denotemos $\mathscr{L} = \mathscr{L}_{-D}$. De la sucesión exacta

$$0 \to \mathscr{L} \to \mathscr{O}_X \to \mathscr{O}_D \to 0$$

se deduce que $\underline{\mathrm{Tor}}_0^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_D) = \mathscr{O}_Y$ y $\underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_D) = \mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{O}_Y$. Por tanto

$$i^!(\mathscr{O}_Y) = j_!\delta(\mathscr{L}_{|Y})$$

siendo j la inclusión de Y en D. Como $\delta(\mathscr{L}_{|Y})$ pertenece a $K_1(Y)$ e Y tiene codimensión $p-1$ en D, se concluye. La última parte es consecuencia de la fórmula de proyección en teoría K. □

15. Teorema de periodicidad para GK**:** *Sea* $\mathbb{P}(E) \xrightarrow{\pi} X$ *un fibrado proyectivo de rango* n *(es decir,* E *es localmente libre de rango* $n+1$*). Denotemos* $x = \delta(\mathscr{O}_{\mathbb{P}(E)}(-1))$*. Entonces* $1, x, \ldots, x^n$ *forman una base de* $GK(\mathbb{P}(E))$ *sobre* $GK(X)$*. Es decir, el morfismo*

$$\begin{aligned} GK(X) \oplus \overset{n+1}{\cdots} \oplus GK(X) &\longrightarrow GK(\mathbb{P}(E)) \\ (a_0, \ldots, a_n) &\longmapsto \sum_{i=0}^{n} \pi^*(a_i) \cdot x^i \end{aligned}$$

es isomorfismo.

Demostración. Se verifica la igualdad (que probaremos después)

$$\pi_*(\pi^*(a) \cdot x^i) = \begin{cases} 0, \text{ para } 0 \leq i < n \\ a, \text{ para } i = n \end{cases}$$

De aquí se deduce que $1, x, \ldots, x^n$ son linealmente independientes: Si existiese una relación $0 = \sum_{i=0}^{n} \pi^*(a_i) \cdot x^i$, aplicando π_* se tiene, por la igualdad anterior, que $a_n = 0$. Multiplicando por x y aplicando π_*, se tiene que $a_{n-1} = 0$. Así sucesivamente, se concluye.

El teorema de periodicidad 17.2.24 implica que $1, x, \ldots, x^n$ son un sistema de generadores de $GK(\mathbb{P}(E))$. En efecto, sea $\mathscr{M}$ un módulo coherente en $\mathbb{P}(E)$ cuyo soporte es de codimensión d y cuya clase en $G_d K(\mathbb{P}(E))$ es no nula. Escribamos $\mathscr{M} = \sum_{i=0}^{n} \pi^!(a_i) x^i$. Sean n_i tales que $0 \neq a_i \in G_{n_i} K(X)$. Sea $d' = \text{ínf}\{n_i - i\}$. Si $d' < d$, entonces la clase de $\mathscr{M}$ en $G_{d'} K(\mathbb{P}(E))$ es no nula, lo cual no es posible porque $\mathscr{M} \in K_d(\mathbb{P}(E))$. Por tanto, $d' \geq d$ y $\mathscr{M} = \sum_i \pi^*(a_i) x^i$, con $a_i \in G_{d-i} K(X)$.

Finalmente, probemos que $\pi_*(\pi^*(a) \cdot x^i)$ es nulo para $i < n$ y es a para $i = n$. Supongamos que a es de grado d. Entonces $\pi_*(\pi^*(a) \cdot x^i)$ es la clase de $\pi_!(\pi^!(a) \cdot x^i)$ módulo $K_{d+i-n+1}(X)$. Teniendo en cuenta que $\pi_!(x^i) = 1$ para todo $0 \leq i \leq n$, se concluye que $\pi_!(\pi^!(a) \cdot x^i) = a$, que es nulo módulo $K_{d+i-n+1}(X)$ para $i < n$.

□

16. Corolario: $GK(\mathbb{P}^n_k) = \mathbb{Z}[x]/(x^{n+1})$*, siendo* x *de grado* 1.

17. Corolario: $GK(X \times_k \mathbb{P}^n_k) = GK(X) \otimes_{\mathbb{Z}} GK(\mathbb{P}^n_k)$.

18. Corolario: *Sea $\pi: E \to X$ localmente (sobre X) isomorfo a $X \times \mathbb{A}^n$. Entonces,*

$$\pi^*: GK(X) \to GK(E)$$

es un epimorfismo.

Demostración. Recordemos que $\pi^!: K_\cdot(X) \to K_\cdot(E)$ es epimorfismo y compatible con la filtración. Por inducción noetheriana y Gysin, se reduce al caso en que E es trivial, $E = X \times \mathbb{A}^n$. Considerando $X \times \mathbb{A}^n$ como abierto de $X \times \mathbb{P}^n$ de cerrado complementario $X \times \mathbb{P}^{n-1}$, se tiene, por Gysin y el teorema de periodicidad, la sucesión exacta

$$GK(X)[\bar{x}]/(\bar{x}^n)) \xrightarrow{i_*} GK(X)[x]/(x^{n+1}) \to GK(X \times \mathbb{A}^n) \to 0$$

Se verifica que $i^*(x) = \bar{x}$, luego por la fórmula de proyección $i_*(\bar{x}^i) = x^{i+1}$. En conclusión, la imagen de i_* son los múltiplos de x. Se concluye. □

19. Corolario: *Sea $E \xrightarrow{\pi} X$ localmente trivial y $X \xhookrightarrow{s} E$ una sección, entonces $s^!(K_p(E)) = K_p(X)$, luego induce un isomorfismo de grado cero*

$$s^*: GK(E) \to GK(X)$$

que es inverso de π^*.

Demostración. Por el corolario anterior, el morfismo $\pi^!: K_p(X) \to K_p(E)$ es epimorfismo. Como $s^!$ es inverso de $\pi^!$ se concluye. □

17.3.2. Deformación al cono normal

Sea $Y \hookrightarrow X$ un subesquema cerrado definido por un ideal $\mathfrak{p}$. Sea $C = \operatorname{Spec} \bigoplus_{n\geq 0} \mathfrak{p}^n/\mathfrak{p}^{n+1}$ el cono normal de Y sobre X. El propósito de esta sección es deformar la inmersión $Y \hookrightarrow X$ a la sección cero $Y \hookrightarrow C$.

Cierre proyectivo de un cono.

Vamos a realizar aquí, en su generalidad necesaria, la operación geométrica básica en Geometría Proyectiva de sumergir un espacio vectorial como la zona afín de un espacio proyectivo, cuyo complementario es el hiperplano del infinito.

20. Definición: Sea X un esquema y $\mathscr{B} = \oplus_{n\in\mathbb{N}} \mathscr{B}_n$ una $\mathscr{O}_X$-álgebra graduada cuasicoherente generada por los elementos de grado 1 (es decir, los morfismos naturales $\mathscr{B}_1^{\otimes n} \to \mathscr{B}_n$ son epimorfismos). Diremos que $C = \operatorname{Spec} \mathscr{B}$ es un cono sobre X. Denotaremos $\mathbb{P}(C) = \operatorname{Proj} \mathscr{B}$.

21. Ejemplos: 1. Si $Y \hookrightarrow X$ es un cerrado definido por un ideal $\mathfrak{p}$, el cono normal de Y sobre X es el cono sobre Y definido por la $\mathscr{O}_Y$-álgebra graduada $\mathscr{B} = \bigoplus_{n\geq 0} \mathfrak{p}^n/\mathfrak{p}^{n+1}$ y se denota $C_Y X$.

2. Si E es un $\mathscr{O}_X$-módulo localmente libre de rango n, entonces el fibrado vectorial asociado es el cono asociado al álgebra $\mathscr{B} = S^{\cdot} E^*$.

22. Definición: Sea $C \to X$ el cono asociado a un álgebra $\mathscr{B}$. Denotaremos $C \oplus 1$ al cono definido por la $\mathscr{O}_X$-álgebra $\mathscr{B}[t] = \mathscr{B} \otimes_{\mathscr{O}_X} \mathscr{O}_X[t]$. Llamaremos cierre proyectivo de C a $\mathbb{P}(C \oplus 1) = \operatorname{Proj} \mathscr{B}[t]$.

Si $C = E$ es un fibrado vectorial, entonces $C \oplus 1$ es el fibrado vectorial asociado al módulo $E \oplus \mathscr{O}_X$. La justificación del nombre de cierre proyectivo viene dada por la siguiente proposición.

23. Proposición: *Sea $C \to X$ un cono. Se tiene una inmersión cerrada $i\colon \mathbb{P}(C) \hookrightarrow \mathbb{P}(C \oplus 1)$ cuyo abierto complementario es isomorfo a C. Además:*

1) La restricción de $\mathscr{O}_{\mathbb{P}(C\oplus 1)}(1)$ a $\mathbb{P}(C)$ es $\mathscr{O}_{\mathbb{P}(C)}(1)$.

2) La restricción de $\mathscr{O}_{\mathbb{P}(C\oplus 1)}(1)$ a C es $\mathscr{O}_C$.

Demostración. El epimorfismo de álgebras graduadas $\mathscr{B}[t] \to \mathscr{B}$, $t \mapsto 0$, define la inmersión cerrada $i\colon \mathbb{P}(C) \hookrightarrow \mathbb{P}(C \oplus 1)$, cuya imagen son los ceros homogéneos de t. El abierto complementario es el espectro del álgebra de localización homogénea por t

$$[\mathscr{B}[t]_t]_0 = \left\{ \frac{b_p t^n}{t^{n+p}}, \text{ con } b_p \in \mathscr{B}^p \right\}$$

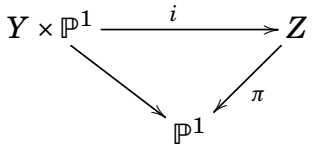
que es claramente isomorfa a $\mathscr{B}$. El resto es trivial.

□

24. Definición: Se dice que $\mathbb{P}(C)$ es el hiperplano del infinito de $\mathbb{P}(C \oplus 1)$ y que C es la parte afín.

El enunciado preciso de la deformación de una inmersión cerrada a la sección cero de su cono normal es el siguiente:

25. Deformación al cono normal: *Sea $Y \hookrightarrow X$ un subesquema cerrado definido por un ideal $\mathfrak{p}$ y $C = \operatorname{Spec} \bigoplus_{n\geq 0} \mathfrak{p}^n/\mathfrak{p}^{n+1}$ el cono normal de Y sobre X. Existe un esquema Z y un diagrama conmutativo*



donde i es una inmersión cerrada, π es plano, y se verifica

(a) $\pi^{-1}(\mathbb{P}^1 \setminus \infty) = X \times \mathbb{A}^1$ y la inmersión $Y \times \mathbb{A}^1 \xrightarrow{i} X \times \mathbb{A}^1$ es la inducida por $Y \hookrightarrow X$.

(b) $\pi^{-1}(\infty) = C_{Y/X}$ *y la inmersión* $i_{\infty *} : Y = Y \times \infty \hookrightarrow C_{Y/X}$ *es la sección cero.*

Demostración. Sea $\widetilde{Z}$ la explosión de $X \times \mathbb{P}^1$ a lo largo de $Y \times \infty$ y $\widetilde{\pi} : \widetilde{Z} \to \mathbb{P}^1$ el morfismo natural. Se verifica

$$\widetilde{\pi}^{-1}(\mathbb{P}^1 \backslash \infty) = X \times \mathbb{A}^1$$

pues $\widetilde{Z} \to X \times \mathbb{P}^1$ es isomorfismo sobre el complementario de $Y \times \infty$, luego sobre $X \times (\mathbb{P}^1 - \infty)$.

Dado un ideal I sobre un esquema X denotaremos $\mathscr{O}_X[\tilde{I}]$ a la dilatación de $\mathscr{O}_X$ por I, es decir, $\mathscr{O}_X[\tilde{I}] = \mathscr{O}_X \oplus I \oplus I^2 \oplus \cdots$. Denotaremos (t) el ideal de ∞ en $\mathbb{P}^1$.

Sea $\widetilde{X}$ la explosión de X a lo largo de Y. Las inmersiones cerradas $Y \times \mathbb{P}^1 \hookrightarrow X \times \mathbb{P}^1 \hookleftarrow X \times \infty = X$ inducen epimorfismos graduados $\mathscr{O}_{Y \times \mathbb{P}^1}[\widetilde{(t)}] \leftarrow \mathscr{O}_{X \times \mathbb{P}^1}[\widetilde{\mathfrak{p} + (t)}] \to \mathscr{O}_X[\tilde{\mathfrak{p}}]$ y, tomando Proj, inmersiones cerradas $Y \times \mathbb{P}^1 \hookrightarrow \widetilde{Z} \hookleftarrow \widetilde{X}$ cuya intersección es vacía, pues la suma de sus ideales homogéneos contiene al ideal irrelevante de $\mathscr{O}_{X \times \mathbb{P}^1}[\widetilde{\mathfrak{p} + (t)}]$.

Veamos que $\widetilde{\pi}^{-1}(\infty) = \mathbb{P}(C_{Y/X} \oplus 1) \cup \widetilde{X}$. Es fácil ver que $\mathscr{O}_{X \times \mathbb{P}^1}[\widetilde{\mathfrak{p} + (t)}]/(t) = (\mathscr{O}_X[\tilde{\mathfrak{p}}] \underset{\mathscr{O}_X}{\otimes} \mathscr{O}_X[t])/(\mathfrak{p}t)$. Entonces

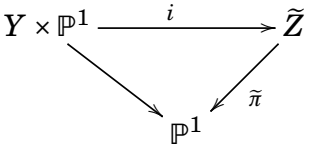
$$\begin{aligned}
\widetilde{\pi}^{-1}(\infty) &= \operatorname{Proj} \mathscr{O}_{X \times \mathbb{P}^1}[\widetilde{\mathfrak{p} + (t)}]/(t) = \operatorname{Proj}(\mathscr{O}_X[\tilde{\mathfrak{p}}] \underset{\mathscr{O}_X}{\otimes} \mathscr{O}_X[t])/(\mathfrak{p}t) \\
&= \operatorname{Proj}[(\mathscr{O}_X[\tilde{\mathfrak{p}}] \underset{\mathscr{O}_X}{\otimes} \mathscr{O}_X[t])/\mathfrak{p}] \quad \cup \quad \operatorname{Proj}[(\mathscr{O}_X[\tilde{\mathfrak{p}}] \underset{\mathscr{O}_X}{\otimes} \mathscr{O}_X[t])/(t)] \\
&= \operatorname{Proj}(\underset{n \geq 0}{\oplus} \mathfrak{p}^n/\mathfrak{p}^{n+1}) \underset{\mathscr{O}_Y}{\otimes} \mathscr{O}_Y[t] \quad \cup \quad \operatorname{Proj} \mathscr{O}_X[\tilde{\mathfrak{p}}] \\
&= \mathbb{P}(C_{Y/X} \oplus 1) \cup \widetilde{X}
\end{aligned}$$

Además, $\widetilde{X} \cap \mathbb{P}(C_{Y/X} \oplus 1) = \mathbb{P}(C_{Y/X})$, luego $\mathbb{P}(C_{Y/X} \oplus 1) \backslash (\widetilde{X} \cap \mathbb{P}(C_{Y/X} \oplus 1)) = C_{Y/X}$.

Sea $Z = \widetilde{Z} \backslash \widetilde{X}$. Como $Y \times \mathbb{P}^1$ no corta a $\widetilde{X}$ se tiene una inmersión cerrada $Y \times \mathbb{P}^1 \hookrightarrow Z$, que verifica todas las condiciones requeridas por lo dicho anteriormente.

□

26. Observación: En la demostración del teorema se ha probado que se tiene un triángulo conmutativo



donde i es una inmersión cerrada, $\widetilde{\pi}$ es propio y plano, y se verifica

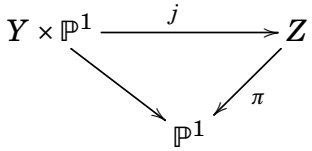
(a) $\widetilde{\pi}^{-1}(\mathbb{P}^1 \backslash \infty) = X \times \mathbb{A}^1$ y la inmersión $Y \times \mathbb{A}^1 \xrightarrow{i} X \times \mathbb{A}^1$ es la inducida por $Y \hookrightarrow X$.

(b) $\tilde{\pi}^{-1}(\infty) = \mathbb{P}(C \oplus 1) \cup \tilde{X}$ y la inmersión $i_\infty : Y \hookrightarrow \mathbb{P}(C \oplus 1)$ es la sección cero (es decir, la composición de la sección cero $Y \hookrightarrow C$ y la inmersión abierta $C \hookrightarrow \mathbb{P}(C \oplus 1)$).

27. Teorema: *Si $i: Y \hookrightarrow X$ es una inmersión cerrada regular, entonces el morfismo $i^!: K_.(X) \to K_.(Y)$ es compatible con la filtración, es decir, $i^!(K_p(X)) \subseteq K_p(Y)$. Por tanto, induce un morfismo homogéneo de grado cero*

$$i^*: GK(X) \to GK(Y)$$

Demostración. Sea



la deformación de la inmersión $Y \hookrightarrow X$ a la sección cero $Y \hookrightarrow C_{Y/X}$ dada por el teorema anterior. Para cada punto cerrado t de $\mathbb{P}^1$, sea $j_t: Y \hookrightarrow Z$ la inmersión cerrada regular definida por $j_t(y) = j(y,t)$. Para $t = 0$, el morfismo j_0 es la composición del morfismo $Y \hookrightarrow X$, la sección nula $X \hookrightarrow X \times \mathbb{A}^1$ y la inmersión abierta $X \times \mathbb{A}^1 \hookrightarrow Z$. El morfismo inducido $K_p(Z) \to K_p(X \times \mathbb{A}^1)$ es epiyectivo y el morfismo $K_p(X \times \mathbb{A}^1) \to K_p(X)$ es isomorfismo, luego basta probar el teorema para $j_0^!$. Pero $j_0^!$ coincide con $j_\infty^!$ (más adelante lo veremos), y j_∞ es la composición de la sección nula $Y \hookrightarrow C_{Y/X}$ y la inmersión cerrada $C_{Y/X} \hookrightarrow Z$, que es un divisor. Para ambos morfismos se verifica el teorema (por 17.3.19 y 17.3.14) luego se concluye.

Para terminar, veamos que el morfismo $j_t^!: K_.(Z) \to K_.(Y)$ es independiente de t. Dado que j_t es la composición de $\lambda_t: Y \hookrightarrow Y \times \mathbb{P}^1$, $y \mapsto (y,t)$, con $Y \times \mathbb{P}^1 \xhookrightarrow{j} Z$, basta ver que $\lambda_t^!: K_.(Y \times \mathbb{P}^1) \to K_.(Y)$ no depende de t. Pero $K_.(Y \times \mathbb{P}^1) = K_.(Y) \otimes \mathbb{Z}[x]/(x^2)$, donde x es la clase de un punto cerrado cualquiera de $\mathbb{P}^1$, y el morfismo $\lambda_t^!: K_.(Y) \otimes \mathbb{Z}[x]/(x^2) \to K_.(Y)$ es mandar x al cero.

□

28. Teorema: *Si X es una k-variedad lisa, el producto de $K(X)$ es compatible con la filtración. Por tanto, induce un producto en $GK(X)$, que lo dota de estructura de anillo.*

Si $f: X \to Y$ es un morfismo entre variedades lisas, el morfismo inducido $f^!: K(Y) \to K(X)$ es compatible con la filtración e induce un morfismo de anillos, homogéneo de grado cero

$$f^*: GK(Y) \to GK(X)$$

Demostración. Tenemos que probar que si Y e Y' son subvariedades íntegras de codimensión d y d', entonces $Y \cdot Y'$ pertenece a $K_{d+d'}(X)$. Ahora bien, por 17.2.22, $Y \cdot Y' = \delta^!(Y \times Y')$, siendo $\delta: X \hookrightarrow X \times X$ la inmersión diagonal. Ahora, $Y \times Y'$ es una subvariedad de codimensión $d + d'$ de $X \times X$ y δ es una inmersión regular, por ser X lisa. Se concluye por el teorema anterior.

Para la segunda parte, el morfismo $f: X \to Y$ es la composición de la gráfica de f, $\Gamma_f: X \to X \times Y$, con la proyección $\pi: X \times Y \to Y$. Tanto $\Gamma_f^!$ como $\pi^!$ son morfismos de anillos compatibles con la filtración (el primero es una inmersión regular y el segundo es plano), luego su composición también. □

29. Corolario: *Si Y e Y' son subvariedades cerradas de X tales que* $\operatorname{codim} Y + \operatorname{codim} Y' > \dim X$*, entonces $Y \cdot Y' = 0$ en teoría K.*

30. Propiedades de $GK(X)$**:** *En la categoría de las k-variedades lisas el graduado de la teoría K verifica:*

1. *$GK(X)$ es un anillo graduado, conmutativo, con unidad, y nulo en grado mayor que la dimensión de X.*
2. *El graduado del grupo K de una unión disjunta es la suma directa del graduado asociado a cada componente de la unión disjunta.*
3. *f^* es un morfismo de anillos que conserva el grado.*
4. *$(f \circ g)^* = g^* \circ f^*$.*
5. *f_* es un morfismo de grupos; si X e Y son conexos, f_* aumenta el grado en* $\dim Y - \dim X$.
6. *Para todo $x \in GK(X)$, $y \in GK(Y)$ se verifica $f_*(x \cdot f^*(y)) = f_*(x) \cdot y$.*
7. *$(f \circ g)_* = f_* \circ g_*$.*

17.4. Clases de Chern

1. Definición: Sea E un haz localmente libre de rango n sobre X, $\pi: \mathbb{P}(E) \to X$ la proyección natural y x_E la clase de obstrucción de $\mathcal{O}_{\mathbb{P}(E)}(-1)$. Llamaremos clases de Chern de E a los coeficientes de la relación que satisfacen $1, x_E, \ldots, x_E^n$ en $GK(\mathbb{P}(E))$. Es decir

$$x_E^n + c_1(E) \cdot x_E^{n-1} + \cdots + c_{n-1}(E) \cdot x_E + c_n(E) = 0$$

con $c_i(E) \in G_iK(X)$, que se denomina i-ésima clase de Chern de E. Por convenio $c_0(E) = 1$.

Sea $\mathbb{P}(E \oplus 1)$ el cierre proyectivo de E y $s: X \hookrightarrow \mathbb{P}(E \oplus 1)$ la sección cero, es decir, el morfismo inducido tomando Proj en el epimorfismo $S^\cdot(E^* \oplus \mathcal{O}_X) \to S^\cdot \mathcal{O}_X$. De otro modo, s es la composición de la sección cero $X \hookrightarrow E$ y la inmersión abierta $E \hookrightarrow \mathbb{P}(E \oplus 1)$. Se verifica:

2. Teorema: *Si $\bar{x}$ es la clase de obstrucción de $\mathcal{O}_{\mathbb{P}(E\oplus 1)}(-1)$, entonces las clases de Chern de E son los coeficientes de la clase de cohomología de la sección cero $s\colon X \hookrightarrow \mathbb{P}(E\oplus 1)$ en la base $1,\bar{x},\dots,\bar{x}^n$. Es decir,*

$$s(X) = s_*(1) = \bar{x}^n + c_1(E)\cdot\bar{x}^{n-1} + \cdots + c_{n-1}(E)\cdot\bar{x} + c_n(E)$$

En particular, $s^*(s_*(1)) = s_0^*(s_{0*}(1)) = c_n(E)$, siendo $s_0\colon X \hookrightarrow E$ la sección cero.

Demostración. Por el teorema de periodicidad para $\mathbb{P}(E\oplus 1)$, $s_*(1)$ es combinación lineal de $1,\bar{x},\dots,\bar{x}^n$.

El coeficiente de $\bar{x}^n$ es 1, como se prueba restringiendo a un abierto que trivialice al fibrado, en cuyo caso $\mathbb{P}(E\oplus 1) = X\times\mathbb{P}^n$, $\bar{x}$ es la clase de un hiperplano $X\times\mathbb{P}^{n-1}$ y $s_*(1)$ es la clase de cohomología de un punto $X\times p \hookrightarrow X\times\mathbb{P}^n$.

Los demás coeficientes son las clases de Chern, porque la restricción de $s_*(1)$ al hiperplano del infinito es nula (ya que la sección cero está contenida en la parte afín) y porque la restricción de $\bar{x}$ al infinito es x_E.

Tomando s^* en la igualdad se obtiene $s^*(s_*(1)) = c_n(E)$, ya que $s^*\bar{x} = 0$ porque la imagen de s está contenida en la parte afín. La igualdad $s^*(s_*(1)) = s_0^*(s_{0*}(1))$ se deduce de la igualdad $s = i\circ s_0$, siendo i la inmersión abierta de la parte afín en $\mathbb{P}(E\oplus 1)$, ya que $i^*\circ s_* = s_{0*}$. □

3. Observación: El mismo teorema y demostración son válidos sustituyendo la sección cero por cualquier sección s' que sea la composición de una sección s'' de E con la inclusión $E\hookrightarrow\mathbb{P}(E\oplus 1)$. En particular, $s'_*(1) = \bar{x}^n + c_1(E)\cdot\bar{x}^{n-1} + \cdots + c_{n-1}(E)\cdot\bar{x} + c_n(E)$ y $c_n(E) = s^*(s'_*(1)) = s_0^*(s''_*(1))$, "la última clase de Chern de E coincide con el número de ceros de cualquier sección suya".

4. Propiedades de las clases de Chern:

1. *La primera clase de Chern de un haz de línea coincide con el opuesto de su clase de obstrucción.*

2. *Si $f\colon X\to Y$ es un morfismo plano o una inmersión cerrada regular, $f^*(c_i(E)) = c_i(f^*(E))$, para todo $i\geq 0$.*

3. *Si X es una variedad lisa, entonces para toda sucesión exacta de $\mathcal{O}_X$-módulos coherentes localmente libres $0\to E'\to E\to E''\to 0$, se verifica:*

$$c_r(E) = \sum_{i+j=r} c_i(E')\cdot c_j(E'')$$

para todo $r\in\mathbb{N}$. Si X no es lisa, véase la observación que sigue a esta proposición.

Demostración. 1. $\mathbb{P}(\mathscr{L}) = X$ y $\mathscr{O}_{\mathbb{P}(\mathscr{L})}(-1) = \mathscr{L}$. Así pues, $x_{\mathscr{L}} = \delta(\mathscr{O}_{\mathbb{P}(\mathscr{L})}(-1)) = \delta(\mathscr{L})$, luego $c_1(\mathscr{L}) = -\delta(\mathscr{L})$.

2. Consideremos el diagrama conmutativo

$$\begin{array}{ccc} \mathbb{P}(f^*E) & \xrightarrow{g} & \mathbb{P}(E) \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

Se cumple que $g^*\mathscr{O}_{\mathbb{P}(E)}(1) = \mathscr{O}_{\mathbb{P}(f^*E)}(1)$, luego $g^*(x_E) = x_{f^*E}$. Aplicando g^* a la relación $x_E^n + c_1(E)x_E^{n-1} + \ldots + c_n(E) = 0$ se concluye.

3. Sea $U = \mathbb{P}(E)\backslash\mathbb{P}(E')$. El morfismo $\pi\colon U \to \mathbb{P}(E'')$ es un fibrado afín, luego $GK(U)$ que es un cociente de $GK(\mathbb{P}(E''))$ es un $GK(X)$-módulo con $d'' = \operatorname{rang} E''$ generadores. Sean $i\colon U \hookrightarrow \mathbb{P}(E)$ y $j\colon \mathbb{P}(E') \hookrightarrow \mathbb{P}(E)$ los morfismos obvios. Como $GK(\mathbb{P}(E'))$ y $GK(\mathbb{P}(E))$ son $GK(X)$-módulo libres de rango d' y $d = d' + d''$, entonces de la sucesión exacta de Gysin $GK(\mathbb{P}(E')) \xrightarrow{j_*} GK(\mathbb{P}(E)) \xrightarrow{i^*} GK(U) \to 0$ se deduce que $GK(U)$ es libre de rango d' y que $GK(U) = GK(\mathbb{P}(E''))$. Además, se tiene la sucesión exacta

$$0 \to GK(\mathbb{P}(E')) \to GK(\mathbb{P}(E)) \to GK(\mathbb{P}(E'')) \to 0$$

Como $j^*(x_E) = x_{E'}$ y $i^*(x_E) = \pi^*(x_{E''})$ y la proposición 17.3.11, se tiene el diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & GK(\mathbb{P}(E')) & \longrightarrow & GK(\mathbb{P}(E)) & \longrightarrow & GK(\mathbb{P}(E'')) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle x_{E'}\cdot} & & \downarrow{\scriptstyle x_E\cdot} & & \downarrow{\scriptstyle x_{E''}\cdot} & & \\ 0 & \longrightarrow & GK(\mathbb{P}(E')) & \longrightarrow & GK(\mathbb{P}(E)) & \longrightarrow & GK(\mathbb{P}(E'')) & \longrightarrow & 0 \end{array}$$

Por tanto, el polinomio característico de $x_E\cdot$ es igual al producto del polinomio característico de $x_{E'}\cdot$ por el de $x_{E''}\cdot$. Se concluye porque el polinomio característico de $x_E\cdot$ es el polinomio de coeficientes las clases de Chern de E.

□

5. Observación: La hipótesis de que X sea lisa, en el apartado 3 anterior, se ha utilizado para que $GK(X)$ sea un anillo y podamos realizar los productos $c_i(E')\cdot c_j(E'')$. Sin embargo no es necesaria, en el siguiente sentido:

Definamos $\widetilde{c}_i(E)$ como el morfismo $GK(X) \to GK(X)$ consistente en multiplicar por $c_i(E)$, o equivalentemente, el morfismo que asocia a cada a el coeficiente en x_E^{n-i} de $-a\cdot x_E^n$ (esta segunda definición no requiere de la estructura de producto en GK). A su vez, $c_i(E)$ se recupera a partir de $\widetilde{c}_i(E)$ por la igualdad $c_i(E) = \widetilde{c}_i(E)(1)$. Entonces podemos enunciar el apartado 3 anterior en el caso no regular por la fórmula

$$\widetilde{c}_r(E) = \sum_{i+j=r} \widetilde{c}_i(E')\cdot\widetilde{c}_j(E'')$$

donde el producto es la composición.

6. Definición: Se llama clase total de Chern de E, y se denota $c(E)$, al elemento $1 + c_1(E) + \ldots + c_n(E) \in GK(X)$.

La tercera propiedad de las clases de Chern afirma que la clase total de Chern es una función aditiva sobre los módulos localmente libres con valores en $1 + \oplus_{i>0} G_iK(X)$. Por tanto, define un morfismo de grupos:

$$c : K^{\cdot}(X) \to 1 + \oplus_{i>0} G_iK(X)$$

Escribiremos $c(x) = \sum_{i\geq 0} c_i(x)$, con $c_i(x) \in G_iK(X)$, y diremos que $c_i(x)$ es la i-ésima clase de Chern de x. Obviamente se cumple que

1. $c_0(x) = 1$.
2. $c_r(x+y) = \sum_{i+j=r} c_i(x) \cdot c_j(y)$.
3. Funtorialidad: $f^*(c_r(x)) = c_r(f^*(x))$ (siempre que tengamos f^* definido en el graduado K).
4. Si x es la clase de un módulo coherente E localmente libre, $c_r(x) = c_r(E)$.

Si E es igual en teoría K a una suma directa de haces de línea, $\mathscr{L}_1 \oplus \ldots \oplus \mathscr{L}_n$, entonces

$$c(E) = c(\mathscr{L}_1) \cdot \ldots \cdot c(\mathscr{L}_n) = (1 + c_1(\mathscr{L}_1)) \cdot \ldots \cdot (1 + c_1(\mathscr{L}_n))$$

Por tanto, $c_i(E)$ es igual a la i-ésima función simétrica elemental de $c_1(\mathscr{L}_1), \ldots, c_1(\mathscr{L}_n)$.

De hecho, igual que en la construcción del cuerpo de descomposición de un polinomio, podemos descomponer todo módulo coherente localmente libre E en suma de haces de línea:

7. Proposición: *Sea E un módulo localmente libre de rango n sobre un esquema X. Existe un morfismo plano de esquemas $X' \xrightarrow{f} X$ tal que:*

(a) Los morfismos $f^! : K^{\cdot}(X) \to K^{\cdot}(X')$, $f^* : GK^{\cdot}(X) \to GK^{\cdot}(X')$ son inyectivos.

(b) f^*E es suma de haces de línea en $K^{\cdot}(X')$.

Demostración. Procedemos por inducción sobre el rango de E. Si es 1, no hay nada que decir. Consideremos el morfismo $\pi : \mathbb{P}(E) \to X$ y la sucesión exacta

$$0 \to E' \to \pi^*E \to \mathscr{O}_{\mathbb{P}(E)}(1) \to 0$$

En teoría K, $\pi^*E = E' \oplus \mathscr{O}_{\mathbb{P}(E)}(1)$. Como E' es de rango uno menor que el de E, existe por inducción un morfismo plano $X' \to \mathbb{P}(E)$ que es inyectivo en teoría K y tal que la

imagen inversa de E' es suma de haces de línea. La composición $X' \to \mathbb{P}(E) \to X$ es el morfismo buscado. □

8. Proposición: *Sea E un módulo localmente libre de rango n. Se verifica:*

1. $c_i(E) = (-1)^i c_i(E^*)$.
2. $c_1(E) = c_1(\Lambda^n E)$.

Demostración. Podemos suponer que E es suma de haces de línea, $E = \mathscr{L}_1 \oplus \cdots \oplus \mathscr{L}_n$. Para todo haz de línea $\mathscr{L}$, $c_1(\mathscr{L}) = -\delta(\mathscr{L}) = \delta(\mathscr{L}^*) = -c_1(\mathscr{L}^*)$. Entonces

1. $c_i(E) = s_i(c_1(\mathscr{L}_1), \ldots, c_1(\mathscr{L}_n)) = (-1)^i s_i(c_1(\mathscr{L}_1^*), \ldots, c_1(\mathscr{L}_n^*)) = (-1)^i s_i(E^*)$.
2. $c_1(E) = c_1(\mathscr{L}_1) + \cdots + c_1(\mathscr{L}_n) = c_1(\mathscr{L}_1 \otimes \cdots \otimes \mathscr{L}_n) = c_1(\Lambda^n E)$, donde la segunda igualdad se debe a que $c_1 = -\delta$ es un morfismo de grupos.

□

17.4.1. Cálculos

Operaciones en teoría K

Vamos a definir unas operaciones en $K^\cdot(X)$ que reflejan los productos simétricos y exteriores de un haz localmente libre.

Sigamos las convenciones $\Lambda^0(\mathscr{P}) = \mathscr{O}_X$ y $\Lambda^1(\mathscr{P}) = \mathscr{P}$.

Si $0 \to \mathscr{P}' \to \mathscr{P} \to \mathscr{P}'' \to 0$ es una sucesión exacta de haces coherentes localmente libres, entonces $\Lambda^n \mathscr{P} = \sum_{i+j=n} \Lambda^i \mathscr{P}' \cdot \Lambda^j \mathscr{P}''$ en $K^\cdot(X)$. En efecto, las imágenes de los morfismos $\Lambda^i \mathscr{P}' \otimes_{\mathscr{O}_X} \Lambda^{n-i} \mathscr{P} \to \Lambda^n \mathscr{P}$ inducen una filtración de $\Lambda^n \mathscr{P}$ cuyo graduado es

$$\bigoplus_{i=0}^{n} (\Lambda^i \mathscr{P}' \otimes_{\mathscr{O}_X} \Lambda^{n-i} \mathscr{P}'')$$

Como en teoría K un módulo es igual a su graduado por una filtración finita, concluimos.

Si $1 + K^\cdot(X)[[t]]$ denota el grupo multiplicativo de las series formales en t con coeficientes en $K^\cdot(X)$ y primer coeficiente la unidad, la igualdad probada demuestra que la función $\Lambda_t(\mathscr{P}) := \sum_{n \geq 0} \Lambda^n(\mathscr{P}) \cdot t^n$ es aditiva, luego induce un morfismo de grupos

$$\lambda_t : K^\cdot(X) \to 1 + K^\cdot(X)[[t]]$$

de modo que para cada módulo $\mathscr{P}$ localmente libre, $\lambda_t(\mathscr{P}) \underset{\text{Not}}{=} \sum_i \lambda^i(\mathscr{P}) t^i := \sum_i \Lambda^i(\mathscr{P}) t^i$.

Procedamos de modo análogo con las álgebras tensoriales simétricas. Sigamos las convenciones $S^0(\mathscr{P}) = \mathscr{O}_X$ y $S^1(\mathscr{P}) = \mathscr{P}$. La función $\sigma_t(\mathscr{P}) \underset{\text{Not.}}{=} \sum_{n\geq 0} \sigma^n(\mathscr{P})\cdot t^n := \sum_{n\geq 0} S^n(\mathscr{P})\cdot t^n$ es aditiva y define un morfismo de grupos

$$\sigma_t : K^{\cdot}(X) \to 1 + K^{\cdot}(X)[[t]]$$

Para todo morfismo $f : Y \to X$ se verifica $f^!(\lambda^n(x)) = \lambda^n(f^!(x))$ y $f^!(\sigma^n(x)) = \sigma^n(f^!(x))$, porque los productos exteriores y simétricos son estables por cambio de base.

9. Ejemplo: Si $\mathscr{L}$ es un haz de línea sobre X, entonces $\lambda_t(\mathscr{L}) = 1 + \mathscr{L}\cdot t$ y $\sigma_t(\mathscr{L}) = \sum_{i\geq 0} \mathscr{L}^i \cdot t^i$, siendo $\mathscr{L}^i = \mathscr{L} \otimes \overset{i}{\ldots} \otimes \mathscr{L}$. Para calcular $\lambda_t(-\mathscr{L})$ y $\sigma_t(-\mathscr{L})$, se procede como sigue:

$$\lambda_t(-\mathscr{L}) = \lambda_t(\mathscr{L})^{-1} = (1+\mathscr{L}\cdot t)^{-1} = \sum_{n\geq 0} (-1)^n \mathscr{L}^n t^n; \quad \lambda^n(-\mathscr{L}) = (-1)^n \mathscr{L}^n$$
$$\sigma_t(-\mathscr{L}) = \sigma_t(\mathscr{L})^{-1} = 1 - \mathscr{L}\cdot t; \qquad \sigma^n(-\mathscr{L}) = 0, \text{ para } n \geq 2$$

10. Proposición : *Sea E un módulo localmente libre de rango n. Se cumple que $\lambda_{-1}(E) \in K_n(X)$ y su clase en $G_nK(X)$ es $c_n(E^*)$.*

Demostración. Podemos suponer que E es suma de haces de línea, $E = \mathscr{L}_1 \oplus \cdots \oplus \mathscr{L}_n$. Para todo haz de línea $\mathscr{L}$, $c_1(\mathscr{L}) = -\delta(\mathscr{L}) = \delta(\mathscr{L}^*) = -c_1(\mathscr{L}^*)$. Entonces $\lambda_{-1}(E) = \lambda_{-1}(\mathscr{L}_1)\cdot\cdots\cdot\lambda_{-1}(\mathscr{L}_n) = (1-\mathscr{L}_1)\cdot\cdots\cdot(1-\mathscr{L}_n)$. Como $1 - \mathscr{L} = \delta(\mathscr{L})$, se concluye. □

Intersección.

Sea $\pi : X \to \operatorname{Spec} k$ un esquema proyectivo de dimensión n. Para cada módulo coherente $\mathscr{M}$, sea $\chi(\mathscr{M})$ su característica. Llamaremos grado al morfismo

$$\operatorname{gr} : G_nK(X) = K_n(X) \to \mathbb{Z},\ \mathscr{M} \mapsto \chi(\mathscr{M})$$

Si X es regular, el morfismo de multiplicación, $G_iK(X) \otimes_{\mathbb{Z}} G_{n-i}K(X) \to G_nK(X)$, compuesto con el grado define un acoplamiento

$$\langle , \rangle : G_iK(X) \otimes_{\mathbb{Z}} G_{n-i}K(X) \to \mathbb{Z}$$

que puede interpretarse como el número global de intersección de ciclos de codimensión i con ciclos de codimensión $n-i$. Por definición de producto en $GK(X)$,

$$\langle \mathscr{M}, \mathscr{M}' \rangle = \sum_{i\geq 0} (-1)^i \chi(\underline{\operatorname{Tor}}_i^{\mathscr{O}_X}(\mathscr{M}, \mathscr{M}'))$$

11. Teorema: *Si E es un haz localmente libre de rango $n = \dim X$, entonces*

$$\mathrm{gr}(c_n(E)) = \sum_{i=0}^{n} (-1)^i \chi(\Lambda^i E^*)$$

Demostración. Como $K_{n+1}(X) = 0$, $c_n(E) = \sum_{i=0}^{n} (-1)^i \Lambda^i(E^*)$ por 17.4.10. Tomando característica se concluye. □

12. Proposición: *Sea $Y \hookrightarrow X$ una inmersión cerrada y regular de codimensión d. Para todo $y \in K_\cdot(Y)$ se verifica*

$$i^! i_!(y) = y \cdot \lambda_{-1}(\mathfrak{p}/\mathfrak{p}^2)$$

siendo $\mathfrak{p}$ el ideal que define a Y. Por tanto, para todo $y \in GK(Y)$ se verifica

$$i^*(i_*(y)) = y \cdot c_d(N_{Y/X})$$

siendo $N_{Y/X}$ el fibrado normal de Y sobre X. En particular, si $\dim Y = d$, entonces

$$\langle Y, Y \rangle = \mathrm{gr}(c_d(N_{Y/X}))$$

"La auto-intersección de Y coincide con el grado del fibrado normal de Y sobre X".

Demostración. Podemos suponer que y es la clase en $K_\cdot(Y)$ de un módulo coherente $\mathscr{M}$ sobre Y. Por definición,

$$i^! i_!(\mathscr{M}) = \sum_{n \geq 0} (-1)^n \underline{\mathrm{Tor}}_n^{\mathscr{O}_X}(\mathscr{M}, \mathscr{O}_Y)$$

Ahora bien, por la teoría del complejo de Koszul, $\underline{\mathrm{Tor}}_n^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_Y) = \Lambda^n(\mathfrak{p}/\mathfrak{p}^2)$, que son $\mathscr{O}_Y$-módulos localmente libres. Por tanto la sucesión espectral $\underline{\mathrm{Tor}}_q^{\mathscr{O}_Y}(\mathscr{M}, \underline{\mathrm{Tor}}_p^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_Y))$, que converge a $\underline{\mathrm{Tor}}_{p+q}^{\mathscr{O}_X}(\mathscr{M}, \mathscr{O}_Y)$, degenera dando lugar a isomorfismos $\mathscr{M} \otimes_{\mathscr{O}_Y} \underline{\mathrm{Tor}}_n^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_Y) \simeq \underline{\mathrm{Tor}}_n^{\mathscr{O}_X}(\mathscr{M}, \mathscr{O}_Y)$. Por tanto,

$$i^! i_!(\mathscr{M}) = \mathscr{M} \underset{\mathscr{O}_Y}{\otimes} \sum_{n \geq 0} (-1)^n \underline{\mathrm{Tor}}_n^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_Y) = \mathscr{M} \cdot \lambda_{-1}(\mathfrak{p}/\mathfrak{p}^2)$$

De aquí se deduce la igualdad $i^*(i_*(y)) = y \cdot c_d(N_{Y/X})$, ya que $c_d(N_{Y/X})$ coincide con la clase de $\lambda_{-1}(\mathfrak{p}/\mathfrak{p}^2)$ (Proposición 17.4.10).

Por último, $i_*(c_d(N_{Y/X})) = i_*(i^* i_*(1)) = i_*(1) \cdot i_*(1)$. Del diagrama conmutativo

$$\begin{array}{ccc} G_d K(Y) & \xrightarrow{\quad i_* \quad} & G_{2d} K(X) \\ & {\scriptstyle \mathrm{gr}} \searrow \quad \swarrow {\scriptstyle \mathrm{gr}} & \\ & \mathbb{Z} & \end{array}$$

se concluye que $\langle Y, Y \rangle = \mathrm{gr}(c_d(N_{Y/X}))$.

□

17.5. Teorema de Riemann-Roch

En esta sección todos los esquemas se consideran lisos sobre un cuerpo k.

17.5.1. Carácter de Chern. Clase de Todd

Sea E un módulo localmente libre de rango n. Escribamos $c(E) = \prod_{i=1}^{n}(1+\alpha_i)$.

1. Definición: Sea $F(t) \in \mathbb{Q}[[t]]$ una serie formal. Llamaremos extensión aditiva de $F(t)$ a $K^{\cdot}(X)$ al morfismo

$$\begin{array}{rccl} F_+: & K^{\cdot}(X) & \to & GK(X)\otimes_{\mathbb{Z}}\mathbb{Q} \\ & E & \mapsto & F_+(E) := \sum_{i=1}^{n} F(\alpha_i) \end{array}$$

que está bien definido porque toda función simétrica en $\alpha_1,\ldots,\alpha_n$ es una función en las clases de Chern de E.

Si el primer coeficiente de la serie $F(t)$ es la unidad, se define

$$F_{\cdot}(E) := \prod_{i=1}^{n} F(\alpha_i)$$

y se denomina extensión multiplicativa de $F(t)$ a $K^{\cdot}(X)$.

2. Propiedades: *Para todo $x,x' \in K(X)$ se verifica:*

1. $F_+(x+x') = F_+(x)+F_+(x')$, $F_{\cdot}(x+x') = F_{\cdot}(x)\cdot F_{\cdot}(x')$.
2. *Si x es la clase de un haz de línea $\mathscr{L}$,* $F_+(x) = F(c_1(\mathscr{L})) = F_{\cdot}(x)$.
3. *Si $f:\bar{X}\to X$ es un morfismo,* $F_+(f^!(x)) = f^*(F_+(x))$, *y* $F_{\cdot}(f^!(x)) = f^*(F_{\cdot}(x))$.

3. Definición: Se llama carácter de Chern al morfismo $\mathrm{ch}: K^{\cdot}(X)\to GK(X)$ obtenido como extensión aditiva de la serie $e^t = \sum_{i\geq 0}\frac{t^i}{i!}$.

4. Proposición: *El carácter de Chern es un morfismo de anillos.*

Demostración. Basta probarlo para los haces de línea. Si $\mathscr{L}$ y $\mathscr{L}'$ son haces de línea

$$\mathrm{ch}(\mathscr{L}\cdot\mathscr{L}') = e^{c_1(\mathscr{L}\otimes\mathscr{L}')} = e^{c_1(\mathscr{L})+c_1(\mathscr{L}')} = e^{c_1(\mathscr{L})}\cdot e^{c_1(\mathscr{L}')} = \mathrm{ch}(\mathscr{L})\cdot\mathrm{ch}(\mathscr{L}')$$

□

5. Definición: Se llama clase de Todd al morfismo $\mathrm{Td}: K^{\cdot}(X)\to GK(X)$ obtenido como extensión multiplicativa de la serie $\frac{t}{1-e^{-t}} = 1+\frac{t}{2}+\frac{t^2}{12}+\ldots$.

17.5.2. Enunciado del teorema

Sea $f: Y \to X$ un morfismo proyectivo entre variedades algebraicas lisas. Sean T_Y, T_X los fibrados tangentes de Y e X respectivamente.

6. Definición: Se llama tangente relativo virtual de f, y se denota T_f, al elemento de $K^{\cdot}(X)$ definido por: $T_f = T_Y - f^! T_X$.

Si $\mathbb{P}(E) \xrightarrow{\pi} X$ es un fibrado proyectivo, entonces el tangente relativo virtual de π es el dual de las diferenciales relativas: $T_\pi = (\Omega_{\mathbb{P}(E)/X})^*$.

Si $Y \xhookrightarrow{i} X$ es una inmersión regular, entonces su tangente relativo virtual es el opuesto del fibrado normal: $T_i = -N_{Y/X}$.

Consideremos el siguiente diagrama:

$$\begin{array}{ccc} K(Y) & \xrightarrow{f_!} & K(X) \\ \Big\downarrow{\scriptstyle \mathrm{ch}} & & \Big\downarrow{\scriptstyle \mathrm{ch}} \\ GK(Y)\otimes_{\mathbb{Z}}\mathbb{Q} & \xrightarrow{f_*} & GK(X)\otimes_{\mathbb{Z}}\mathbb{Q} \end{array}$$

El teorema de Riemann-Roch afirma que este diagrama es conmutativo salvo un factor de corrección.

7. Teorema (de Riemann-Roch): *Sea $f: Y \to X$ un morfismo proyectivo entre k-variedades lisas. Para todo $y \in K(Y)$ se verifica*

$$f_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_Y)] = \mathrm{ch}(f_!(y))\cdot \mathrm{Td}(T_X)$$

Un enunciado alternativo es:

8. Teorema (de Riemann-Roch): $\mathrm{ch}(f_!(y)) = f_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_f)]$.

La equivalencia de ambos enunciados se deduce de la fórmula de proyección:

$$f_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_Y - f^! T_X)] = f_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_Y)\cdot f^*\,\mathrm{Td}(T_X)^{-1}] = f_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_Y)]\cdot \mathrm{Td}(T_X)^{-1}$$

17.5.3. Demostración del teorema de Riemann-Roch

9. Proposición: *Si el teorema de Riemann-Roch es cierto para dos morfismos, también lo es para la composición.*

Demostración. Supongamos que los morfismos $Y \xrightarrow{f} X$ y $X \xrightarrow{g} Z$ verifican el teorema de Riemann-Roch. Entonces,

$$\begin{aligned}(g\circ f)_*[\mathrm{ch}(y)\cdot \mathrm{Td}(T_Y)] &= g_*[\mathrm{ch}(f_!(y))\cdot \mathrm{Td}(T_X)] = \mathrm{ch}(g_! f_!(y))\cdot \mathrm{Td}(T_Z) \\ &= \mathrm{ch}((g\circ f)_!(y))\cdot \mathrm{Td}(T_Z)\end{aligned}$$

□

10. Corolario : *Si el teorema de Riemann-Roch es cierto para inmersión cerrada y para la proyección $X \times \mathbb{P}^r \to X$, entonces es cierto para cualquier morfismo proyectivo.*

11. Teorema: *Si $i : Y \hookrightarrow X$ es una inmersión cerrada de codimensión 1 y el morfismo $i^! : K(X) \to K(Y)$ es epiyectivo, entonces verifica el Riemann-Roch.*

Demostración. Tenemos que ver que $\mathrm{ch}(i_!(a)) = i_*[\mathrm{ch}(a) \cdot \mathrm{Td}(-N)]$, siendo $N = N_{Y/X}$ el fibrado normal de Y sobre X. Por hipótesis podemos poner $a = i^!(b)$. Por la fórmula de proyección, se reduce a probar la igualdad

$$\mathrm{ch}(i_!(1)) = i_* \mathrm{Td}(-N)$$

Por un lado $\mathrm{ch}(i_!(1)) = \mathrm{ch}(1 - \mathfrak{p}) = 1 - e^{c_1(\mathfrak{p})}$, siendo $\mathfrak{p}$ el ideal (de línea) que define a Y.

Por otra parte, $i_* \mathrm{Td}(-N) = i_* i^* \mathrm{Td}(-\mathfrak{p}^*) = \mathrm{Td}(-\mathfrak{p}^*) \cdot Y = \frac{Y}{\mathrm{Td}(\mathfrak{p}^*)} = Y \cdot \frac{(1-e^{-c_1(\mathfrak{p}^*)})}{c_1(\mathfrak{p}^*)}$. Como $Y = c_1(\mathfrak{p}^*) = -c_1(\mathfrak{p})$, se concluye. □

12. Teorema: *Sea E un módulo localmente libre sobre un esquema X. El teorema de Riemann-Roch se verifica para la sección cero $X \hookrightarrow \mathbb{P}(E \oplus 1)$.*

Demostración. Después de un cambio de base, podemos suponer que E admite una filtración cuyos cocientes son haces de línea. Entonces la sección nula es composición de inmersiones de codimensión 1 cuyas imágenes inversas admirables son epiyectivas, luego se concluye por el teorema anterior. □

13. Teorema: *El teorema de Riemann-Roch se verifica para toda inmersión regular $Y \hookrightarrow X$.*

Demostración. La demostración consiste en reducir el teorema al caso anterior mediante la deformación al cono normal. Sea $\widetilde{Z}$ la explosión de $X \times \mathbb{P}^1$ a lo largo de $Y \times \infty$. Consideremos el diagrama

$$\begin{array}{ccc} Y \times \mathbb{P}^1 & \xrightarrow{\ j\ } & \widetilde{Z} \\ & \searrow \quad \swarrow_{\tilde{\pi}} & \\ & \mathbb{P}^1 & \end{array}$$

construido en la demostración del teorema de deformación al cono normal (véase la observación que sigue a dicho teorema). Para cada punto cerrado $t \in \mathbb{P}^1$, sea $\widetilde{Z}_t$ la fibra de t por la proyección $\widetilde{Z} \to \mathbb{P}^1$. Sea $j_t : Y = Y \times t \hookrightarrow \widetilde{Z}_t$ la inmersión inducida. Para $t = 0$ se obtiene la inmersión de partida $Y \hookrightarrow X$ y para $t = \infty$ la sección cero $Y \hookrightarrow \mathbb{P}(N \oplus 1) \cup \tilde{X}$

(de modo que $Y \cap \tilde{X} = \emptyset$). Denotemos $i_t \colon \widetilde{Z}_t \hookrightarrow \widetilde{Z}$ la inclusión. Se tiene el diagrama cartesiano

$$\begin{array}{ccc} Y \times \mathbb{P}^1 & \xrightarrow{j} & \widetilde{Z} \\ {\scriptstyle 1\times t}\uparrow & & \uparrow{\scriptstyle i_t} \\ Y \times t & \xrightarrow{j_t} & \widetilde{Z}_t \end{array}$$

y por tanto, si para cada $a \in K(Y)$ denotamos $a \times \mathbb{P}^1 = j_!({\pi_1}^!(a))$, se verifica la igualdad $j_{t_!}(a) \overset{(*)}{=} i_t^!(a \times \mathbb{P}^1)$

Tenemos que probar que $\mathrm{ch}(j_{0_!}(a)) = j_{0*}[\mathrm{ch}(a) \cdot \mathrm{Td}(-N)]$. El morfismo $i_{0*} \colon GK(\widetilde{Z}_0) = GK(X) \to GK(\widetilde{Z})$ es inyectivo, pues tiene retracto (la imagen directa de la proyección $\widetilde{Z} \to X$). Por tanto, basta probar la fórmula después de aplicar i_{0*}.

Por un lado

$$i_{0*}\,\mathrm{ch}(j_{0_!}(a)) \overset{(*)}{=} i_{0*} i_0^* \,\mathrm{ch}(a \times \mathbb{P}^1) = \mathrm{ch}(a \times \mathbb{P}^1) \cdot \widetilde{Z}_0$$

por la fórmula de proyección.

Por otro lado

$$i_{0*} j_{0*}[\mathrm{ch}(a) \cdot \mathrm{Td}(-N)] = i_{\infty *} j_{\infty *}[\mathrm{ch}(a) \cdot \mathrm{Td}(-N)] = i_{\infty *}\,\mathrm{ch}(j_{\infty_!}(a))$$

donde la última igualdad es por Riemann-Roch para $j_\infty \colon Y \hookrightarrow \mathbb{P}(N \oplus 1)$, teniendo en cuenta que $T_{j_\infty} = T_{j_0} = -N$. Ahora, de nuevo por la igualdad $(*)$,

$$i_{\infty *}\,\mathrm{ch}(j_{\infty_!}(a)) = i_{\infty *} i_\infty^* \,\mathrm{ch}(a \times \mathbb{P}^1) = \mathrm{ch}(a \times \mathbb{P}^1) \cdot \widetilde{Z}_\infty$$

Como $\widetilde{Z}_0 = \widetilde{Z}_\infty$ en teoría K, hemos concluido. □

Para terminar la demostración del teorema de Riemann-Roch necesitamos probarlo para la proyección $X \times \mathbb{P}^r \to X$. Para ello es necesario calcular la clase de Todd. Esta vendrá dada por el siguiente teorema.

En Geometría Diferencial, consideremos la proyección regular natural $E \setminus \{0\} \xrightarrow{f} \mathbb{P}(E)$, cuyas fibras son las curvas integrales del campo D de las homotecias. Por el teorema de Fröbenius, las 1-formas diferenciales de $\mathbb{P}(E)$ se corresponden con las 1-formas w diferenciales de E, constantes a lo largo de las fibras (i.e., $D^L w = 0$) tales que $i_D w = 0$. Denotemos por $\mathscr{E}$ el haz de $C^\infty_{\mathbb{P}(E)}$-módulos de las secciones de $E \times \mathbb{P}(E) \to \mathbb{P}(E)$. Se cumple que $f_* \Omega_{E-0} = \mathscr{E}^*$ y que el haz de módulos sobre $\mathbb{P}(E)$ de las 1-formas diferenciables constantes a lo largo de las fibras de π es isomorfo a $\mathscr{E}^*(-1)$. Luego se obtiene la siguiente sucesión exacta

$$0 \to \Omega_{\mathbb{P}^n(E)} \to \mathscr{E}^*(-1) \xrightarrow{i_D} C^\infty_{\mathbb{P}(E)} \to 0$$

14. Teorema: *Sea $\mathbb{P}(E) \xrightarrow{\pi} X$ un fibrado proyectivo de rango n. Se tiene una sucesión exacta*

$$0 \to \Omega_{\mathbb{P}(E)/X} \to (\pi^* E^*)(-1) \to \mathscr{O}_{\mathbb{P}(E)} \to 0$$

Demostración. Dar una sección $s\colon X \to \mathbb{P}(E)$ de π, equivale a dar un haz de línea $\mathscr{L}$ y un epimorfismo $E^* \to \mathscr{L}$. En efecto, si denotamos por K el núcleo de este epimorfismo, tenemos la sucesión exacta $0 \to K \to E^* \to \mathscr{L} \to 0$ que induce la sucesión exacta $K \otimes_{\mathscr{O}_X} S^{\cdot}_{\mathscr{O}_X}(E^*)(-1) \to S^{\cdot}_{\mathscr{O}_X}(E^*) \to S^{\cdot}_{\mathscr{O}_X}(\mathscr{L}) \to 0$, de modo que el epimorfismo al tomar Proj define s. Por localización homogénea obtenemos la sucesión exacta de $\mathscr{O}_{\mathbb{P}(E)}$-módulos

$$(\pi^* K)(-1) \to \mathscr{O}_{\mathbb{P}(\pi^* E)} \to s_* \mathscr{O}_X \to 0$$

luego un epimorfismo $(\pi^* K)(-1) \to \mathfrak{p}_{s(X)}$, donde $\mathfrak{p}_{s(X)}$ es el ideal de las funciones de $\mathbb{P}(E)$ que se anulan en $s(X)$. Tomando imagen inversa por s, se obtiene un epimorfismo $K \otimes \mathscr{L}^* \to \mathfrak{p}_{s(X)}/\mathfrak{p}^2_{s(X)}$, que es isomorfismo por ser ambos localmente libres del mismo rango, luego $K = \mathfrak{p}_{s(X)}/\mathfrak{p}^2_{s(X)} \otimes \mathscr{L}$. Por tanto se tiene la sucesión exacta

$$0 \to \mathfrak{p}_{s(X)}/\mathfrak{p}^2_{s(X)} \otimes \mathscr{L} \to E^* \to \mathscr{L} \to 0$$

Ahora ya, si cambiamos de base $\mathbb{P}(E) \to X$ por el mismo $\pi\colon \mathbb{P}(E) \to X$ con lo que obtenemos $\mathbb{P}(\pi^* E) = \mathbb{P}(E) \times_X \mathbb{P}(E) \to \mathbb{P}(E)$ y consideramos como sección la inmersión diagonal (que es el morfismo obtenido del epimorfismo $\pi^* E^* \to \mathscr{O}_{\mathbb{P}(E)}(1)$) concluimos el teorema.

□

15. Teorema: *La proyección natural $X \times \mathbb{P}^r \xrightarrow{\pi} X$ verifica el teorema de Riemann-Roch.*

Demostración. Calculemos en primer lugar la clase de Todd. Denotemos $\mathbb{P}^r_X = X \times \mathbb{P}^r$. Por el teorema anterior, $\mathrm{Td}(T_\pi) = \mathrm{Td}(\mathscr{O}_{\mathbb{P}^r_X}(1))^{r+1} = (\frac{x}{1-e^{-x}})^{r+1}$, siendo x la clase de un hiperplano.

Por el teorema de periodicidad, basta probar el teorema de Riemann-Roch para $1, x, \ldots, x^r$. Para 1, se reduce a probar que $1 = \pi_*[(\frac{x}{1-e^{-x}})^{r+1}]$. Dado que $\pi_*(x^i) = 0$ para $i < r$ y $\pi_*(x^r) = 1$, basta probar que el coeficiente de $(\frac{x}{1-e^{-x}})^{r+1}$ en x^r es 1. Equivalentemente, hay que ver que el residuo en el origen de la forma $(\frac{1}{1-e^{-t}})^{r+1} dt$ es 1. Efectuando el cambio de variable $u = 1 - e^{-t}$, se obtiene:

$$\mathrm{Res}_0\left(\frac{dt}{(1-e^{-t})^{r+1}}\right) = \mathrm{Res}_0\left(\frac{du}{u^{r+1} \cdot (1-u)}\right) = \mathrm{Res}_0\left(\sum_{n \geq 0} \frac{u^n}{u^{r+1}} du\right) = 1$$

Para probar el teorema para $x, \ldots, x^r$, se puede hacer un cálculo análogo al anterior. De otra forma, basta probar que el teorema es cierto para $i_*(a)$, siendo $i\colon \mathbb{P}^{r-1}_X \hookrightarrow \mathbb{P}^r_X$ un hiperplano. Esto se deduce fácilmente del teorema de Riemann-Roch para i y para $\pi'\colon \mathbb{P}^{r-1}_X \to X$ (por inducción), teniendo en cuenta que $T_{\pi'} = i^! T_\pi - T_i$. □

Vamos a probar, como consecuencia del Riemann-Roch, que el carácter de Chern induce un isomorfismo de anillos $\mathrm{ch}_{\mathbb{Q}}\colon K(X)\otimes_{\mathbb{Z}}\mathbb{Q}\to GK(X)\otimes_{\mathbb{Z}}\mathbb{Q}$.

16. Lema: *Si* ch_i *es la componente homogénea de grado* i *del carácter de Chern, entonces*

$$\mathrm{ch}_i=\frac{1}{i!}\left[(-1)^{i-1}i\cdot c_i+P(c_1,\ldots,c_{i-1})\right]$$

para cierto polinomio P *con coeficientes enteros.*

Demostración. Tenemos que probar que si $s_1,\ldots,s_n$ son las funciones simétricas elementales de las variables $x_1,\ldots x_n$, entonces

$$x_1^i+\ldots+x_n^i=(-1)^{i-1}i\cdot s_i+P(s_1,\ldots,s_{i-1})$$

Ahora bien, $x_1^i+\ldots+x_n^i$ es un polinomio universal de grado i en $s_1,\ldots,s_n$, considerando que s_j tiene grado j. Para determinar el coeficiente de s_i hacemos cociente por $(s_1,\ldots,\hat{s}_i,\ldots,s_n)$, luego podemos suponer que $x_1,\ldots,x_n$ son las raíces de la ecuación $T^n+(-1)^i s_i T^{n-i}=T^{n-i}\cdot(T^i+(-1)^i s_i)$. En este caso, $x_1^i+\ldots+x_n^i=(-1)^{i-1}\cdot i\cdot s_i$, y se concluye.

□

17. Proposición: *Si* Y *es una subvariedad irreducible de codimensión* d *de una* k*-variedad lisa proyectiva, entonces*

1. $c_i(Y)=0$*, para* $0\le i<d$.
2. $c_d(Y)=(-1)^d(d-1)!\cdot Y$ *en* $GK(X)\otimes_{\mathbb{Z}}\mathbb{Q}$.

Demostración. Aplicando Riemann-Roch a la inmersión cerrada $i\colon Y\hookrightarrow X$ obtenemos

$$\begin{aligned}\mathrm{ch}(i_!(1))&=i_*(\mathrm{ch}(1)\cdot\mathrm{Td}(T_i))=i_*(1+\text{ términos de codimensión mayor que 1})\\&=Y+\text{ términos de codimensión mayor que d}\end{aligned}$$

La expresión del carácter de Chern en términos de las clases de Chern dada por el lema anterior permite concluir que $c_d(Y)=(-1)^{d-1}(d-1)!\cdot Y$ en $GK(X)\otimes_{\mathbb{Z}}\mathbb{Q}$. □

En la subsección siguiente veremos que esta proposición es cierta sin denominadores, es decir, en $GK(X)$.

18. Teorema: *Sea* X *una variedad proyectiva lisa. El morfismo* $\mathrm{ch}_{\mathbb{Q}}\colon K(X)\otimes_{\mathbb{Z}}\mathbb{Q}\to GK(X)\otimes_{\mathbb{Z}}\mathbb{Q}$ *es un isomorfismo.*

Demostración. Por la proposición y lema anteriores, $\mathrm{ch}_{\mathbb{Q}}$ es compatible con las respectivas filtraciones. De nuevo por la proposición y lema anteriores, el morfismo inducido por $\mathrm{ch}_{\mathbb{Q}}$ en los graduados es un isomorfismo, es más, es el morfismo identidad (salvo un factor multiplicativo). Por el teorema formal de la función inversa $\mathrm{ch}_{\mathbb{Q}}$ es un isomorfismo. □

17.5.4. Riemann-Roch sin denominadores

Sea $i\colon Y \hookrightarrow X$ una inmersión cerrada entre variedades lisas. Para todo módulo localmente libre E sobre Y, el Riemann-Roch nos dice

$$\mathrm{ch}(i_*E) = i_*[\mathrm{ch}(E)\cdot \mathrm{Td}(-N)]$$

que es una igualdad en $GK(X)\otimes_{\mathbb{Z}}\mathbb{Q}$. Nuestro propósito ahora es dar una fórmula sin denominadores, es decir, en $GK(X)$, en vez de para el carácter de Chern, para la clase total de Chern $c(i_*(E))$.

19. Lema: *Fijemos enteros positivos d,r. Existe una única serie formal $P(x_1,\dots,x_d,y_1,\dots,y_r)$ con coeficientes enteros tal que para cualesquiera fibrados N,E de rangos d,r sobre cualquier variedad Y, se verifica*

$$c((\lambda_{-1}N^*)\otimes E) = 1 + c_d(N)\cdot P(N,E)$$

donde $P(N,E)$ denota $P(c_1(N),\dots,c_d(N),c_1(E),\dots,c_r(E))$. En particular $c_i((\lambda_{-1}N^*)\otimes E) = 0$ para todo $0<i<d$.

Demostración. Sean $\alpha_1,\dots,\alpha_d$ las raíces de Chern de N y $\beta_1,\dots,\beta_r$ las raíces de Chern de E. Entonces

$$c((\lambda_{-1}N^*)\otimes E) - 1 = \prod_{p=0}^{d}\prod_{j=1}^{r}\prod_{i_1<\cdots<i_p}(1+\beta_j-\alpha_{i_1}-\cdots-\alpha_{i_p})^{(-1)^p} - 1.$$

Basta ver que el término derecho de esta ecuación es divisible por α_1, pues entonces, por simetría, es divisible por todos los α_i, y por tanto por su producto, que es $c_d(N)$. Si hacemos α_1 igual a cero, cada término del producto con $i_1>1$ y exponente $(-1)^p$ se cancela con un término con $i_1=1$ y exponente $(-1)^{p+1}$. □

20. Proposición: *Sea $E = E'\oplus\mathscr{O}_X$ un $\mathscr{O}_X$-módulo localmente libre de rango n y consideremos la sección cero $s\colon X\to\mathbb{P}(E'\oplus\mathscr{O}_X)$. Entonces*

1. $s_!(1) = \lambda_{-1}(E'^*(-1))$
2. $s_!(1) = \lambda_{-1}(\Omega_{\mathbb{P}(E)/X}(1))$.

Demostración. (1) El epimorfismo $E'^*\oplus\mathscr{O}_X\to\mathscr{O}_X$ define la sección cero s, tomando espectros proyectivos en el epimorfismo $S^\cdot(E'^*\oplus\mathscr{O}_X)\to S^\cdot(\mathscr{O}_X)$. El núcleo de este epimorfismo es claramente $E'^*\otimes_{\mathscr{O}_X}S^\cdot(E^*)(-1)$. En conclusión, por Koszul, se tiene la sucesión exacta

$$0\to\Lambda^n\mathscr{M}\to\Lambda^{n-1}\mathscr{M}\to\cdots\to\mathscr{M}\to\mathscr{O}_{\mathbb{P}(E)}\to s_*\mathscr{O}_X\to 0,\quad \mathscr{M}=\pi^*E'^*(-1)$$

luego $s_!(1) = \lambda_{-1}(\pi^* E'^*(-1))$

(2) Consideremos la sucesión exacta $0 \to \Omega_{\mathbb{P}(E)/X}(1) \to \pi^* E^* \to \mathscr{O}_{\mathbb{P}(E)}(1) \to 0$. Entonces

$$\begin{aligned}\lambda_{-1}(\Omega_{\mathbb{P}(E)/X}(1)) &= \lambda^n(\Omega_{\mathbb{P}(E)/X}(1) - \mathscr{O}_{\mathbb{P}(E)}) = \lambda^n(E^* - \mathscr{O}_{\mathbb{P}(E)} - \mathscr{O}_{\mathbb{P}(E)}(1)) = \lambda^n(E'^* - \mathscr{O}_{\mathbb{P}(E)}(1)) \\ &= \lambda^n(E'^*(-1) - \mathscr{O}_{\mathbb{P}(E)}) \otimes \mathscr{O}_{\mathbb{P}(E)}(n) = \lambda_{-1}(E'^*(-1)) \otimes \mathscr{O}_{\mathbb{P}(E)}(n) = s_!(1) \otimes \mathscr{O}_{\mathbb{P}(E)}(n) \\ &= s_!(1)\end{aligned}$$

donde la ultima igualdad se debe a que $\mathscr{O}_{\mathbb{P}(E)}(n)$ restringido a $s(X)$ es $\mathscr{O}_{s(X)}$. □

21. Teorema (Riemann-Roch sin denominadores): *Sea $i\colon Y \hookrightarrow X$ una inmersión cerrada entre variedades lisas, de codimensión d y fibrado normal N. Sea E un $\mathscr{O}_Y$-módulo localmente libre de rango r. Entonces*

$$c(i_! E) = 1 + i_*(P(N, E)),$$

donde P es el definido en el lema anterior.

Demostración. Veamos primero el caso de la sección cero $s\colon Y \hookrightarrow \mathbb{P}(N \oplus 1)$. Denotemos por π la proyección de $\mathbb{P}(N \oplus 1)$ en Y. Para todo $\mathscr{O}_Y$-módulo localmente libre E,

$$c(s_! E) = c(s_! s^! \pi^! E) = c((\lambda_{-1}\mathscr{M}) \otimes \pi^* E) = 1 + c_d(\mathscr{M}^*) \cdot P(\mathscr{M}^*, \pi^* E)$$

donde la última igualdad es por el lema anterior. Ahora bien, $c_d(\mathscr{M}^*)$ es la clase de $\lambda_{-1}\mathscr{M}$ (por 17.4.10) y este último coincide con $s_*(1)$ por la proposición anterior. En definitiva, $c_d(\mathscr{M}^*) \cdot P(\mathscr{M}^*, \pi^* E) = s_*(1) \cdot P(\mathscr{M}^*, \pi^* E) = s_*(P(s^* \mathscr{M}^*, E)) = s_*(P(N, E))$, pues $s^* \mathscr{O}_{\mathbb{P}(N \oplus 1)}(1) = \mathscr{O}_Y$, y queda terminada la demostración para s.

El caso general se reduce a éste último mediante la deformación al cono normal: cópiese literalmente la demostración del Riemann-Roch para una inmersión cerrada, sustituyendo el carácter de Chern por la clase total de Chern en todas las fórmulas. □

22. Corolario: *Si $i\colon Y \hookrightarrow X$ es una subvariedad no singular de codimensión d de una k-variedad no singular y proyectiva X, entonces para todo $\mathscr{O}_Y$-módulo localmente libre E de rango r*

1. $c_i(i_! E) = 0$, para $0 < i < d$.
2. $c_d(i_! E) = (-1)^d (d-1)!\, r \cdot Y$.

en $GK(X)$. En particular, $c_i(Y) = 0$ para $0 < i < d$ y $c_d(Y) = (-1)^d (d-1)! \cdot Y$.

Demostración. Si denotamos P_q la componente homogénea de grado q de P (donde c_i se dota de grado i), se verifica (para $q>0$)

$$c_q(i_!E) = i_*(P_{q-d}(N,E))$$

luego $c_q(i_!E)=0$ para $0<q<d$ y $c_d(i_!E)=i_*(P_0(N,E))$. Para concluir, basta ver que $P_0(N,E)=(-1)^d(d-1)!\,r$. Para cualesquiera fibrados N,E de rangos d,r sobre cualquier variedad Y se tienen las igualdades

$$c_d(N)\cdot P_0(N,E) = c_d((\lambda_{-1}N^*)\otimes E) = (-1)^{d-1}(d-1)!\,\mathrm{ch}_d((\lambda_{-1}N^*)\otimes E)$$

donde la segunda igualdad es por el lema 17.5.16 y porque $c_i((\lambda_{-1}N^*)\otimes E)=0$ para $0<i<d$, por el Lema 17.5.19. Ahora bien,

$$\mathrm{ch}_d((\lambda_{-1}N^*)\otimes E) = [\mathrm{ch}(\lambda_{-1}N^*)\cdot\mathrm{ch}(E)]_d = c_d(N)[\mathrm{Td}(N)^{-1}\mathrm{ch}(E)]_0 = c_d(N)\,\mathrm{ch}_0(E) = r\cdot c_d(N)$$

donde la segunda igualdad se debe a que $\mathrm{ch}(\lambda_{-1}N^*)\cdot\mathrm{Td}(N)=c_d(N)$ para todo fibrado N de rango d (véase 17.6.14). Con todo, se concluye. □

17.6. Cálculos y ejemplos

En esta sección vamos a ver ejemplos y aplicaciones de la teoría dada en las secciones anteriores: teoría K, clases de Chern y Riemann-Roch.

17.6.1. Teoría K

1) Si $X=\mathrm{Spec}\mathscr{O}$, siendo $\mathscr{O}$ un anillo local noetheriano, entonces $K^{\cdot}(X)\simeq\mathbb{Z}$, y el isomorfismo está definido por el rango.

2) Si X es una curva irreducible y no singular, el morfismo

$$\begin{aligned} K^{\cdot}(X) &\to \mathbb{Z}\oplus\mathrm{Pic}(X)\\ \mathscr{P} &\mapsto (\mathrm{rg}(\mathscr{P}),\Lambda^n\mathscr{P})\end{aligned}$$

es isomorfismo. En efecto:

Evidentemente es epiyectivo, porque dado $(n,\mathscr{L})$, $\mathscr{O}_X^{n-1}\oplus\mathscr{L}$ se aplica en él.

Para demostrar la inyectividad, recordemos que $K^{\cdot}(X)=K_{\cdot}(X)$. Todo haz localmente libre admite un subhaz de línea tal que el cociente no tiene torsión, luego $K(X)$ está generado por los haces de línea. Todo haz de línea es suma de $\mathscr{O}_X$ y un haz de torsión, en $K(X)$. En efecto, si $\mathscr{L}=\mathscr{L}_{D-D'}$, siendo D,D' divisores efectivos, de las sucesiones exactas

$$\begin{aligned} 0\to\mathscr{L}_{-D'}\to\mathscr{L}\to\mathscr{N}\to 0\\ 0\to\mathscr{L}_{-D'}\to\mathscr{O}_X\to\mathscr{N}'\to 0\end{aligned}$$

se deduce que $\mathscr{L} = 1 + \mathscr{N} - \mathscr{N}'$ en $K(X)$ y los haces $\mathscr{N}$, $\mathscr{N}'$ están concentrados en puntos cerrados. En conclusión, todo elemento $\mathscr{P}$ de $K(X)$ es de la forma $n+T-T'$, para ciertos haces T, T' concentrados en puntos. Si $D = \sum_x l(T_x)\cdot x$ y $D' = \sum_x l(T'_x)\cdot x$, entonces $\mathscr{P} := n-1+\mathscr{L}_{D-D'} = n+T-T'$. Si $\mathscr{P}$ está en el núcleo del morfismo $K^\cdot(X) \to \mathbb{Z}\oplus \mathrm{Pic}(X)$, entonces $n=0$ y $\mathscr{L}_{D-D'} = \mathscr{O}_X$. Hemos terminado.

3) **Números globales de intersección** Sea X una variedad proyectiva. La característica de Euler-Poincaré:

$$\chi(\mathscr{M}) = \sum_{i\geq 0}(-1)^i \dim_k H^i(X,\mathscr{M})$$

es una función aditiva sobre los $\mathscr{O}_X$-módulos coherentes, luego define un morfismo $\chi\colon K_\cdot(X) \to \mathbb{Z}$.

Si Y, Y' son cerrados de X de codimensiones complementarias en cada componente conexa de X, se define el número global de intersección de Y con Y' como

$$\langle Y, Y'\rangle := \chi(\mathscr{O}_Y \cdot \mathscr{O}_{Y'}) = \sum_{i\geq 0}(-1)^i \chi(\underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{Y'}))$$

Por ejemplo, si Y, Y' son curvas proyectivas planas de grados r y s, veamos que el número global de intersección es $r\cdot s$. De la sucesión exacta

$$0 \to \mathscr{O}_{\mathbb{P}^2}(-r) \to \mathscr{O}_{\mathbb{P}^2} \to \mathscr{O}_Y \to 0$$

se deduce que $\mathscr{O}_Y = 1 - \mathscr{O}_{\mathbb{P}^2}(-r)$ en teoría K. Es decir, Y es igual, en teoría K, a una recta contada r veces. Podemos suponer entonces que $Y \equiv x_0^r = 0$, $Y' \equiv x_1^s = 0$ y entonces

$$\begin{aligned}\langle Y, Y'\rangle := \chi(\mathscr{O}_Y \cdot \mathscr{O}_{Y'}) &= \sum_{i\geq 0}\chi(\underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{Y'})) = \sum_{i\geq 0}\chi(\mathrm{Tor}_i^{k[x,y]}(k[x,y]/(x^r), k[x,y]/(y^s)) \\ &= \dim_k k[x,y]/(x^r,y^s) = r\cdot s\end{aligned}$$

Si X es una curva lisa y Δ es la diagonal de $X\times X$, entonces

$$\mathscr{O}_\Delta \cdot \mathscr{O}_\Delta = (1-\mathscr{L}_{-\Delta})^2 = 1 - 2\mathscr{L}_{-\Delta} + \mathscr{L}_{-2\Delta} = (1-\mathscr{L}_{-\Delta}) - (\mathscr{L}_{-\Delta} - \mathscr{L}_{-2\Delta})$$

De la sucesión exacta $0 \to \mathscr{L}_{-2\Delta} \to \mathscr{L}_{-\Delta} \to \Omega_X \to 0$ obtenemos que $\mathscr{O}_\Delta \cdot \mathscr{O}_\Delta = 1 - \Omega_X$. Por tanto, $\langle \Delta, \Delta\rangle = \chi(\mathscr{O}_\Delta \cdot \mathscr{O}_\Delta) = \chi(\mathscr{O}_X) - \chi(\Omega_X) = 2-2g$, siendo g el género de X.

En general, si X es una variedad propia lisa, la diagonal Δ es un subesquema regular de $X\times X$, y la teoría del complejo de Koszul permite probar que (denotemos $\mathscr{O} = \mathscr{O}_{X\times X}$)

$$\underline{\mathrm{Tor}}_i^{\mathscr{O}}(\mathscr{O}_\Delta, \mathscr{O}_\Delta) = \Lambda^i \underline{\mathrm{Tor}}_1^{\mathscr{O}}(\mathscr{O}_\Delta, \mathscr{O}_\Delta) = \Lambda^i(\mathfrak{p}_\Delta/\mathfrak{p}_\Delta^2) = \Omega_X^i$$

luego $\mathscr{O}_\Delta \cdot \mathscr{O}_\Delta = \sum_{i\geq 0}(-1)^i \Omega_X^i$ y

$$\langle \Delta, \Delta \rangle = \sum_{i\geq 0} \chi(\Omega_X^i) = \sum_{i,j} (-1)^{i+j} \dim_k H^j(X, \Omega_X^i)$$

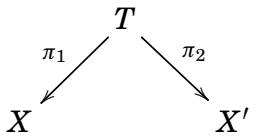
4) **Correspondencias algebraicas de curvas:** Sean X y X' curvas irreducibles, completas y lisas sobre un cuerpo k. Σ y Σ' denotarán sus respectivos cuerpos de funciones. Todos los morfismos y productos directos serán sobre k.

La determinación de la teoría K de las curvas no singulares se puede aplicar al estudio de las correspondencias algebraicas. Una correspondencia de X en X' es, por definición, un divisor de $X \times X'$. Se dice que la correspondencia es irreducible cuando es el divisor definido por una curva íntegra de $X \times X'$. Se llaman correspondencias verticales a las sumas finitas de fibras de la proyección de $X \times X' \to X$, y correspondencias horizontales a las sumas finitas de fibras de $X \times X' \to X'$. Estas correspondencias se consideran triviales, y se llama grupo de las correspondencias de X en X', y se denota $C(X, X')$, al grupo de libre generado por todas las correspondencias, módulo las verticales y horizontales. Por definición,

$$C(X, X') := \mathrm{Div}(\Sigma \otimes_k \Sigma')$$

Observemos que $\Sigma \otimes_k \Sigma'$ es un dominio de Dedekind cuyo espectro consiste en el punto genérico de $X \times X'$ y las correspondencias de X en X'.

Si T es una correspondencia irreducible que no sea vertical ni horizontal, entonces es una curva de $X \times X'$, y está dotada de proyecciones no constantes sobre X y X'



que son morfismos finitos planos (porque $\mathscr{O}_X$ y $\mathscr{O}_{X'}$ son localmente dominios de ideales principales y $\mathscr{O}_T$ no tiene torsión).

Dado un divisor $D = \sum_i n_i x_i$ de X, definimos $\pi_1^{-1}(D) := \sum_i n_i \pi_1^{-1}(x_i)$, donde

$$\pi_1^{-1}(x_i) := \sum_{t \in \pi_1^{-1}(x_i)} l(\mathscr{O}_t / \mathfrak{m}_{x_i} \mathscr{O}_t) \cdot t$$

Dado un divisor $D' = \sum_i n_i t_i$ en T, se define $\pi_{2*}(D') := \sum_i n_i \pi_{2*}(t_i)$, donde

$$\pi_{2*}(t_i) := \mathrm{gr}(t_i) \cdot \pi_2(t_i)$$

siendo $\mathrm{gr}(t_i)$ el grado de la extensión $k(\pi_2(t_i)) \to k(t_i)$. Tenemos pues un morfismo $\pi_{2*}\pi_1^{-1}\colon \mathrm{Div}(X) \to \mathrm{Div}(X')$. Extendiendo por linealidad, se obtiene un morfismo de grupos

$$C(X,X') \to \mathrm{Hom}(\mathrm{Div}(X), \mathrm{Div}(X'))$$

que da la interpretación geométrica de las correspondencias: son las aplicaciones algebraicas de X en X' que asignan a cada punto de X varios puntos de X'.

a) Las imágenes por una correspondencia de divisores linealmente equivalentes, son divisores linealmente equivalentes:

Basta demostrarlo para correspondencias irreducibles. Sea T una correspondencia irreducible. La composición de los morfismos $K(X) = K_\cdot(X) \overset{\pi_1^!}{\to} K_\cdot(T) \overset{\pi_{2!}}{\to} K_\cdot(X') = K(X')$, define, por la determinación de los grupos K de las curvas no singulares, un morfismo $\mathrm{Pic}(X) \to \mathrm{Pic}(X')$, que coincide con el morfismo inducido entre los divisores, módulo la equivalencia lineal.

b) El morfismo $\mathrm{Pic}(X) \to \mathrm{Pic}(X')$ definido por una correspondencia vertical es nulo. Las correspondencias horizontales definen un morfismo $\mathrm{Pic}(X) \to \mathrm{Pic}(X')$ que es nulo entre los respectivos Pic_0, como es fácil de comprobar.

Se dice que dos correspondencias son equivalentes cuando son linealmente equivalentes en $X \times X'$, módulo correspondencias verticales y horizontales. El grupo de las clases de correspondencias se denota $A(X,X')$. Por definición,

$$A(X,X') := \mathrm{Pic}(\Sigma \otimes_k \Sigma')$$

Veamos que el morfismo $\mathrm{Pic}_0(X) \to \mathrm{Pic}_0(X')$ inducido por una correspondencia sólo depende de su clase de equivalencia. Es decir, el morfismo natural $C(X,X') \to \mathrm{Hom}(\mathrm{Div}(X), \mathrm{Div}(X'))$, induce un morfismo $A(X,X') \to \mathrm{Hom}(\mathrm{Pic}_0(X), \mathrm{Pic}_0(X'))$.

Denotemos p_1 y p_2 las proyecciones de $X \times X'$ en X y X', respectivamente. Sea $i\colon T \hookrightarrow X \times X'$ la inclusión. Si demostramos que el morfismo $T\colon \mathrm{Pic}(X) \to \mathrm{Pic}(X')$ inducido por la correspondencia T es: $T(D) = p_{2_!}(\mathscr{O}_T \cdot p_1^!(D))$ habremos concluido. Ahora bien,

$$p_{2_!}(\mathscr{O}_T \cdot p_1^!(D)) = p_{2_!}(i_!(1) \cdot p_1^!(D)) = p_{2_!}(i_!(i^!(p_1^!(D)))) = \pi_{2_!}\pi_1^!(D) = T(D)$$

donde la segunda igualdad se debe a la fórmula de la proyección.

El teorema de periodicidad.

Sea $\mathbb{P}(E) \to X$ un fibrado proyectivo de rango n y $x = 1 - \mathscr{O}_{\mathbb{P}(E)}(-1)$. Por el teorema de periodicidad x^{n+1} es combinación lineal de $1, x, \ldots, x^n$. Se tiene por tanto una relación

$$x^{n+1} + a_0 x^n + \cdots + a_{n-1}x + a_n, \qquad a_i \in K_\cdot(X)$$

Veamos cómo calcular explícitamente los coeficientes de este relación. Siguiendo las notaciones del teorema de periodicidad, sea t la clase de $\mathscr{O}_{\mathbb{P}(E)}(-1)$ en $K(\mathbb{P}(E))$. Entonces de la sucesión exacta

$$0 \to \Omega_{\mathbb{P}(E)/X} \to (\pi^* E^*)(-1) \to \mathscr{O}_{\mathbb{P}(E)} \to 0$$

se obtiene en teoría K

$$\begin{aligned} 0 = \lambda^{n+1}(\Omega_{\mathbb{P}(E)/X}) = \lambda^{n+1}(\pi^* E^*(-1) - \mathscr{O}_{\mathbb{P}(E)}) = \sum_{i=0}^{n+1} \lambda^i(\pi^* E^*(-1)) \cdot \lambda^{n+1-i}(-\mathscr{O}_{\mathbb{P}(E)}) \\ = \sum_{i=0}^{n+1} (-1)^{n+1-i} \lambda^i(E^*) \cdot t^i \end{aligned}$$

lo cual nos permite despejar cómo se expresa t^{n+1} como combinación lineal de $1, t, \ldots, t^n$ con coeficientes en $K(X)$. De aquí se puede calcular la expresión de x^{n+1} en función de $1, x, \ldots, x^n$, sin más que tener en cuenta que $t = 1 - x$. En definitiva, se puede reenunciar el teorema de periodicidad diciendo que se tiene el isomorfismo de $K(X)$-álgebras

$$K(\mathbb{P}(E)) = K(X)[x]/(\sum_{i=0}^{n+1} (-1)^{n+1-i} \lambda^i(E^*) \cdot (1-x)^i)$$

Vamos a computar de otro modo los coeficientes de la relación mediante una operación en teoría K que facilita el estudio de las clases de Chern, que es la función γ.

Para todo $x \in K^\cdot(X)$, definamos $\gamma^n(x) = \lambda^n(x + n - 1)$ y $\gamma_t(x) = \sum_{i \geq 0} \gamma^i(x) t^i$. Si $\mathscr{L}$ es un haz de línea y $x = 1 - \mathscr{L}$, entonces

$$\begin{aligned} \gamma^n(x) = \gamma^n(1 - \mathscr{L}) = \lambda^n(n - \mathscr{L}) = \sum_{i+j=n} \lambda^i(n) \cdot \lambda^j(-\mathscr{L}) = \sum_{i+j=n} (-1)^j \binom{n}{i} \mathscr{L}^j = (1 - \mathscr{L})^n \\ = x^n \end{aligned}$$

Además

$$\begin{aligned} \gamma_t(x) = \sum_{i \geq 0} \lambda^i(x + i - 1) t^i = \sum_{i \geq 0} (\sum_{r=0}^{i} \lambda^r(i-1) \lambda^{i-r}(x)) t^i = \sum_{i \geq 0} (\sum_{r=0}^{i} \binom{i-1}{r} \lambda^{i-r}(x)) t^i \\ = \sum_{n \geq 0} \lambda^n(x) \cdot (\binom{n-1}{0} t^r + \binom{n}{1} t^{r+1} + \binom{n+1}{2} t^{r+2} + \cdots) = \sum_{n \geq 0} \lambda^n(x) (\frac{t}{1-t})^n = \lambda_{\frac{t}{1-t}}(x) \end{aligned}$$

Recíprocamente, se cumple que $\lambda_t(x) = \gamma_{\frac{t}{1+t}}(x)$. Como consecuencia, $\gamma_t \colon K(X) \to 1 + K(X)[[t]]$ es una función aditiva. Se puede reenunciar el teorema de periodicidad de la siguiente manera

$$K(\mathbb{P}(E)) = K(X)[x]/(\sum_{i=0}^{n+1} \gamma^{n+1-i}(E-n-1)x^i)$$

En efecto, el conúcleo del morfismo universal $\mathscr{O}_{\mathbb{P}(E)}(-1) \to \pi^* E$ es un haz localmente libre de rango n. Por tanto:

$$\begin{aligned} 0 = \lambda^{n+1}(\pi^! E - t) = \gamma^{n+1}(\pi^! E - t - n) = \gamma^{n+1}(\pi^! E - n - 1 + x) \\ = \sum_{i=0}^{n+1} \gamma^{n+1-i}(\pi^! E - n - 1) \cdot \gamma^i(x) = \sum_{i=0}^{n+1} \gamma^{n+1-i}(\pi^! E - n - 1) \cdot x^i \end{aligned}$$

El teorema de Periodicidad nos permite calcular con precisión la clase en teoría K de un haz coherente en un espacio proyectivo sobre un cuerpo k. Si x es la clase de un hiperplano en $K(\mathbb{P}^n)$, entonces x^i es la clase de un subespacio lineal de codimensión i; por tanto, $\chi(x^i) = 1$ para todo $0 \le i \le n$.

Si V es una subvariedad de $\mathbb{P}^n$ de dimensión r y grado d, entonces $\chi(\mathscr{O}_V \cdot x^i) = 0$ para $i > n-r$, porque se puede encontrar un subespacio lineal de codimensión i que no corte a V. Además, $\chi(\mathscr{O}_V \cdot x^{n-r}) = d$, por definición de grado. En consecuencia:

$$\mathscr{O}_V = d \cdot x^{n-r} + \sum_{i>n-r} m_i \cdot x^i$$

En particular, si C es una curva de grado d en $\mathbb{P}^3$, entonces $\mathscr{O}_C = dx^2 + mx^3$. Tomando característica en esta igualdad, se concluye

$$\mathscr{O}_C = d \cdot x^2 + (1 - \pi - d) \cdot x, \text{ siendo } 1 - \pi = \chi(\mathscr{O}_C)$$

Si S es una superficie de grado d en $\mathbb{P}^3$, y π es el género aritmético de sus secciones hiperplanas, $\mathscr{O}_S = d \cdot x + m \cdot x^2 + l \cdot x^3$. Cortando con un hiperplano, obtenemos

$$1 - \pi = \chi(\mathscr{O}_S \cdot x) = \chi(dx^2 + mx^3) = d + m$$

además, si escribimos $\chi(\mathscr{O}_S) = 1 - p_a$ se obtiene

$$\mathscr{O}_S = d \cdot x + (1 - \pi - d) \cdot x^2 + (\pi - p_a) \cdot x^3$$

Grupo K de una explosión.

Sea X un esquema noetheriano e $Y \hookrightarrow X$ un subesquema cerrado definido por un ideal $\mathfrak{p}$. Sea $f : X' \to X$ la explosión de X a lo largo de Y e $Y' = f^{-1}(Y)$ la fibra excepcional. Denotaremos $\mathfrak{p}'$ el ideal de la fibra excepcional, es decir, $\mathfrak{p}' = \mathfrak{p}\mathscr{O}_{X'}$.

1. Lema: $\mathfrak{p}' = \mathscr{O}_{X'}(1)$.

Demostración. Localizando homogéneamente la sucesión exacta

$$0 \to (\bigoplus_{n+1\geq 0} \mathfrak{p}^{n+1})(1) \to (\bigoplus_{n\geq 0} \mathfrak{p}^n) \to (\bigoplus_{n\geq 0} \mathfrak{p}^n/\mathfrak{p}^{n+1}) \to 0$$

se obtiene la sucesión exacta

$$0 \to \mathscr{O}_{X'}(1) \to \mathscr{O}_{X'} \to \mathscr{O}_{Y'} \to 0$$

y se concluye que $\mathfrak{p}' = \mathscr{O}_{X'}(1)$. □

2. Lema de estabilidad: *Para $n >> 0$,*

$$R^i f_*(\mathscr{O}_{X'}(n)) = \begin{cases} \mathfrak{p}^n & para\ i = 0 \\ 0 & para\ i > 0 \end{cases}$$

Demostración. Por el teorema de Serre, $R^i f_*(\mathscr{O}_{X'}(n)) = 0$, para todo $i > 0$ y $n >> 0$. $\mathscr{O}_{X'}$ es la localización homogénea de $\oplus_n \mathfrak{p}^n$, y de $\oplus_n f_*\mathscr{O}_{X'}(n)$. Por **??**, $f_*(\mathscr{O}_{X'}(n)) = \mathfrak{p}^n$, para $n >> 0$. □

3. Ejemplo: Por el lema de estabilidad, para $n >> 0$,

$$\chi(X, \mathscr{O}_X/\mathfrak{p}^n) = \chi(X, \mathscr{O}_X) - \chi(X, \mathfrak{p}^n) = \chi(X, \mathscr{O}_X) - \chi(X', \mathfrak{p}^n\mathscr{O}_{X'})$$

Denotemos Y' a la clase de $\mathscr{O}_{Y'}$ en $K_\cdot(X')$. Por ser $\mathfrak{p}\mathscr{O}_{X'} = \mathscr{O}_{X'}(1)$ un haz de línea, se tiene que $\mathfrak{p}^n\mathscr{O}_{X'} = (1 - Y')^n = \sum_i (-1)^i \binom{n}{i} Y'^i$. Por tanto,

$$\chi(X, \mathscr{O}_X/\mathfrak{p}^n) = \chi(X, \mathscr{O}_X) - \chi(X', \mathscr{O}_{X'}) - \sum_{i>0} (-1)^i \binom{n}{i} \chi(Y'^i)$$

igualdad que determina los números de intersección de Y' consigo misma.

Este ejemplo explica por qué $\mathfrak{p}'$ tiene a veces propiedades de polo. Por ejemplo, si X es el plano proyectivo sobre un cuerpo, o cualquier superficie lisa propia, e Y es un punto racional, la intersección de Y' consigo misma en X' es -1, pues $\chi(X, \mathscr{O}_X/\mathfrak{p}^n) = \binom{n+1}{2}$ es el polinomio de Samuel de X en el punto racional.

4. Notación: A partir de ahora, X será un esquema noetheriano, regular y separado, e $i : Y \to X$ un subesquema cerrado y regular. Por el teorema 8.2.7, X' es un esquema regular.

Consideremos el diagrama

$$\begin{array}{ccc} Y' = f^{-1}(Y) & \xrightarrow{j} & X' \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{i} & X \end{array}$$

Por el teorema 8.2.5, $Y' = \mathrm{Proj}(G_{\mathfrak{p}}\mathscr{O}_X) = \mathbb{P}((\mathfrak{p}/\mathfrak{p}^2)^*)$ es un fibrado proyectivo sobre Y.

5. Fórmula llave: *Para todo $y \in K(Y)$ se verifica*

$$f^! i_!(y) = j_![g^!(y) \cdot \lambda_{-1}(\Omega_{Y'/Y}(1))]$$

Dado que $\lambda_{-1}(\Omega_{Y'/Y}(1))$ se puede interpretar como la clase en teoría K de una sección de $Y' \to Y$ que no corta a un hiperplano, la fórmula llave tiene la siguiente significación geométrica: Meter un ciclo de Y en X y subirlo a X' equivale a subirlo a Y', cortar con una sección del morfismo $Y' \to Y$ y meterlo en X'.

Demostración. Por definición, si $\mathscr{P}$ es un $\mathscr{O}_Y$-módulo localmente libre, se verifica:

$$\begin{aligned} &f^! i_!(\mathscr{P}) = \sum_{i\geq 0} (-1)^i \underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{P}, \mathscr{O}_{X'}). \\ &j_![g^!(\mathscr{P}) \cdot \lambda_{-1}(\Omega_{Y'/Y}(1))] = (\mathscr{P} \otimes_{\mathscr{O}_Y} \mathscr{O}_{Y'}) \cdot (\sum_{i\geq 0} (-1)^i \Omega^i_{Y'/Y}(i)) \\ &= \sum_{i\geq 0} (-1)^i \mathscr{P} \otimes_{\mathscr{O}_Y} \Omega^i_{Y'/Y}(i) \end{aligned}$$

En consecuencia, es suficiente probar que $\underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{P}, \mathscr{O}_{X'}) \simeq \mathscr{P} \otimes_{\mathscr{O}_Y} \Omega^i_{Y'/Y}(i)$. Ahora bien, debido al isomorfismo $\underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{P}, \mathscr{O}_{X'}) = \mathscr{P} \otimes_{\mathscr{O}_Y} \underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'})$, basta demostrar, para todo $i \geq 0$ que

$$\underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) = \Lambda^i_{\mathscr{O}_{Y'}}(\Omega^i_{Y'/Y}(1))$$

Para $i = 0$ es cierto. Para $i = 1$: De la sucesión exacta $0 \to \mathfrak{p} \to \mathscr{O}_X \to \mathscr{O}_Y \to 0$, obtenemos la sucesión exacta

$$0 \to \underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) \to \mathfrak{p} \otimes_{\mathscr{O}_X} \mathscr{O}_{X'} \to \mathfrak{p}' \to 0$$

Por ser $\mathfrak{p}'$ localmente libre sobre $\mathscr{O}_{X'}$, tensando por $\otimes_{\mathscr{O}_{X'}} \mathscr{O}_{Y'}$ obtenemos la sucesión exacta

$$0 \to \underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) \to \mathfrak{p}/\mathfrak{p}^2 \otimes_{\mathscr{O}_Y} \mathscr{O}_{Y'} \to \mathfrak{p}'/\mathfrak{p}'^2 \to 0 \qquad (*)$$

Por otra parte, la sucesión exacta de diferenciales del fibrado proyectivo $Y' \to Y$ es

$$0 \to \Omega_{Y'/Y} \to \mathfrak{p}/\mathfrak{p}^2 \otimes_{\mathscr{O}_Y} \mathscr{O}_{Y'}(-1) \to \mathscr{O}_{Y'} \to 0$$

Tensando por $\mathscr{O}_{Y'}(1)$ y utilizando que $\mathfrak{p}'/\mathfrak{p}'^2 = \mathscr{O}_{Y'}(1)$, pues $\mathscr{O}_{X'}(1) = \mathfrak{p}'$, tenemos la sucesión exacta

$$0 \to \Omega_{Y'/Y}(1) \to \mathfrak{p}/\mathfrak{p}^2 \otimes_{\mathscr{O}_Y} \mathscr{O}_{Y'} \to \mathfrak{p}'/\mathfrak{p}'^2 \to 0 \qquad (**)$$

Comparando $(*)$ y $(**)$ obtenemos que $\underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) = \Omega_{Y'/Y}(1)$.

Para $i > 1$ basta demostrar que $\Lambda^i \underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) = \underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'})$. En primer lugar, veamos que hay un morfismo natural $\Lambda^i \underline{\mathrm{Tor}}_1^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'}) \to \underline{\mathrm{Tor}}_i^{\mathscr{O}_X}(\mathscr{O}_Y, \mathscr{O}_{X'})$. En efecto, sea $\mathscr{P}_\cdot \to \mathscr{O}_Y$ una resolución por $\mathscr{O}_X$-módulos localmente libres, con $\mathscr{P}_0 = \mathscr{O}_X$. El

morfismo $\mathscr{P}_1 \to \mathscr{O}_X$ define una diferencial en $\Lambda^{\cdot}\mathscr{P}_1$ (la contracción interior) y la igualdad $\mathscr{P}_1 = \mathscr{P}_1$ levanta localmente a un morfismo de complejos $\Lambda^{\cdot}\mathscr{P}_1 \to \mathscr{P}_{\cdot}$, único en homología, que define el morfismo natural buscado. Para ver que este último morfismo es isomorfismo basta verlo localmente en X'.

Sea $U \subseteq X$ un abierto afín en el que $\mathfrak{p}$ esté engendrado por una sucesión regular $f_0, f_1, \ldots, f_p$; y sea $K_{\cdot} \to \mathscr{O}_Y(U) \to 0$ el complejo de Koszul asociado. Recubriendo $f^{-1}(U)$ por los abiertos V_i en los que $\mathfrak{p}' = (f_i)$, se puede suponer, para $i = 0$ que $\mathfrak{p}' = (f_0)$ y que $\frac{f_i}{f_0}$ están definidos. Si $e_0, \ldots, e_p$ es una base de K_1, tal que $d(e_i) = f_i$ para $0 \leq i \leq p$, consideremos la nueva base

$$e'_0 = e_0, e'_i = e_i - \frac{f_i}{f_0} \cdot e_0 \text{ para } i > 0$$

En esta base $d(e'_0) = f_0$ y $d(e'_i) = 0$. En consecuencia, los ciclos de grado i del complejo $K_{\cdot} \otimes_{\mathscr{O}_X} \mathscr{O}_{X'}$ se identifican con la potencia exterior i-ésima de $\langle e'_1, \ldots, e'_p \rangle \otimes_{\mathscr{O}_X} \mathscr{O}_{X'}$, y los bordes son $f_0 \cdot K_i \otimes_{\mathscr{O}_X} \mathscr{O}_{X'}$. Hemos concluido. □

6. Lema: *Para todo $n \geq 0$ se cumple*

$$R^i f_*(\mathscr{O}_{X'}(n)) = \begin{cases} \mathfrak{p}^n & \text{para } i = 0 \\ 0 & \text{para } i > 0 \end{cases}$$

En particular, $f_!(\mathscr{O}_{X'}(n)) = \mathfrak{p}^n$.

Demostración. Tenemos morfismos naturales $\mathfrak{p}^n \hookrightarrow f_*\mathscr{O}_{X'}(n)$, luego el teorema es local en X. Podemos suponer que $X = \operatorname{Spec} A$ e $\mathfrak{p}$ está generado por una sucesión regular $(f_0, \ldots, f_r)$.

Vamos a demostrar el teorema por inducción sobre $\dim X$. Sea $Z = (f_0)_0$ y Z' la explosión de Z a lo largo de Y. Denotemos $\bar{\mathfrak{p}}$ a la clase de $\mathfrak{p}$ en $\mathscr{O}_Z = A/f_0A$. Por 4.2.5, $\bar{\mathfrak{p}}^n = \mathfrak{p}^n/((f_0) \cap \mathfrak{p}^n) = \mathfrak{p}^n/f_0 \cdot \mathfrak{p}^{n-1}$. Ahora ya, es fácil ver que tenemos la sucesión exacta

$$0 \to \mathscr{O}_{X'}(n-1) \xrightarrow{\cdot f_0} \mathscr{O}_{X'}(n) \to \mathscr{O}_{Z'}(n) \to 0$$

Como $f_*(\mathscr{O}_{Z'}(n)) = \bar{\mathfrak{p}}^n$, $R^i f_*(\mathscr{O}_{Z'}(n)) = 0$ para $i > 0$, y $\mathfrak{p}^n \hookrightarrow f_*\mathscr{O}_{X'}(n)$, tenemos la sucesión exacta

$$0 \to f_*(\mathscr{O}_{X'}(n-1)) \to f_*(\mathscr{O}_{X'}(n)) \to \bar{\mathfrak{p}}^n \to 0$$

y $R^i f_*(\mathscr{O}_{X'}(n-1)) = R^i f_*(\mathscr{O}_{X'}(n))$, para $i > 0$. Por 17.6.2, concluimos ya que $f_*(\mathscr{O}_{X'}(n)) = \mathfrak{p}^n$, y $R^i f_*(\mathscr{O}_{X'}(n)) = 0$, para todo $n \geq 0$.

□

7. Grupo K de una explosión: *La sucesión*

$$0 \to K(Y) \xrightarrow{\alpha} K(X) \oplus K(Y') \xrightarrow{f^!+j_!} K(X') \to 0$$

es exacta, siendo $\alpha(y) = (i_!(y), -g^!(y)\cdot\lambda_{-1}(F))$ *y* $F = \Omega_{Y'/Y}(1)$.

Demostración. 1) α es inyectivo: Si $\alpha(y) = (0,0)$, entonces $g^!(y)\cdot\lambda_{-1}(F) = 0$. La fórmula de la proyección implica $0 = y\cdot g_!(\lambda_{-1}(F))$ y basta demostrar que $g_!(\lambda_{-1}(F)) = 1$. Si el fibrado proyectivo $g\colon Y' \to Y$, tiene una sección s, entonces $g_!(\lambda_{-1}(F)) = g_!(s_!(1)) = 1$. Por cambio de la base Y a Y', el teorema de periodicidad y el teorema de cambio de base 17.2.15, podemos suponer que la sección s existe.

2) $f^! + j_!$ es epiyectivo: Es consecuencia del teorema de Gysin, 17.2.16.

3) $\operatorname{Im}\alpha \subseteq \operatorname{Ker}(f^! + j_!)$, según afirma la fórmula llave.

4) $\operatorname{Im}\alpha \supseteq \operatorname{Ker}(f^! + j_!)$: Sea $(x,y') \in \operatorname{Ker}(f^! + j_!)$, es decir, $f^!(x) + j_!(y') = 0$. Hay que encontrar un $y \in K(Y)$ tal que $\alpha(y) = (i_!(y), -g^!(y)\cdot\lambda_{-1}(F)) = (x,y')$. Sea $y = -g_!(y')$. Se cumple que

$$i_!(y) = i_!(-g_!(y')) = (i\circ g)_!(-y') = (f\circ j)_!(y') = f_!(j_!(-y')) = f_!(f^!(x)) = x\cdot f_!(1) = x$$

Nos falta probar que $-g^!(y)\cdot\lambda_{-1}(F) = y'$. Por la fórmula llave,

$$j_!(-g^!(y)\cdot\lambda_{-1}(F)) = -f^! i_!(y) = -f^!(x) = j_!(y')$$

Además, $g_!(-g^!(y)\cdot\lambda_{-1}(F)) = -y\cdot g_!(\lambda_{-1}(F)) = -y = g_!(y')$. Habremos terminado si probamos que $\operatorname{Ker} j_! \cap \operatorname{Ker} g_! = 0$. Si $a \in \operatorname{Ker} j_!$, entonces $0 = j^!(j_!(a)) = a\cdot j^!(\mathscr{O}_{Y'}) = a\cdot(\mathscr{O}_{Y'} - \mathscr{O}_{Y'}(1))$. Por tanto, $a\cdot\mathscr{O}_{Y'}(n) = a$. Si además $a = \sum_{i=0}^{d-1} a_i\mathscr{O}_{X'}(i) \in \operatorname{Ker} g_!$, entonces $0 = g_!(a) = g_!(a\cdot\mathscr{O}_{X'}(-d+1)) = a_{d-1}$, luego $0 = g_!(a) = g_!(a\cdot\mathscr{O}_{X'}(-d+2)) = a_{d-2}$, y así sucesivamente obtenemos que $a = 0$.

□

17.6.2. Clases de Chern

8. Definición: Llamaremos clases de Chern de una variedad regular X a las clases de Chern de su fibrado tangente $T_X = (\Omega_{X/k})^*$, y se denotan $c_i(X)$.

9. Proposición: *La primera clase de Chern de X coincide con el opuesto del divisor canónico, es decir, con la clase de obstrucción de* $\Omega^n_{X/k}$ *($n = \dim X$).*

Demostración. $c_1(T_X) = c_1(\Lambda^n T_X) = c_1((\Omega^n_{X/k})^*) = -c_1(\Omega^n_{X/k}) = \delta(\Omega^n_{X/k})$. □

10. Proposición: *Sea X un esquema liso y proyectivo sobre k, de dimensión constante n. El grado de $c_n(X)$ coincide con la auto-intersección de la diagonal en $X \times_k X$.*

Demostración. Se deduce de 17.4.12 porque el fibrado normal a la inmersión diagonal es el fibrado tangente. □

11. Proposición: *Si H es un hiperplano de $\mathbb{P}^n$, entonces*

$$c(\Omega_{\mathbb{P}^n/k}) = (1-H)^{n+1}$$

y por tanto $c_i(\mathbb{P}^n) = \binom{n+1}{i} H^i$.

Demostración. La segunda afirmación es consecuencia de la primera y de que $c_i(\mathbb{P}^n) = (-1)^i c_i(\Omega_{\mathbb{P}^n/k})$. La primera igualdad se deduce de la aditividad de las clases de Chern y de la sucesión exacta:

$$0 \to \Omega_{\mathbb{P}^n/k} \to \mathcal{O}_{\mathbb{P}^n}(-1)^{n+1} \to \mathcal{O}_{\mathbb{P}^n} \to 0$$

□

12. Ejercicio: Probar que el grado de la última clase de Chern de una variedad es igual al "número de ceros de un campo tangente".

13. Ejercicio: Probar que si E es un módulo localmente libre de rango n, entonces $\gamma^i(E-n)$ pertenece a $K_i(X)$. Concluir que la clase de $\gamma^i(E-n)$ en $GK^i(X)$ es la i-ésima clase de Chern de E. Utilizando esta igualdad y la aditividad de la función γ_t, concluir la aditividad de las clases de Chern.

14. Proposición: *Si E es un módulo localmente libre de rango n, entonces*

$$\mathrm{Td}(E) \cdot \mathrm{ch}(\lambda_{-1}(E^*)) = c_n(E)$$

Demostración. Podemos suponer que $E = \mathscr{L}_1 \oplus \ldots \oplus \mathscr{L}_n$. Entonces,

$$\begin{aligned} \mathrm{Td}(E) = \mathrm{Td}(\mathscr{L}_1) \cdot \ldots \cdot \mathrm{Td}(\mathscr{L}_n) &= \frac{c_1(\mathscr{L}_1)}{1-e^{-c_1(\mathscr{L}_1)}} \cdot \ldots \cdot \frac{c_1(\mathscr{L}_n)}{1-e^{-c_1(\mathscr{L}_n)}} \\ \mathrm{ch}(\lambda_{-1}(E^*)) = \mathrm{ch}(\lambda_{-1}(\mathscr{L}_1^*)) \cdot \ldots \cdot \mathrm{ch}(\lambda_{-1}(\mathscr{L}_n^*)) &= \mathrm{ch}(1-\mathscr{L}_1^*) \cdot \ldots \cdot \mathrm{ch}(1-\mathscr{L}_n^*) \\ &= (1-e^{-c_1(\mathscr{L}_1)}) \cdot \ldots \cdot (1-e^{-c_1(\mathscr{L}_n)}) \end{aligned}$$

luego $\mathrm{Td}(E) \cdot \mathrm{ch}(\lambda_{-1}(E^*)) = c_1(\mathscr{L}_1) \cdot \ldots \cdot c_1(\mathscr{L}_n) = c_n(E)$. □

Clases de Segre.

Sea C un cono sobre un esquema X, es decir, $C = \mathrm{Spec}\, S^\cdot$, donde $S^\cdot$ es un haz de $\mathcal{O}_X$-álgebras graduadas. Suponemos que $\mathcal{O}_X \to S^0$ es epiyectivo, que S^1 es coherente y $S^\cdot$ está generado por S^1. Sea $\mathbb{P}(C \oplus 1) \xrightarrow{\pi} X$ el cierre proyectivo de C y $\mathcal{O}(1)$ el haz de línea tautológico de $\mathbb{P}(C \oplus 1)$. Denotemos $x = c_1(\mathcal{O}(1))$.

15. Definición: Llamaremos clase total de Segre de C, y lo denotaremos $s(C)$, al elemento de $GK(X)$ definido por

$$s(C) = \pi_*(1 + x + x^2 + \cdots) = \pi_*(\frac{1}{1-x})$$

La componente de $s(C)$ en grado i la denotaremos $s_i(C)$ y la denominaremos i-ésima clase de Segre de C.

Los casos de mayor interés son el de un fibrado proyectivo y el del cono normal de un subesquema: Si $E \to X$ es un fibrado vectorial, denotaremos $s(E)$ a la clase de Segre del cono $S^{\cdot}E^*$ y lo denominaremos clase de Segre de E. Si $Y \hookrightarrow X$ es un subesquema cerrado, denotaremos $s(Y,X)$ a la clase de Segre del cono normal de Y sobre X, y lo denominaremos clase de Segre de Y en X.

16. Teorema: *Si $E \to X$ es un fibrado vectorial, entonces su clase de Segre es el inverso de su clase total de Chern:*

$$s(E) = \frac{1}{c(E)}$$

En particular, si $Y \hookrightarrow X$ es una inmersión regular, entonces

$$s(Y,X) = \frac{1}{c(\mathcal{N}_{Y/X})}.$$

Demostración. Sea $s\colon X \hookrightarrow \mathbb{P}(E \oplus 1)$ la sección cero. Por el Teorema 17.4.2, $s_*(1) = \sum c_i(E) \cdot x^{n-i}$, siendo n el rango de E y $x = c_1(\mathcal{O}_{\mathbb{P}(E\oplus 1)}(1))$. Como x coincide con la clase de cohomología del hiperplano del infinito y éste no corta a $s(X)$, se tiene

$$s_*(1) = s_*(1) \cdot \frac{1}{1-x} = \sum_{i=0}^{n} c_i(E) \cdot (x^{n-i} + x^{n-i+1} + x^{n-i+2} + \cdots)$$

Proyectando en X, y teniendo en cuenta que $\pi_*(x^i) = 0$ para $i < n$, se obtiene $1 = c(E) \cdot s(E)$. □

17. Teorema: *Sea $f\colon X' \to X$ un morfismo propio y epiyectivo entre variedades algebraicas, $Y \hookrightarrow X$ un subesquema cerrado e $Y' = f^{-1}(Y)$. Entonces*

$$f_* s(Y',X') = \mathrm{gr}(X'/X) \cdot s(Y,X)$$

En particular, si f es birracional, $f_* s(Y',X') = s(Y,X)$, es decir, las clases de Segre son birracionalmente invariantes.

Demostración. Sean C, C' los conos normales de Y en X y de Y' en X' respectivamente. Denotemos Z, Z' las explosiones de $X \times \mathbb{A}^1$ y $X' \times \mathbb{A}^1$ a lo largo de $Y \times 0$ e $Y' \times 0$ respectivamente. Las fibras excepcionales son $\mathbb{P}(C \oplus 1)$ y $\mathbb{P}(C' \oplus 1)$ respectivamente. El morfismo

f induce de modo natural un morfismo $G\colon Z' \to Z$ de modo que $G^{-1}(\mathbb{P}(C\oplus 1)) = \mathbb{P}(C'\oplus 1)$. Denotemos $F\colon \mathbb{P}(C'\oplus 1) \to \mathbb{P}(C\oplus 1)$ la restricción de G a $\mathbb{P}(C'\oplus 1)$. Es claro que $G_*(1) = \mathrm{gr}(X'/X)\cdot Z$, de donde se concluye que $F_*(1) = \mathrm{gr}(X'/X)\cdot \mathbb{P}(C\oplus 1)$.

Por otra parte, $F^*(\mathscr{O}_{\mathbb{P}(C\oplus 1)}(1)) = \mathscr{O}_{\mathbb{P}(C'\oplus 1)}(1)$ y se tiene un diagrama conmutativo

$$\begin{array}{ccc} \mathbb{P}(C'\oplus 1) & \xrightarrow{F} & \mathbb{P}(C\oplus 1) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ Y' & \xrightarrow{f} & Y \end{array}$$

Si denotamos $x = c_1(\mathscr{O}_{\mathbb{P}(C\oplus 1)}(1))$, $x' = c_1(\mathscr{O}_{\mathbb{P}(C'\oplus 1)}(1))$, se tiene

$$f_*s(Y',X') = f_*\pi'_*(\frac{1}{1-x'}) = \pi_*F_*F^*(\frac{1}{1-x}) = \pi_*\left(F_*(1)\cdot\frac{1}{1-x}\right)$$

y se concluye porque $F_*(1) = \mathrm{gr}(X'/X)\cdot 1$. □

Multiplicidad a lo largo de una subvariedad.

Sea X una variedad irreducible e $Y \hookrightarrow X$ un subesquema cerrado irreducible. Sea $\mathscr{O}$ el anillo local de X en el punto genérico de Y y sea I el ideal de Y en $\mathscr{O}$. Consideremos el polinomio de Samuel $S(n) = l_{\mathscr{O}}(\mathscr{O}/I^n)$. Para $n >> 0$, $S(n)$ es un polinomio en n de grado $d = \dim\mathscr{O} = \mathrm{codim}(Y,X)$.

18. Definición: Llamaremos multiplicidad de X a lo largo de Y al número entero $m_Y(X) = \Delta^d S(n)$. Es decir, $S(n) = m_Y(X)\frac{n^d}{d!}+$ términos de grado $< d$. Si Y es íntegro, entonces $m_Y(X)$ es la multiplicidad del anillo $\mathscr{O}$.

Si I está generado por una sucesión regular, entonces la multiplicidad de X a lo largo de Y coincide con la longitud de $\mathscr{O}/I$.

19. Teorema: *Vía el isomorfismo $GK^0(Y) = \mathbb{Z}$, $[M] \mapsto l_{\mathscr{O}}(\mathscr{M}_g)$, se verifica que $s_0(Y,X) = m_Y(X)$. En otras palabras, $s_0(Y,X) = m_Y(X)\cdot Y_{red}$.*

Además, si $\widetilde{X} \xrightarrow{\pi} X$ es la explosión de X a lo largo de Y y $p\colon F \to Y$ es la fibra excepcional, entonces

$$m_Y(X) = (-1)^{d-1}F^d, \qquad d = \mathrm{codim}(Y,X)$$

siendo F^d el número de auto-intersección de F.

Demostración. Sea $X' = \mathrm{Spec}\mathscr{O}$ y $f\colon X' \to X$ el morfismo natural. Es claro que $s_0(Y,X) = s_0(Y',X')$, con $Y' = \mathrm{Spec}\mathscr{O}/I$, vía el isomorfismo $GK^0(Y) \to GK^0(Y') = \mathbb{Z}$. Por tanto, podemos suponer que X es el espectro de $\mathscr{O}$. Probemos que $m_Y(X) = (-1)^{d-1}F^d$. Por el

teorema de estabilidad 17.6.2, para $n >> 0$, $\mathscr{O}_{\tilde{X}}(n)$ es acíclico y $\pi_*\mathscr{O}_{\tilde{X}}(n) = I^n$. Por tanto,

$$\mathscr{O}/I^n = \pi_*[1-\mathscr{O}_{\tilde{X}}(n)] = \pi_*[1-(1-F)^n] = (-1)^{d-1}\pi_*(1\cdot F^d)\binom{n}{d}$$

donde la última igualdad se debe a que $\pi_*(1\cdot F^i) = 0$ para $0 < i < d$. Tomando característica se concluye.

Veamos ahora la igualdad $s_0(Y,X) = m_Y(X)$. Sea $q\colon \mathbb{P}(C\oplus 1) \to Y$, $i\colon F \hookrightarrow \mathbb{P}(C\oplus 1)$ la parte de infinito, y $j\colon F \hookrightarrow \widetilde{X}$. Denotemos $x = c_1(\mathscr{O}_{\mathbb{P}(C\oplus 1)}(1)) = F$. Entonces

$$s_0(Y,X) = q_*(x^d) = p_*(c_1(\mathscr{O}_F(1))^{d-1}) = (-1)^{d-1}\pi_*(1\cdot F^d)$$

donde la última igualdad se debe a que $c_1(\mathscr{O}_F(1)) = j^*c_1(\mathscr{O}_{\tilde{X}}(1)) = -j^*F$. Se concluye por la igualdad $m_Y(X) = (-1)^{d-1}F^d$. □

20. Observación: Si Y no es irreducible e $Y_1,\dots,Y_r$ son sus componentes irreducibles, supongamos que todas ellas son de la misma codimensión $=d$. Entonces

$$s_0(Y,X) = m_1\cdot(Y_1)_{\text{red}} + \cdots + m_r\cdot(Y_r)_{\text{red}}$$

siendo m_i la multiplicidad de X a lo largo de Y_i. Además, $s_0(Y,X) = (-1)^{d-1}p_*(F^d)$.

Singularidades de un morfismo.

Sea $f\colon F \to E$ un morfismo entre módulos localmente libres de rangos r,n respectivamente, sobre un esquema irreducible X.

21. Definición: Llamaremos locus singular de f, y lo denotaremos $\mathrm{Sing}(f)$, al conjunto de puntos $x\in X$ donde el morfismo $F\otimes k(x) \to E\otimes k(x)$ no es inyectivo. Equivalentemente, $\mathrm{Sing}(f)$ es el conjunto de puntos donde $\mathrm{Coker}\, f$ tiene dimensión mayor que $n-r$. Este conjunto es el cerrado definido por el ideal de Fitting $F_{n-r}(\mathrm{Coker}\, f)$. Por tanto, dotaremos a $\mathrm{Sing}(f)$ de estructura de esquema, definiéndolo como el subesquema cerrado definido por el ideal $\mathscr{J} = F_{n-r}(\mathrm{Coker}\, f)$:

$$\mathrm{Sing}(f) = \mathrm{Spec}(\mathscr{O}_X/\mathscr{J})$$

Es fácil ver que $\mathrm{Sing}(f)$ es un cerrado de codimensión menor o igual que $n-r+1$.

Si $F = L$ es de línea, el morfismo $L\to E$ equivale a dar un morfismo $\mathscr{O}_X \to E\otimes L^*$, es decir una sección s de $E\otimes L^*$. El locus singular del morfismo son los puntos donde la sección se anula, y lo denotamos $\mathrm{Sing}(s)$.

22. Teorema (Fórmula de Thom-Porteous): *Supongamos que X es Cohen-Macaulay. Si* $\mathrm{Sing}(f)$ *tiene codimensión $n-r+1$ o es vacío, entonces la clase de Chern $c_{n-r+1}(E-F)$ coincide con la clase de* $\mathrm{Sing}(f)$ *en $GK^{n-r+1}(X)$, es decir,*

$$c_{n-r+1}(E-F) = \sum n_i \cdot (Y_i)_{red}$$

siendo Y_i las componentes irreducibles de $\mathrm{Sing}(f)$ *y n_i la longitud de $\mathcal{O}_{\mathrm{Sing}(f)}$ en el punto genérico de Y_i.*

Demostración. Si el locus singular es vacío, entonces F es un subfibrado de E, luego E/F es un fibrado de rango $n-r$ y por tanto $c_{n-r+1}(E/F) = 0$.

Procedemos por inducción sobre el rango de F.

a) Rango de $F = 1$. Entonces $F = L$ es un haz de línea y el morfismo $L \to E$ equivale a dar una sección de s de $E \otimes L^*$. Se verifica que $c_n(E-L) = c_n(E \otimes L^*)$. En efecto, si $\alpha_1, \ldots, \alpha_n$ son las raíces de E y β es la raíz de L^*, se tiene la igualdad

$$s_n(\alpha_1+\beta, \ldots, \alpha_n+\beta) = \sum_{i=0}^{n} s_i(\alpha_1, \ldots, \alpha_n) \cdot \beta^{n-i}$$

de donde se deduce la igualdad de clases de Chern. Por el Teorema 17.4.2,

$$c_n(E \otimes L^*) = s_0^*[s(X)] = [\mathrm{Sing}(s)] \qquad (s_0 = \text{ sección cero})$$

donde la última igualdad se debe a que $s_0^{-1}(s(X)) = \mathrm{Sing}(s)$ y a que s corta sin tores a la sección cero (en efecto, por ser X Cohen-Macaulay y $\mathrm{Sing}(s)$ de codimensión n, la sucesión regular que define a $s(X)$ como subesquema de $E \otimes L^*$ sigue siendo regular al cortar con la sección nula).

b) Supongamos el teorema cierto si el rango de F es menor que r. Sea ahora F de rango r, y denotemos X_0 el cerrado de X formado por los puntos donde el morfismo $F \to E$ es nulo (es el cerrado definido por el ideal de Fitting $F_{n-1}(\mathrm{Coker}\, f)$). Evidentemente, $X_0 \subset \mathrm{Sing}(f)$. Demostremos la fórmula de Thom-Porteous suponiendo que X_0 es de codimensión estrictamente superior a la de $\mathrm{Sing}(f)$. Podemos suponer por tanto que X_0 es vacío, sin más que pasar a su abierto complementario. Sea $\pi\colon \mathbb{P}(F) \to X$ y $T = \mathcal{O}_{\mathbb{P}(F)}(-1)$ el subfibrado de línea tautológico de π^*F. Por ser X_0 vacío, el locus singular del morfismo $T \to \pi^*E$ (composición de $T \hookrightarrow \pi^*F \to \pi^*E$) es un cerrado de codimensión mayor que $n-r+1$, luego podemos suponer que es vacío. Es decir, podemos suponer que T es un subfibrado de π^*E. Denotemos $F' = \pi^*F/T$, $E' = \pi^*E/T$ y $\bar{f}\colon F' \to E'$ el morfismo inducido. Es claro que el locus singular de $\pi^*F \to \pi^*E$ coincide con el locus singular de $\bar{f}$. Por inducción sobre el rango,

$$\pi^* c_{n-r+1}(E-F) = c_{n-r+1}(E'-F') = [\mathrm{Sing}(\bar{f})] = \pi^*[\mathrm{Sing}(f)]$$

donde la última igualdad se debe a la estabilidad de los ideales de Fitting por cambio de base. Como π^* es inyectivo se concluye.

c) En general, sea $H = \underline{\mathrm{Hom}}(F,E)$ el fibrado de homomorfismos de F en E, $\pi: H \to X$ el morfismo estructural y $u: \pi^*F \to \pi^*E$ el morfismo universal. El morfismo f define una sección $s: X \to H$ de π, tal que $s^*(u) = f$. El teorema es cierto para el morfismo universal, por b), pues su locus singular tiene la codimensión debida y H_0 es de codimensión estrictamente mayor (exactamente rn). Por tanto,

$$c_{n-r+1}(\pi^*E - \pi^*F) = [\mathrm{Sing}(u)]$$

Tomando imagen inversa por s, obtenemos que $c_{n-r+1}(E-F) = s^*[\mathrm{Sing}(u)]$. Para concluir, basta ver que $s^*[\mathrm{Sing}(u)] = [\mathrm{Sing}(f)]$. Como $s^*(u) = f$ y los ideales de Fitting cambian de base, se obtiene que $s^{-1}(\mathrm{Sing}(u)) = \mathrm{Sing}(f)$; para terminar, basta ver que la sección s corta sin tores a $\mathrm{Sing}(u)$. En primer lugar, $\mathrm{Sing}(u)$ es Cohen-Macaulay (esto no lo demostraremos, puede verse en [Laksov, D: The arithmetic Cohen-Macaulay character of Schubert schemes. Acta Mathematica 129 (1972), 1-9]); como $\mathrm{Sing}(f)$ tiene codimensión rn en $\mathrm{Sing}(u)$, la sucesión regular que define localmente a $s(X)$ como subesquema de H sigue siendo regular al especializar a $\mathrm{Sing}(u)$, con lo que se concluye. □

23. Observación: Si X no es Cohen-Macaulay y el locus de los puntos donde el morfismo $F \to E$ tiene rango menor que $r-1$ es de codimensión estrictamente mayor que $n-r+1$, entonces la fórmula de Thom-Porteous sigue siendo válida sustituyendo n_i por la multiplicidad de X a lo largo de Y_i.

24. Ejemplo: *Singularidades de una ecuación diferencial.* Una ecuación diferencial sobre X es un morfismo $D: \mathscr{L} \to T_X$, donde $\mathscr{L}$ es un haz de línea. Localmente, equivale a dar un campo $D = f_1 \frac{\partial}{\partial x_1} + \cdots + f_n \frac{\partial}{\partial x_n}$. Las singularidades del morfismo vienen dadas, localmente, por los ceros de las funciones $f_1, \ldots, f_n$. Si el locus singular de D son puntos aislados, la fórmula de Thom-Porteous dice que

$$c_n(T_X - \mathscr{L}) = \sum n_i \cdot p_i$$

siendo p_i los puntos singulares de la ecuación diferencial y n_i la longitud de $\mathscr{O}_{p_i}/(f_1, \ldots, f_n)$. Esta es la fórmula de Baum-Bott. En el caso de que X sea una superficie, es el invariante de Zeuthen-Segre. Si X es la recta proyectiva compleja (es decir, la esfera) y $\mathscr{L}$ es trivial, la fórmula dice que el número de puntos singulares de un campo en una esfera es 2.

25. Ejemplo: *Construcción geométrica de las clases de Chern.* Sea E un fibrado vectorial de rango n sobre una variedad quasi-proyectiva X sobre un cuerpo algebraicamente cerrado.

Existe un haz de línea $\mathscr{L}$ y n secciones $s_1,\dots,s_n$ de $E\otimes\mathscr{L}$ tales que:
- Para cada $1\le r\le n$, el morfismo $f_r\colon \mathscr{O}_X^r\to E\otimes\mathscr{L}$ definido por $s_1,\dots,s_r$ tiene locus singular de codimensión $n-r+1$ o vacío.

Por la fórmula de Thom-Porteous (y su observación posterior en el caso no Cohen-Macaulay),

$$c_{n-r+1}(E\otimes\mathscr{L})=[\mathrm{Sing}(f_r)]$$

Las clases de Chern de E están determinadas por las de $E\otimes\mathscr{L}$ y por $c_1(\mathscr{L})$ por la fórmula:

$$c_r(E)=\sum_{i=0}^{r}(-1)^{r-i}\binom{n-i}{r-i}c_1(\mathscr{L})^{r-i}c_i(E\otimes\mathscr{L})$$

17.6.3. Riemann-Roch

Veamos en qué se traduce el teorema de Riemann-Roch en el caso de las curvas, las superficies y las hipersuperficies.

Curvas

Sea C una curva completa y lisa sobre k, y $\pi\colon C\to\mathrm{Spec}\,k$ la proyección estructural. Si K es el divisor canónico de C, entonces $T_C=\mathscr{L}_{-K}$; luego

$$\mathrm{Td}(\mathscr{L}_{-K})=1-\frac{K}{2},\ \text{porque } K^2=K^3=\ldots=0$$

Dado un haz de línea $\mathscr{L}_D$, entonces $c_1(\mathscr{L}_D)=D$ y $\mathrm{ch}(\mathscr{L}_D)=e^D=1+D$. El teorema de Riemann-Roch dice

$$\begin{aligned}&\pi_*(\mathrm{ch}(\mathscr{L}_D)\cdot\mathrm{Td}(T_\pi))=\mathrm{ch}(\pi_!(\mathscr{L}_D))\\&\pi_*((1+D)\cdot(1-\tfrac{K}{2}))=\mathrm{ch}(\chi(\mathscr{L}_D))=\chi(\mathscr{L}_D)\\&\pi_*(1+D-\tfrac{K}{2})=\mathrm{gr}\,D-\tfrac{\mathrm{gr}\,K}{2}=\chi(\mathscr{L}_D)\end{aligned}$$

Todo módulo coherente $\mathscr{M}$ es equivalente, en teoría K, a $n-1+\Lambda^n\mathscr{M}$, donde n es el rango de $\mathscr{M}$. Entonces $c_1(\mathscr{M})=c_1(\Lambda^n\mathscr{M})$ y $\mathrm{ch}(\mathscr{M})=n+c_1(\Lambda^n\mathscr{M})$ y el teorema de Riemann-Roch dice que $\chi(\mathscr{M})=(\mathrm{rg}\,\mathscr{M})(1-g)+\mathrm{gr}\,c_1(\mathscr{M})$, donde $g=h^0(\mathscr{L}_K)=h^1(\mathscr{O}_X)$.

Hipersuperficies

Sea $i\colon Y\hookrightarrow X$ una inmersión cerrada de codimensión 1 entre k-esquemas lisos y proyectivos.

Sean K_X, K_Y los divisores canónicos de X e Y respectivamente. Aplicando el teorema de Riemann-Roch a $\mathcal{O}_Y$ se obtiene

$$i_*(\mathrm{Td}(T_Y)) = \mathrm{ch}(\mathcal{O}_Y)\cdot \mathrm{Td}(T_X) = \mathrm{ch}(1-\mathscr{L}_{-Y})\mathrm{Td}(T_X)$$
$$(Y - \tfrac{i_*K_Y}{2} + \ldots) = (1-e^{-Y})\cdot \mathrm{Td}(T_X) = (Y - \tfrac{Y^2}{2} + \ldots)\cdot(1 - \tfrac{K}{2} + \ldots)$$

Igualando las partes homogéneas de grado 2 obtenemos:

$$i_*(K_Y) = Y\cdot(K_X + Y)$$

que es la fórmula de residuos obtenida en la teoría de la dualidad. En particular, si X es una superficie lisa e Y una curva lisa de género g, tendremos que

$$(2g-2) = Y\cdot(K_X + Y)$$

Superficies

Sea S una superficie lisa y proyectiva sobre k, y $\pi\colon S \to \mathrm{Spec}\, k$ el morfismo estructural. Sea K el divisor canónico de S, $\mathscr{L}_K = \Omega^2_{S/k}$. Entonces $c_1(\Omega_{S/k}) = K$. Si escribimos $T_S = \mathscr{L}_{\alpha_1} \oplus \mathscr{L}_{\alpha_2}$, entonces $\mathrm{Td}(T_S) = (1+\alpha_1+\frac{\alpha_1^2}{12})\cdot(1+\alpha_2+\frac{\alpha_2^2}{12}) = 1 + \frac{\alpha_1+\alpha_2}{2} + \frac{(\alpha_1+\alpha_2)^2+\alpha_1\cdot\alpha_2}{12}$, luego

$$\mathrm{Td}(T_S) = 1 - \frac{K}{2} + \frac{K^2 + c_2(T_S)}{12}$$

El grado de $c_2(T_S)$ se denomina característica topológica de S y se denota χ_{top}. Sabemos que coincide con la auto-intersección de la diagonal en $S\times S$ y con los ceros de un campo tangente.

Si $\mathscr{L}_D$ es un haz de línea, $\mathrm{ch}(\mathscr{L}_D) = 1 + D + \frac{D^2}{2}$, y el teorema de Riemann-Roch afirma:

$$\chi(\mathscr{L}_D) = \frac{D^2}{2} - \frac{K\cdot D}{2} + \frac{K^2 + \chi_{\mathrm{top}}}{12}$$

En particular, se obtiene la igualdad de Noether: $\chi(\mathcal{O}_S) = \frac{K^2+\chi_{\mathrm{top}}}{12}$.

Si $\mathscr{M}$ es un módulo coherente de rango r sobre S, se verifica:

$$\mathrm{ch}(\mathscr{M}) = r + c_1(\mathscr{M}) + \frac{c_1(\mathscr{M})^2 - 2c_2(\mathscr{M})}{2}$$

y por Riemann-Roch

$$\chi(\mathscr{M}) = r(\frac{K^2+\chi_{\mathrm{top}}}{12}) - \frac{K\cdot c_1(\mathscr{M})}{2} + \frac{c_1(\mathscr{M})^2 - 2\,\mathrm{gr}\, c_2(\mathscr{M})}{2}$$

26. Proposición: *Sea $\pi\colon S' \to S$ el morfismo de explosión de la superficie S lisa proyectiva en un punto racional x. Se cumple que*

1. $\pi^{-1}(x)\cdot\pi^{-1}(x) = -1$
2. $\pi^*(C)\cdot\pi^*C = C\cdot C'$, *para cualesquiera curvas C y C'.*
3. $\pi^*(C)\cdot\pi^{-1}(x) = 0$, *para toda curva C.*
4. $\operatorname{Pic}S' = \operatorname{Pic}S \oplus \mathbb{Z}$.

Demostración. 1. lo sabemos por 17.6.3. 2. Sustituyendo C y C' por divisores de S, linealmente equivalentes a C y C', podemos reducirnos (por linealidad) al caso en el que C y C' son curvas irreducibles que no pasan por x y no tienen componentes comunes. En tal caso $C\cdot C'$ y $\pi^*C\cdot\pi^*C'$ coincide con el número de puntos de corte (contando multiplicidades) de $C = \pi^{-1}C$ y $C' = \pi^{-1}C'$. 3. Puede suponerse que C no pasa por x y en tal caso $C = \pi^{-1}C$ es disjunto con $\pi^{-1}x$ y se concluye. 4. Tenemos la sucesión exacta

$$\mathbb{Z}\cdot\pi^{-1}(x) \xrightarrow{i} \operatorname{Pic}S' \xrightarrow{j} \operatorname{Pic}(S'-\pi^{-1}(x)) = \operatorname{Pic}(S-x) = \operatorname{Pic}S \to 0$$

Si $n\cdot\pi^{-1}(x) = 0$ en $\operatorname{Pic}S$ entonces $0 = (n\cdot\pi^{-1}(x))\cdot(n\cdot\pi^{-1}(x)) = -n^2$ y $n = 0$. Luego i es inyectivo. El morfismo π^* es una sección de j y hemos terminado. □

27. Corolario: *Sea $\pi\colon S' \to S$ el morfismo de explosión de la superficie S lisa proyectiva en un punto racional x. Se cumple que*

$$K_{S'} = K_S + \pi^{-1}(x)$$

Demostración. Por la proposición anterior, como los haces canónicos en $S'-\pi^{-1}(x)$ y $S-x$ son los mismos, $K_{S'} = K_S + n\pi^{-1}(x)$. Para determinar n, podemos usar la fórmula de adjunción $-2 = \pi^{-1}(x)\cdot(K_{S'} + \pi^{-1}(x))$, luego $-2 = -n-1$ y $n = 1$.

□

28. Corolario: *Sea $\pi\colon S' \to S$ el morfismo de explosión de la superficie S lisa proyectiva en un punto racional x, C una curva irreducible de multiplicidad r en x y C' la explosión de C en x. Se cumple que $\pi^*C = C' + r\pi^{-1}(x)$.*

Demostración. La multiplicidad de una curva en un punto coincide con la multiplicidad de corte de la curva explotada con la fibra excepcional. Por tanto, $r = C'\cdot\pi^{-1}(x)$ y $\pi^*C = C' + r\pi^{-1}(x)$. □

Como aplicación del teorema de Riemann-Roch en superficies probemos el teorema del índice de Hodge y el criterio de amplitud de Nakai, siguiendo a Hartshorne.

Diremos que un divisor es amplio si el haz de línea asociado es amplio. Si H es un divisor amplio entonces nH es un divisor muy amplio para $n >> 0$. Por tanto, nH define una inmersión cerrada de S en un espacio proyectivo. Dada una curva D en S, $D \cdot nH$ coincide con el grado de la curva en el espacio proyectivo. Por tanto, $D \cdot nH > 0$ y $C \cdot H > 0$. Dado un divisor D, $D \cdot H$ va a representar el papel asignado al grado de un divisor en la teoría de curvas.

29. Lema : *Sea H un divisor amplio de la superficie S. Entonces existe un número natural n_0 tal que para todo divisor D, si $D \cdot H > n_0$ entonces $H^2(S, \mathscr{L}_D) = 0$.*

Demostración. Por dualidad $h^2(S, \mathscr{L}_D) = h^0(S, \mathscr{L}_{K-D})$. Si $h^0(S, \mathscr{L}_{K-D}) > 0$ entonces $K - D$ es equivalente a un divisor efectivo y $(K - D) \cdot H > 0$. Luego $K \cdot H > D \cdot H$. Por tanto, basta tomar $n_0 = K \cdot H$. □

30. Corolario : *Si H es un divisor amplio de S y D es un divisor tal que $D \cdot H > 0$ y $D^2 > 0$, entonces nD es efectivo para todo $n >> 0$.*

Demostración. Por el lema anterior, $H^2(S, \mathscr{L}_{nD}) = 0$ para todo $n >> 0$. Por Riemann-Roch, para todo $n >> 0$

$$h^0(\mathscr{L}_{nD}) \geq \chi(\mathscr{L}_{nD}) = \frac{n^2 D^2}{2} - \frac{nK \cdot D}{2} + \frac{K^2 + \chi_{\text{top}}}{12} > 0$$

□

31. Definición : Diremos que un divisor D en S es numéricamente equivalente a cero, escrito $D \equiv 0$, si $D \cdot E = 0$ para todo divisor E.

32. Teorema del índice de Hodge: *Sea H un divisor amplio en la superficie S. Si $D \not\equiv 0$ es un divisor tal que $D \cdot H = 0$ entonces $D^2 < 0$.*

Demostración. Supongamos que $D^2 > 0$. El divisor $H' = D + nH$ es linealmente equivalente a un divisor efectivo y es amplio para $n >> 0$. $D \cdot H' = D^2 > 0$, luego mD es efectivo para $m >> 0$, por el corolario anterior. Pero entonces $mD \cdot H > 0$, contradicción.

Supongamos que $D^2 = 0$. Sea E un divisor tal que $D \cdot E > 0$. Sustituyendo E por $E' = (H^2)E - (E \cdot H)H$ podemos suponer que $E \cdot H = 0$. Sea $D' = nD + E$. $D'^2 = 2n(D \cdot E) + E^2 > 0$ para $n \in \mathbb{Z}$ conveniente y $D' \cdot H = 0$. Lo que es contradictorio, por el párrafo anterior. □

La intersección de divisores define en $\operatorname{Pic} S \otimes_{\mathbb{Z}} \mathbb{R}$ una métrica simétrica, de modo que los divisores numéricamente equivalentes a cero pertenecen a su radical. Denotemos a $\operatorname{Pic} S$ cociente por los divisores numéricamente equivalentes a cero $\operatorname{Num} S$. El teorema de Nerón-Severi afirma que $\operatorname{Num} S$ es un $\mathbb{Z}$-módulo libre finito generado. El

teorema del índice de Hodge nos dice que la métrica simétrica definida en $\mathrm{Num}\, S \otimes_{\mathbb{Z}} \mathbb{R}$ es diagonalizable, con un único 1 en la diagonal y todos los demás -1.

33. Criterio de amplitud de Nakai-Moishezon: *Un divisor en una superficie es amplio si y sólo si la autointersección consigo mismo y la intersección con toda curva irreducible es estrictamente positiva.*

Demostración. Si D es amplio sabemos que verifica el criterio.

Recíprocamente, supongamos que $D^2 > 0$ y que $D \cdot C > 0$ para toda curva irreducible C. Sea H un divisor muy amplio, entonces H es equivalente a una curva y $D \cdot H > 0$. Por 17.6.30, para $n >> 0$, nD es efectivo. Sustituyendo D por nD, podemos suponer que $D = \sum_i n_i C_i$, con $n_i > 0$ y C_i curvas reducidas.

Veamos que la restricción de $\mathscr{L}_D$ a D es amplio en D. Considerando el morfismo finito $\coprod C_i \to D$ y 13.12.5, basta ver que la restricción de $\mathscr{L}_D$ a cada C_i es amplio. Considerando el morfismo de desingularización $f : \tilde{C}_i \to C_i$ y 13.12.5, basta ver que $f^*(\mathscr{L}_D \otimes_{\mathscr{O}_S} \mathscr{O}_{C_i}$ es amplio en $\tilde{C}_i$. Ahora bien, $f^*(\mathscr{L}_D \otimes_{\mathscr{O}_S} \mathscr{O}_{C_i}$ es un haz de línea de grado $D \cdot C_i > 0$, luego amplio.

Veamos que $\mathscr{L}_D^n$ está generado por sus secciones globales, para $n >> 0$. Consideremos la sucesión exacta

$$0 \to \mathscr{L}_{-D} \to \mathscr{O}_S \to \mathscr{O}_D \to 0$$

tensando por $\mathscr{L}_{nD}$ obtenemos las sucesiones exactas largas de cohomología

$$H^0(S, \mathscr{L}_{nD}) \to H^0(S, \mathscr{L}_{nD} \otimes \mathscr{O}_D) \to H^1(S, \mathscr{L}_{(n-1)D} \to H^1(S, \mathscr{L}_{nD} \to H^1(S, \mathscr{L}_{nD} \otimes \mathscr{O}_D)$$

Como la restricción de $\mathscr{L}_D$ a D es amplio, por 13.12.3, $H^1(S, \mathscr{L}_{nD} \otimes \mathscr{O}_D) = 0$ para todo $n >> 0$. Luego, $h^1(\mathscr{L}_{nD}) \leq h^1(\mathscr{L}_{(n-1)D}$ y dado que son espacios vectoriales de dimensión finita, para todo $n >> 0$, $h^1(\mathscr{L}_{nD}) = h^1(\mathscr{L}_{(n-1)D}$. Por tanto, el morfismo

$$H^0(S, \mathscr{L}_{nD}) \to H^0(S, \mathscr{L}_{nD} \otimes \mathscr{O}_D)$$

es epiyectivo, para todo $n >> 0$.

Así pues, si consideramos un n de modo que el morfismo anterior sea epimorfismo y nD sea muy amplio sobre D, tenemos que $\mathscr{L}_{nD}$ define un morfismo $\phi : S \to \mathbb{P}^N$ (que es una inmersión cerrada al restringirse a D). El morfismo ϕ es de fibras finitas ya que si la fibra de un punto contiene una curva C, si consideramos un hiperplano H que no pase por el punto, tendremos que $(nD) \cdot C = (H \cap S) \cdot C = 0$, que contradice la hipótesis $D \cdot C = 0$. Por el Main Theorem de Zariski, ϕ es un morfismo finito y por 13.12.3 nD es amplio.

□

Capítulo 18

Teoría del descenso fielmente plano

18.1. Introducción al problema del descenso

El problema que estudia la teoría del descenso fielmente plano es el siguiente: dado un morfismo de esquemas

$$f : X \to Y$$

fielmente plano (plano y epiyectivo) de tipo finito y dada una estructura M sobre X se trata de dar condiciones para la existencia de una estructura N sobre Y tal que $f^*N = M$, así como la clasificación de dichas estructuras. A N se le denomina descenso de M.

1. Ejemplo: 1. Sea $X = \coprod_{i=1}^n U_i$ un recubrimiento por abiertos $U_i = \operatorname{Spec} A_i$ afines de Y y M el espacio proyectivo $\mathbb{P}^n_X$, entonces N es cualquier fibrado proyectivo sobre Y, de rango n, trivializado por el recubrimiento X, es decir, $N_{|U_i} = \mathbb{P}^n \times U_i$

2. En las mismas condiciones sobre X e Y, sea $M = \mathscr{O}_X^n$ como haz de $\mathscr{O}_X$-módulos. Un descenso N es un haz de $\mathscr{O}_Y$-módulos coherente localmente libre de rango n, que trivializa en el recubrimiento, es decir, $N_{|U_i} = \mathscr{O}_{U_i}^n$.

3. Si $X = \operatorname{Spec} B \to \operatorname{Spec} A = Y$ es un morfismo fielmente plano y M es un B-módulo, un descenso es un A-módulo N tal que $M = N \otimes_A B$.

4. Si $k \hookrightarrow K$ es una extensión finita de Galois, $X = \operatorname{Spec} K$, $Y = \operatorname{Spec} k$ y M es la K-álgebra trivial $K \times \overset{n}{\ldots} \times K$, entonces N es cualquier k-álgebra finita A de dimensión n trivializada por K, $A \otimes_k K = K^n$ (por ejemplo, las subextensiones de K de dimensión n). El estudio de este caso es la teoría de Galois.

Si los morfismos de anillos fielmente planos se entienden (por paso a los espectros) como recubrimientos por abiertos de un espacio topológico y los módulos como haces,

el problema de la teoría del descenso es dar las condiciones que ha de verificar un haz en un recubrimiento para descender a un haz global. Es decir, la teoría de descenso así planteada es el problema de "recollement".

La teoría del descenso fielmente plano, como teoría que clasifica diversas estructuras, tiene aplicaciones sorprendentemente variadas. Como veremos el teorema de Galois, el teorema 90 de Hilbert, el teorema 90 aditivo, la teoría de Kummer y la de Artin-Schreier para extensiones cíclicas, el teorema de Fröbenius para la clasificación de las álgebras de Azumaya sobre R, la clasificación cohomológica de los haces de línea, etc., son aplicaciones de la teoría del descenso.

Podríamos haber desarrollado la teoría del descenso en la categoría de esquemas afines (o anillos), donde las estructuras consideradas fueran los módulos (y A-álgebras). Sin embargo la hemos desarrollado, con toda generalidad, en la categoría de esquemas, donde las estructuras consideradas serán haces en la topología fielmente plana. Las dos exposiciones son equivalentes formalmente. Hemos procurado adoptar unas notaciones que reflejen, lo mejor posible, esta equivalencia formal.

18.2. Notaciones

Fijado un morfismo de esquemas $f: X \to Y$ diremos que X es un Y-esquema. Dados dos Y-esquemas $f: X \to Y$ y $f': X' \to Y$, diremos que $g: X \to X'$ es un morfismo de Y-esquemas si es un morfismo de esquemas que verifica $f' \circ g = f$. Denotaremos por $\mathscr{C}_Y$ la categoría de los Y-esquemas, donde los morfismos son morfismos de Y-esquemas. Dado un funtor F (que siempre supondremos contravariante) sobre $\mathscr{C}_Y$ y un morfismo $f: X \to Y$ se define el funtor f^*F en $\mathscr{C}_X$ por la igualdad $f^*F(Z) := F(Z)$, siendo Z un X-esquema y, por tanto, Y-esquema vía f. Igualmente, dado un funtor G sobre $\mathscr{C}_X$ se define f_*G sobre Y por la igualdad $(f_*G)(Z') := G(Z' \times_Y X) = G(f^*Z)$. Seguiremos las notaciones, motivadas por la teoría de módulos, $f^*F = F \otimes_Y X$ y $f_*G = G$ como funtor sobre $\mathscr{C}_Y$ (es decir, G sobre $\mathscr{C}_Y$ entenderemos que es la imagen directa de G sobre $\mathscr{C}_X$ por f).

Existe un morfismo natural $F \to F \otimes_{\underline{Y}} X$ (donde hemos subrayado la Y para indicar que estamos considerando $F \otimes_Y X$ como funtor sobre Y): Dado un Y-esquema Z, denotemos $\pi: Z \times_Y X \to Z$ la proyección natural. El morfismo $F(Z) \xrightarrow{\pi^*} F(Z \times_Y X) = (F \otimes_{\underline{Y}} X)(Z)$ es el morfismo natural buscado.

También existe un morfismo natural $G \otimes_Y X \to G$ (donde el funtor G de la izquierda de la flecha lo estamos considerando como funtor sobre Y): Dado un X-esquema T, consideremos el morfismo natural $i: T \to T \times_Y X$. El morfismo $(G \otimes_Y X)(T) = G(T \times_Y X) \xrightarrow{i^*} G(T)$ es el morfismo natural buscado.

1. Proposición: *La imagen directa e inversa son adjuntas entre sí, es decir,*

$$\mathrm{Hom}_Y(F, f_*G) = \mathrm{Hom}_X(f^*F, G)$$

Demostración. Dado un morfismo $F \to f_*G$, si tomamos f^* obtenemos $f^*F \to f^*f_*G$, que compuesto con $f^*f_*G \to G$ define un morfismo $f_*F \to G$. Recíprocamente, dado un morfismo $f^*F \to G$, si tomamos f_* obtenemos $f_*f^*F \to f_*G$, que compuesto con $F \to f_*f^*F$ define un morfismo $F \to f_*G$.

□

2. Ejemplo: Un módulo cuasicoherente $\mathscr{N}$ sobre Y define un funtor $\mathscr{N}(X) = \Gamma(X, f^*\mathscr{N})$. Se verifica que la imagen inversa del funtor asociado a $\mathscr{N}$ es el funtor asociado a la imagen inversa del módulo cuasicoherente $\mathscr{N}$. Supongamos que $Y = \mathrm{Spec}A$ es afín y que $\mathscr{C}_Y$ es la categoría de los esquemas afines sobre Y. Se verifica que los módulos cuasicoherentes sobre Y se corresponden con los A-módulos. Escribamos $f\colon \mathrm{Spec}B \to \mathrm{Spec}A$. En esta situación, sea un A-módulo N y un B-módulo M. Se verifica que $f^*N = N \otimes_A B$, $f_*M = M$, y los morfismos usuales $N \to N \otimes_A B$, $M \otimes_A B \to M$ son los morfismos antes definidos.

Éste es el ejemplo que guía el capítulo. Para una lectura más fluida del capítulo puede suponerse siempre que estamos en situación afín y que los funtores son los módulos.

Denotaremos $d_i\colon X \times \overset{n}{\cdots} \times X \to X \times \overset{n-1}{\cdots} \times X$ a la proyección consistente en "olvidar" la componente i-ésima.

18.3. Haces en la topología fielmente plana

Diremos que un funtor F sobre $\mathscr{C}_Y$ es haz para la topología fielmente plana si:

1. F es haz para la topología de Zariski, es decir, F sobre los abiertos de cada Y-esquema X es un haz en X.

2. Para todo morfismo fielmente plano de tipo finito $T \to S$ la sucesión

$$F(S) \to F(T) \underset{d_2^*}{\overset{d_1^*}{\rightrightarrows}} F(T \times_S T)$$

es exacta.

Como F es haz en la topología de Zariski, la exactitud de esta sucesión es una cuestión local en S, luego podremos suponer en la definición de haz que S es afín. Además, puede comprobarse también que se puede suponer que T es afín.

Denotemos por $\pi: S \to Y$ al morfismo estructural y para cada morfismo fielmente plano de tipo finito $T \to S$ consideremos la sucesión

$$\pi^*F \to \pi^*F \otimes_{\underline{S}} T \rightrightarrows \pi^*F \otimes_{\underline{S}} T \otimes_{\underline{S}} T \qquad (*)$$

F será haz si tomando secciones sobre S la sucesión $(*)$ es exacta.

1. Lema: *Sea $A \to B$ un morfismo de anillos fielmente plano y M un A-módulo. La sucesión*

$$M \to M \underset{A}{\otimes} B \underset{d_2}{\overset{d_1}{\rightrightarrows}} M \underset{A}{\otimes} B \underset{A}{\otimes} B \underset{d_3}{\overset{d_1}{\overset{d_2}{\rightrightarrows}}} M \underset{A}{\otimes} B \underset{A}{\otimes} B \underset{A}{\otimes} B \cdots$$

es exacta, es decir, si definimos $d_i(m \otimes b_1 \otimes \cdots \otimes b_n) = m \otimes b_1 \otimes \cdots \otimes 1 \otimes b_i \otimes \cdots \otimes b_n$ y $d = \sum(-1)^{i+1} d_i$, entonces $\operatorname{Ker} d = \operatorname{Im} d$.

Demostración. Es fácil comprobar que $d^2 = 0$, luego $\operatorname{Im} d \subseteq \operatorname{Ker} d$. Nos falta probar la igualdad. Por cambio de base fielmente plano $(\underset{A}{\otimes} B)$ podemos suponer que el morfismo $A \to B$ tiene retracto $s: B \to A$. Para todo n, sea $s(m \otimes b_1 \otimes \cdots \otimes b_n) := s(b_1)m \otimes (b_2 \otimes \cdots \otimes b_n)$. Se verifica que $s \circ d + d \circ s = Id$. Por tanto $\operatorname{Ker} d \subseteq \operatorname{Im} d$ y concluimos la igualdad.

□

2. Teorema: *Todo módulo cuasicoherente $\mathscr{M}$ sobre Y es un haz para la topología fielmente plana.*

Demostración. Es bien conocido que $\mathscr{M}$ es un haz para la topología de Zariski. Además la imagen inversa de un módulo cuasicoherente es cuasicoherente. Por tanto, sólo tenemos que probar, dado un morfismo fielmente plano de tipo finito $T = \operatorname{Spec} B \xrightarrow{d} Y = \operatorname{Spec} A$, la exactitud de la sucesión,

$$M \to M \otimes_A B \rightrightarrows M \otimes_A B \otimes_A B$$

Por el lema anterior concluimos.

□

3. Teorema: *El funtor de puntos $X^{\cdot} := \operatorname{Hom}_Y(-, X)$ asociado a un Y-esquema X es un haz para la topología fielmente plana.*

Demostración. En primer lugar es bien conocido, que el funtor de puntos de un esquema es un haz para la topología de Zariski. Dado un morfismo $f: S \to Y$ se verifica que $f^*X^{\cdot} = (X \times_Y S)^{\cdot}$. Así pues, sólo tenemos que comprobar, dado un morfismo fielmente plano de tipo finito $T = \operatorname{Spec} B \xrightarrow{d} Y = \operatorname{Spec} A$, la exactitud de la sucesión

$$\operatorname{Hom}_Y(Y, X) \xrightarrow{d^*} \operatorname{Hom}_Y(T, X) \rightrightarrows \operatorname{Hom}_Y(T \times_Y T, X)$$

Si X es afín, la exactitud de la sucesión requerida se deduce de la exactitud de

$$A \to B \rightrightarrows B \underset{A}{\otimes} B$$

que hemos demostrado en el lema anterior.

Observemos en primer lugar que la sucesión

$$T \times_Y T \overset{d_1}{\underset{d_2}{\rightrightarrows}} T \xrightarrow{d} Y$$

es topológicamente exacta, es decir, Y es el conúcleo topológico de $T \times_Y T \rightrightarrows T$: Obviamente $d_1 \circ d = d_2 \circ d$. Dados $y \in Y$ y $t, t' \in d^{-1}(y)$, sea $z \in t \times_Y t'$, entonces $d_1(z) = t'$ y $d_2(z) = t$. Por último, $V \subset Y$ es un abierto si y sólo si $d^{-1}(V)$ es abierto ya que d es una aplicación abierta por 7.7.19, y $d(d^{-1}(V)) = V$.

Veamos ahora la inyectividad de d^*. Dados dos morfismos $g, g' : Y \to X$ tales que $g \circ d = g' \circ d$, entonces $g = g'$ como morfismo topológico. Para ver que $g = g'$ bastará hacerlo localmente en X, luego podemos suponer que X es afín y concluimos.

Para terminar, nos falta probar que dado un morfismo $f : T \to X$ tal que $f \circ d_1 = f \circ d_2$, entonces existe un morfismo $g : Y \to X$ tal que $f = g \circ d$. Gráficamente

$$\begin{array}{ccccc} T \times_Y T & \overset{d_1}{\underset{d_2}{\rightrightarrows}} & T & \xrightarrow{d} & Y \\ & & \downarrow f & \swarrow g & \\ & & X & & \end{array}$$

Sea pues, un morfismo $f : T \to X$ tal que $f \circ d_1 = f \circ d_2$. Sea $g : Y \to X$ la única aplicación continua tal que $f = g \circ d$.

Dado un punto $y \in Y$, existen un abierto básico U_y que contiene a y y un abierto afín $U \subset X$ que contiene a $f(U_y)$. Considerando los abiertos afines $U_y, d^{-1}(U_y), U$ sabemos que g restringida a U_y es un morfismo de esquemas. Por tanto, $g : Y \to X$ es un morfismo de esquemas.

□

4. Teorema de descenso de homomorfismos: *Sean N, N' dos haces en $\mathscr{C}_Y$ para la topología fielmente plana. El funtor de homomorfismos $Hom_Y(N, N')$ es un haz, es decir, la sucesión natural*

$$\mathrm{Hom}_Y(N, N') \to \mathrm{Hom}_X(N \otimes_Y X, N' \otimes_Y X) \overset{d_1^*}{\underset{d_2^*}{\rightrightarrows}} \mathrm{Hom}_{X \times_Y X}(N \otimes_Y X \otimes_Y X, N' \otimes_Y X \otimes_Y X)$$

es exacta, donde los morfismos asignan a cada morfismo el morfismo cambiado de base.

Demostración. Dado un morfismo $f: N \otimes_Y X \to N' \otimes_Y X$ tal que $d_1^* f = d_2^* f$ existe un único $f': N \to N'$ tal que hace el diagrama

$$\begin{array}{ccccc} N & \longrightarrow & N \otimes_{\underline{Y}} X & \overset{d_1}{\underset{d_2}{\rightrightarrows}} & N \otimes_{\underline{Y}} X \otimes_{\underline{Y}} X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle d_1^* f}\ \downarrow{\scriptstyle d_2^* f} \\ N' & \longrightarrow & N' \otimes_{\underline{Y}} X & \overset{d_1}{\underset{d_2}{\rightrightarrows}} & N' \otimes_{\underline{Y}} X \otimes_{\underline{Y}} X \end{array}$$

conmutativo. Cambiando de base por $d: X \to Y$ el cuadrado de la izquierda del diagrama anterior

$$\begin{array}{ccccc} N \otimes_Y X & \longrightarrow & (N \otimes_{\underline{Y}} X) \otimes_Y X & \longrightarrow & N \otimes_Y X \\ \downarrow{\scriptstyle d^* f'} & & \downarrow{\scriptstyle d^* f} & & \downarrow{\scriptstyle f} \\ N' \otimes_Y X & \longrightarrow & (N' \otimes_{\underline{Y}} X) \otimes_Y X & \longrightarrow & N' \otimes_Y X \end{array}$$

obtenemos fácilmente que $d^* f' = f$.

Con todo es sencillo concluir.

□

18.4. Dato de construcción, condiciones de descenso.

Como sabemos de la construcción de haces de módulos, construir un haz N en Y a partir de su construcción local ($N_{|U_i} = M_i$) equivale a dar las funciones de transición, es decir, isomorfismos

$$\theta_{ij}: M_{i|U_i \cap U_j} \xrightarrow{\sim} M_{j|U_i \cap U_j}, \qquad \text{para cualesquiera } i, j$$

verificando la condición de cociclo:

$$\theta_{jk|U_j \cap U_k \cap U_i} \circ \theta_{ij|U_i \cap U_j \cap U_k} = \theta_{ik|U_i \cap U_k \cap U_j}, \qquad \text{para todo } i, j, k$$

Sea $X = \coprod_i U_i$, $X \to Y$ el recubrimiento obvio y M el haz de módulos sobre X, tal que sobre cada abierto U_i sea M_i. Los isomorfismos anteriores equivalen a dar un isomorfismo de funtores

$$\theta: M \otimes_Y X \xrightarrow{\sim} X \otimes_Y M$$

verificando que el diagrama

$$\begin{array}{ccc} M\otimes_Y X\otimes_Y X & \xrightarrow{\quad\theta_3\quad} & X\otimes_Y M\otimes_Y X \\ & {\scriptstyle\theta_2}\searrow \quad \swarrow{\scriptstyle\theta_1} & \\ & X\otimes_Y X\otimes_Y M & \end{array}$$

es conmutativo, donde el índice indica la coordenada que queda fija, es decir, $\theta_i = d_i^*\theta$.

1. Definición: Sea $X \to Y$ un morfismo fielmente plano de tipo finito y M un haz en $\mathscr{C}_X$, para la topología fielmente plana. Llamaremos dato de construcción a cada isomorfismo de funtores sobre $\mathscr{C}_{X\times_Y X}$, $\theta\colon M\otimes_Y X \xrightarrow{\sim} X\otimes_Y M$, verificando la condición de cociclo $\theta_1\circ\theta_3 = \theta_2$.

Observemos que si restringimos el diagrama anterior a la diagonal ($\Delta\colon X \to X\times X\times X$) tendremos que $\theta_{1|\Delta}\circ\theta_{3|\Delta} = \theta_{2|\Delta}$, luego $\theta^2_{|\Delta} = \theta_{|\Delta}$ (considerando ahora la diagonal $\Delta\colon X \to X\times X$). Por tanto, $\theta_{|\Delta} = \mathrm{Id}\colon M \to M$.

Dado un haz N en Y, existe de modo obvio, un dato de construcción en $N\otimes_Y X$ ($N\otimes_Y X\otimes_Y X = X\otimes_Y N\otimes_Y X$). Dato de construcción que llamaremos trivial. Se trata ahora de ver que los datos de construcción son efectivos, es decir, son esencialmente triviales.

2. Teorema de descenso de haces: *Sea $X \to Y$ un morfismo fielmente plano de tipo finito. Dado un haz M sobre $\mathscr{C}_X$, para la topología fielmente plana, junto con un dato de construcción θ, existe un haz N sobre $\mathscr{C}_Y$, para la topología fielmente plana, y un isomorfismo de funtores*

$$g\colon N\otimes_Y X \xrightarrow{\sim} M$$

tal que el diagrama de funtores sobre $X\times_Y X$

$$\begin{array}{ccc} (N\otimes_Y X)\otimes_Y X & \xrightarrow{g\otimes 1} & M\otimes_Y X \\ \| & & \downarrow{\scriptstyle\theta} \\ X\otimes_Y (N\otimes_Y X) & \xrightarrow{1\otimes g} & X\otimes_Y M \end{array}$$

es conmutativo. Es decir, θ en $N\otimes_Y X$ (a través de g) induce el dato de construcción trivial. Además N es única salvo isomorfismos.

Demostración. La idea de la construcción de N proviene del ejemplo para módulos: las secciones de N son las familias de secciones locales en un recubrimiento -es decir, las de M- que coinciden en las intersecciones. Se define N como el funtor que verifica que la sucesión

$$N \to M \underset{\theta\circ d_2}{\overset{d_1}{\rightrightarrows}} X\otimes_{\underline{Y}} M$$

es exacta, como sucesión de funtores sobre Y, siendo d_1, d_2 los morfismos inducidos en los funtores por las proyecciones $X \times_Y X \overset{d_1}{\underset{d_2}{\rightrightarrows}} X$.

Considerando esta sucesión, relevada a X, junto con la sucesión exacta de haz para M para el morfismo fielmente plano $X \times_Y X = \overline{X} \overset{d_1}{\to} X$, tenemos el diagrama de filas exactas

$$\begin{array}{ccccc} N \otimes_Y \underline{X} & \longrightarrow & M \otimes_Y \underline{X} & \overset{d_1\otimes 1}{\underset{\theta\circ d_2\otimes 1}{\rightrightarrows}} & X \otimes_Y M \otimes_Y \underline{X} \\ \downarrow \wr g & & \downarrow \wr\theta & & \downarrow \wr 1\otimes\theta \\ \underline{M} & \longrightarrow & X \otimes_Y \underline{M} & \overset{d_1}{\underset{d_2}{\rightrightarrows}} & X \otimes_Y X \otimes_Y \underline{M} \end{array}$$

donde los cuadrados de la derecha son conmutativos por la condición de cociclo. Por tanto, tenemos definido un isomorfismo $g : N \otimes_Y X \simeq M$.

Ahora del cuadrado conmutativo de la izquierda obtenemos el diagrama conmutativo

$$\begin{array}{ccccc} N \otimes_Y \underline{X} & \longrightarrow & M \otimes_Y \underline{X} & \longrightarrow & \underline{M} \\ \downarrow \wr g & & \downarrow \wr\theta & & \downarrow \mathrm{Id} \\ \underline{M} & \longrightarrow & X \otimes_Y \underline{M} & \longrightarrow & \underline{M} \end{array}$$

Del cual se deduce que g es el morfismo inducido, por adjunción, por $N \to M$.

Del cuadrado conmutativo de la izquierda del diagrama que precede al anterior obtenemos también

$$\begin{array}{ccccc} \underline{X} \otimes_Y N \otimes_Y \underline{X} & \longrightarrow & \underline{X} \otimes_Y M \otimes_Y \underline{X} & \longrightarrow & \underline{M} \otimes_Y \underline{X} \\ \downarrow 1\otimes g & & \downarrow \wr 1\otimes\theta & & \downarrow \wr\theta \\ \underline{X} \otimes_Y \underline{M} & \longrightarrow & \underline{X} \otimes_Y X \otimes_Y \underline{M} & \longrightarrow & \underline{X} \otimes_Y \underline{M} \end{array}$$

Por tanto obtenemos el diagrama requerido.

$$\begin{array}{ccc} \underline{X} \otimes_Y N \otimes_Y \underline{X} & \overset{g\otimes 1}{\longrightarrow} & \underline{M} \otimes_Y \underline{X} \\ \downarrow 1\otimes g & & \downarrow \wr\theta \\ \underline{X} \otimes_Y \underline{M} & = & \underline{X} \otimes_Y \underline{M} \end{array}$$

En cuanto a la unicidad, resulta del teorema de descenso de homomorfismos.

□

Si un $\mathscr{O}_X$-módulo cuasicoherente tiene estructura de $\mathscr{O}_X$-álgebra diremos que es una $\mathscr{O}_X$-álgebra cuasicoherente.

3. Teorema de descenso de módulos: *Dado un $\mathscr{O}_X$-módulo $\mathscr{M}$ cuasicoherente (resp. una $\mathscr{O}_X$-álgebra cuasicoherente) sobre X, junto con un dato de construcción θ, existe un $\mathscr{O}_Y$-módulo $\mathscr{N}$ cuasicoherente (resp. una $\mathscr{O}_Y$-álgebra cuasicoherente) sobre Y, y un isomorfismo*

$$g\colon \mathscr{N}\otimes_Y X \tilde{\to} \mathscr{M}$$

tal que el diagrama sobre $X\times_Y X$

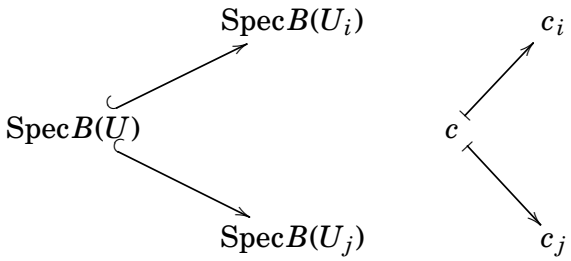
$$\begin{array}{ccc} (\mathscr{N}\otimes_Y X)\otimes_Y X & \xrightarrow{g\otimes 1} & \mathscr{M}\otimes_Y X \\ \| & & \downarrow{\scriptstyle\theta} \\ X\otimes_Y(\mathscr{N}\otimes_Y X) & \xrightarrow{1\otimes g} & X\otimes_Y \mathscr{M} \end{array}$$

es conmutativo. Es decir, θ en $\mathscr{N}\otimes_Y X$ (a través de g) induce el dato de construcción trivial. Además $\mathscr{N}$ es única salvo isomorfismos.

Demostración. Sólo es observar que el descenso $\mathscr{N}$, construido en el teorema anterior, es un $\mathscr{O}_Y$-módulo cuasicoherente (resp. una $\mathscr{O}_Y$-álgebra cuasicoherente). □

Ahora, nuestro objetivo, es dar condiciones para que el descenso del haz de puntos de un esquema, sea también el haz de puntos de un esquema.

Dado un morfismo $\pi\colon C\to X$ afín, tenemos la $\mathscr{O}_X$-álgebra cuasicoherente $\pi_*\mathscr{O}_C$. Recíprocamente, dada una $\mathscr{O}_X$-álgebra cuasicoherente B, consideremos un recubrimiento $X=\bigcup_i U_i$ por abiertos afines y sea $\bar{C}=\coprod_i \operatorname{Spec}B(U_i)$. Dado $x_i\in\operatorname{Spec}B(U_i)$ y dado $x_j\in\operatorname{Spec}B(U_j)$, diremos que $c_i\sim c_j$ si existe un abierto U básico en U_i y U_j, y un $c\in U$, de modo que se verifica el diagrama



Se cumple que $C=\bar{C}/\sim$ es un esquema y el morfismo natural $\pi\colon C\to X$ es un morfismo de esquemas afín, de modo que $\pi^{-1}(U_i)=\operatorname{Spec}B(U_i)$. La construcción de C se puede obtener también de 11.5.11, pues C es el representante del funtor, sobre la categoría de los X-esquemas, $F(X'):=\operatorname{Hom}_{\mathscr{O}_X-\text{álg}}(B,\mathscr{O}_{X'})$, que es un haz localmente representable.

En conclusión, la categoría de los esquemas afines sobre X es equivalente a la categoría de las $\mathcal{O}_X$-álgebras cuasicoherentes. Por tanto, por el corolario anterior, hemos demostrado el siguiente corolario.

4. Corolario: *El descenso de un esquema afín sobre X es un esquema afín sobre Y. El descenso de un subesquema cerrado de X es un subesquema cerrado de Y.*

5. Lema: *Sea $A \to B$ un morfismo finito fielmente plano. Dado $b \in B$ consideremos el endomorfismo A-lineal $B \xrightarrow{b\cdot} B$. Denotemos $N(b) \in A$ el determinante de endomorfismo (observemos que si A es local B es un A-módulo libre). Sea $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido en espectros. Dados $x, x' \in \operatorname{Spec} B$ diremos que $x \sim x'$ si $f(x) = f(x')$. Se cumple que $N(b)(x) = 0$ si y sólo si $b(x') = 0$ para algún $x' \sim x$.*

Demostración. Sea $y = f(x)$. $N(b)(x) = 0$ si y sólo si $N(b)(y) = 0$. Ahora bien, $N(b)(y)$ es el determinante de la aplicación

$$B_y/\mathfrak{p}_y B_y \xrightarrow{b(y)\cdot} B_y/\mathfrak{p}_y B_y$$

que es nulo si y sólo si $b(y)$ no es invertible en $B_y/\mathfrak{p}_y B_y$, es decir, $b(y)$ (o b) se anula en algún punto de $\operatorname{Spec} B_y/\mathfrak{p}_y B_y = \{x' \in \operatorname{Spec} B : x' \sim x\}$. □

6. Teorema: *Sea $X \to Y$ un morfismo finito fielmente plano. Sean $Z \to X$ un morfismo de esquemas cuasiproyectivo y $\theta\colon Z \times_Y X \simeq X \times_Y Z$ un dato de construcción. Existe un descenso, es decir, un esquema $Z' \to Y$ de modo que $Z' \times_Y X = Z$. Además los descensos son únicos salvo isomorfismos.*

Demostración. Sólo tenemos que probar que el haz F obtenido como el descenso del haz de puntos de Z, es el haz de puntos de un esquema.

Obviamente esto es un problema local en Y, luego podemos suponer que $Y = \operatorname{Spec} A$ y por tanto $X = \operatorname{Spec} B$, donde B es una A-álgebra finita fielmente plana.

Si U es un abierto de Z estable por θ y Z' es un descenso de Z, y denotamos por $\pi\colon Z = Z' \times_Y X \to Z'$ la proyección natural, entonces es fácil ver que el abierto $\pi(U)$ de Z' es un descenso de U. Por recollement y la unicidad del descenso, si $\{U_i\}$ es un recubrimiento de Z por abiertos estables por θ, para los que existen descensos U_i', entonces el descenso Z' se obtiene por recollement de los U_i'. En conclusión, basta probar que existe un recubrimiento de Z por abiertos afines estables por θ.

Por cambio de base $\times_Y X$ tendremos que Z es el descenso de $Z \times_Y X$ y el dato de construcción θ (cambiado de base) es isomorfo al dato de construcción trivial. Hechos que importa recalcar, porque muchas de las afirmaciones que siguen son ciertas si lo son por cambio de base $\times_Y X$.

Sean $d_1\colon Z \times_Y X \to Z$, $d_2\colon X \times_Y Z \to Z$ las dos proyecciones naturales, que son finitas. Denotemos $\bar{\theta} = d_2 \circ \theta$. Dado un punto cerrado $z \in Z$, denotemos $R(z) = \bar{\theta}(z \times_Y X)$,

que es un número finito de puntos cerrados de Z. Sea U un abierto afín que contenga a $R(z)$. Sea $C = Z - U$ y denotemos $R(C) = \bar{\theta}(C \times_Y X)$ que es un cerrado de Z. Sea $U' = Z - R(C)$, que es un abierto estable por θ, que contiene a $R(z)$ y está contenido en U. Sea $f \in \mathcal{O}_Z(U)$, de modo que $R(z) \subset U_f \subset U' \subset U$.

Consideremos los morfismos

$$\mathcal{O}_Z(U') \underset{\bar{\theta}}{\overset{d_1}{\rightrightarrows}} \mathcal{O}_Z(U') \otimes_A B = \mathcal{O}_{\bar{Z}}(\bar{U}')$$

donde denotamos $\bar{Z} = Z \times_{\mathrm{Spec}A} \mathrm{Spec}B$, $\bar{U}' = U' \times_{\mathrm{Spec}A} \mathrm{Spec}B$. Por cambio de base $\otimes_A B$ se corresponden con los morfismos naturales

$$\mathcal{O}_{\bar{Z}}(\bar{U}') \rightrightarrows \mathcal{O}_{\bar{Z}}(\bar{U}') \otimes_{\mathcal{O}_Z(U')} \mathcal{O}_{\bar{Z}}(\bar{U}')$$

Observemos que $\mathcal{O}_Z(U') \otimes_A B$ es un $\mathcal{O}_Z(U')$-módulo finito generado a través de $\bar{\theta}$ y la norma de $f \otimes 1 \in \mathcal{O}_Z(U') \otimes_A B$, $N(f)$ (es decir, el determinante de la homotecia en $\mathcal{O}_Z(U') \otimes_A B$ multiplicar por $f \otimes 1$) cumple que tiene la misma imagen por d_1 que por $\bar{\theta}$, porque así sucede si cambiamos de base $\otimes_A B$. Además $N(f)$ no se anula en ningún punto de $R(z)$ y se anula en los puntos donde f se anula. Por tanto, $U_{N(f)} = U'_{N(f)}$ es un abierto afín estable por θ, que contiene a z. Hemos concluido. □

18.5. Cohomología en la topología fielmente plana

Dado un haz F de grupos abeliano y un "recubrimiento" X de Y en la topología fielmente plana, es decir, un morfismo $X \to Y$ fielmente plano de tipo finito, consideremos la sucesión

$$\cdots \to X \times_Y X \times_Y X \underset{d_3}{\overset{d_1}{\underset{d_2}{\rightrightarrows}}} X \times_Y X \underset{d_2}{\overset{d_1}{\rightrightarrows}} X \to Y$$

Consideremos el complejo $C^{\cdot}F(X) := \oplus C^i F(X) := \oplus F(X \times \overset{i+1}{\cdots} \times X)$ de diferenciales

$$d^i : F(X \times \overset{i}{\cdots} \times X) \to F(X \times \overset{i+1}{\cdots} \times X) \text{ definidas por } d^i := \sum_{j=1}^{i+1} (-1)^{j+1} d_j^*.$$

Se define $H^i(X/Y, F) := \mathrm{Ker}\, d^{i+1} / \mathrm{Im}\, d^i$.

En particular, $H^0(X/Y, F) = F(Y)$.

El primer "grupo de cohomología" de F (con notaciones multiplicativas) asociado a la "resolución de Cech" definida por el "recubrimiento" $X \to Y$ es

$$H^1(X/Y, F) := \left[\begin{array}{l} s \in F(X \times_Y X): \\ d_3^* s \cdot d_2^* s^{-1} \cdot d_1^* s = 1 \end{array} \right] / \left[d_2^* \tau \cdot d_1^* \tau^{-1}, \tau \in F(X) \right]$$

Dada una sucesión de haces de grupos $1 \to F_1 \to F_2 \to F_3 \to 1$, si define una sucesión exacta $1 \to C^{\cdot}F_1(X) \to C^{\cdot}F_2(X) \to C^{\cdot}F_3(X) \to 1$ tendremos definida la sucesión exacta larga

$$1 \to F_1(Y) \to F_2(Y) \to F_3(Y) \xrightarrow{\delta} H^1(X/Y,F_1) \to H^1(X/Y,F_2) \to H^1(X/Y,F_3) \to \cdots$$

Una sucesión $1 \to F_1 \to F_2 \to F_3$ de haces de grupos en la topología fielmente plana, se dice que es exacta si para todo Y-esquema X la sucesión de grupos $1 \to F_1(X) \to F_2(X) \to F_3(X)$ es exacta. Esta definición tiene una justificación categorial, pero para nuestros objetivos nos basta con lo dicho.

Si sólo tenemos garantizada la exactitud de $1 \to F_1 \to F_2 \to F_3$ y de la sucesión $1 \to C^0F_1(X) \to C^0F_2(X) \to C^0F_3(X) \to 1$ sólo podremos afirmar la exactitud de la sucesión

$$1 \to F_1(Y) \to F_2(Y) \to F_3(Y) \xrightarrow{\delta} H^1(X/Y,F_1) \to H^1(X/Y,F_2) \to H^1(X/Y,F_3) \qquad (*)$$

Si F es un haz de grupos (no abeliano), definiremos

$$H^1(X/Y,F) := \left[\begin{array}{l} s \in F(X \times_Y X): \\ d_3^* s \cdot d_2^* s^{-1} \cdot d_1^* s = 1 \end{array} \right] \Big/ \left[\begin{array}{l} s \sim s' \text{ si existe } \tau \in F(X): \\ d_2^* \tau \cdot s \cdot d_1^* \tau^{-1} = s' \end{array} \right]$$

Se verifica también la sucesión $(*)$, donde ahora la exactitud quiere decir que la imagen de cada morfismo son los elementos que se aplican, por el morfismo siguiente, en la clase del elemento neutro.

Supongamos ahora que $X \to Y$ es un revestimiento de Galois de grupo G. A través de las identificaciones $G \times \overset{n}{\cdots} \times G \times X = X \times_Y \overset{n}{\cdots} \times_Y X \times_Y X$, $(g_1,\ldots,g_n,x) \mapsto (g_1 x,\ldots,g_n x,x)$ y $F(G \times \overset{n}{\cdots} \times G \times X) = \mathrm{Aplic}(G \times \overset{n}{\cdots} \times G, F(X))$, obtendremos que

$$H^1(X/Y,F) = \left[\begin{array}{l} f \in \mathrm{Aplic}(G,F(X)): \\ f(\sigma \cdot \sigma') = f(\sigma) \cdot \sigma(f(\sigma')) \end{array} \right] \Big/ \left[\begin{array}{l} f \sim f' \text{ si existe } c \in F(X): \\ f'(\sigma) = c \cdot f(\sigma) \cdot \sigma(c)^{-1} \end{array} \right]$$

Denotaremos $H^1(X/Y,F) \underset{\text{Not.}}{=} H^1(G,F(X))$.

18.6. Clasificación de construcciones.

Planteemos ahora el problema de la clasificación de los descensos.

Dado N tal que $N \otimes_Y X \simeq M$, entonces el dato de construcción trivial de $N \otimes_Y X$ induce vía el isomorfismo un dato de construcción θ para M. El teorema del descenso nos dice que M con el dato de construcción θ desciende a N. Luego el conjunto de clases de isomorfía de los descensos de M son un cociente del conjunto de los datos de construcción de M .

Dos datos de construcción θ, θ' dan el mismo descenso N si y sólo si existen dos isomorfismos $N \otimes_Y X \simeq M$ de modo que vía esos dos isomorfismos el dato de construcción trivial de $N \otimes_Y X$ induce θ y θ' para M. Esto equivale a decir que θ, θ' dan el mismo descenso si y sólo si existe un isomorfismo $M \simeq M$ de modo que vía este isomorfismo θ induce θ'. Así pues, la clase de isomorfismos de descensos de M equivale a los datos de construcción θ, módulo la relación de equivalencia inducida por los automorfismos de M.

Supongamos ahora que $M = N \otimes_Y X$. Los descensos de M, se corresponden con los isomorfismos

$$\begin{array}{ccc} (N \otimes_Y X) \otimes_Y X & \xrightarrow{\theta}_{\sim} & X \otimes_Y (N \otimes_Y X) \\ \| & & \| \\ N \otimes_Y (X \otimes_Y X) & & N \otimes_Y (X \otimes_Y X) \end{array}$$

(donde para cada isomorfismo $\tau : N \otimes_Y X = M \to N \otimes_Y X = M$ diremos que $\theta \sim d_2^* \tau \circ \theta \circ d_1^* \tau^{-1}$) que verifican la condición de cociclo

$$\begin{array}{ccccc} N \otimes_Y X \otimes_Y X \otimes_Y X & \xrightarrow{\theta_3} & X \otimes_Y N \otimes_Y X \otimes_Y X & = & N \otimes_Y X \otimes_Y X \otimes_Y X \\ & \searrow^{\theta_2} & \downarrow{\scriptstyle \theta_1} & & \\ & & X \otimes_Y X \otimes_Y N \otimes_Y X & = & N \otimes_Y X \otimes_Y X \otimes_Y X \end{array}$$

es decir, $d_1^* \theta \circ d_3^* \theta = d_2^* \theta$ (donde recordemos que $\theta \in \mathrm{Aut}(N \otimes_Y X \otimes_Y X)$). En resumen:

1. Teorema de clasificación: *Los descensos de $M = N \otimes_Y X$ se corresponden biunívocamente con el conjunto*

$$H^1(X/Y, Aut(N)) = \left[\begin{array}{l} \text{automorfismos } \theta \text{ de} \\ N \otimes_Y X \otimes_Y X: \\ d_1^* \theta \circ d_3^* \theta = d_2^* \theta \end{array} \right] \Big/ \left[\begin{array}{l} \overline{\theta} \sim \theta \text{ si y sólo si} \\ \theta = d_2^* \tau \circ \overline{\theta} \circ d_1^* \tau^{-1} \text{ para} \\ \text{algún } \tau \in \mathrm{Aut}(N \otimes_Y X) \end{array} \right]$$

18.7. Ejemplos y aplicaciones

1) Supongamos que Y es un esquema noetheriano.

Sea $\{U_i\}_{i=1}^n$ un recubrimiento finito de Y, $X = \coprod_i U_i$, el morfismo natural $f : X \to Y$ y el haz de módulos $\mathscr{M} = \mathscr{O}_X$. Un descenso de $\mathscr{M}$ es $\mathscr{O}_Y$ y $Aut(\mathscr{O}_Y) = \mathscr{O}_Y^*$, luego

$$\left[\begin{array}{l} \text{haces de línea de } Y \\ \text{triviales sobre el} \\ \text{recubrimiento } X \end{array} \right] = H^1(X/Y, \mathscr{O}_Y^*)$$

$$= \left[\begin{array}{l} \text{cociclos:} \\ \{g_{ij} \in \mathscr{O}(U_i \cap U_j)^*\}_{i,j} \\ \text{tales que } g_{ij} g_{jk} = g_{ik} \end{array} \right] \Big/ \left[\begin{array}{l} \text{bordes:} \\ \{g_i \cdot g_j^{-1} \in \mathscr{O}(U_i \cap U_j)^*\}_{i,j} \\ \text{con } \{g_i\}_i \in \{\mathscr{O}(U_i)^*\}_i \end{array} \right]$$

Notaciones: Como la categoría de los anillos es equivalente a la categoría de los esquemas afines, continuamente identificaremos un esquema afín, con su anillo de funciones. Por ejemplo, dado un morfismo $A \to B$ fielmente plano, denotaremos $H^1(\mathrm{Spec}B/\mathrm{Spec}A, F) = H^1(B/A, F)$, o $F(\mathrm{Spec}B) = F(B)$.

2) Teorema de Galois.

Sea $k \hookrightarrow K$ una extensión de cuerpos de Galois de grupo G. Se verifica

$$\left[\begin{array}{l}\text{Clases de isomorfía de las}\\ k-\text{álgebras separables de grado } n\\ \text{trivializadas por } K\end{array}\right] = H^1(K/k, \mathrm{Aut}_{k-alg}(k^n)) = H^1(G, S_n)$$

$$= \left[\begin{array}{l}\text{Morfismos de grupos}\\ f: G \to S_n\end{array}\right] \Big/ \text{ conjugación } = \left[\begin{array}{l}\text{Clases de isomorfía de}\\ G-\text{conjuntos de orden } n\end{array}\right]$$

3) Teorema 90 de Hilbert.

Sea $k \hookrightarrow K$ una extensión finita de cuerpos, $Y = \mathrm{Spec}k$, $X = \mathrm{Spec}K$. Se trata de clasificar los k-módulos N tales que $N \otimes_k K = N \otimes_Y X = K \oplus \overset{n}{\cdots} \oplus K$. Es claro que no hay más que uno, $N = k \oplus \overset{n}{\cdots} \oplus k$, ya que los k-módulos están clasificados por su dimensión sobre k, que es la misma que la de $N \otimes_k K$ sobre K. Por tanto, se obtiene, por ser $Aut(N) = Gl_n$, el siguiente teorema.

1. Teorema: $H^1(K/k, Gl_n) = 0$

Sea Gl_n el funtor $Gl_n(X) = \mathrm{Aut}_{\mathscr{O}_X-\mathrm{mód}}(\mathscr{O}_X^n)$, que es un haz en $\mathscr{C}_Y$, para la topología fielmente plana. Denotaremos $Gl_1 = G_m$, es decir, $G_m(X) := Gl_1(X) = \Gamma(X, \mathscr{O}_X^*)$.

2. Corolario: $H^1(K/k, G_m) = 0$.

3. Teorema 90 de Hilbert: *Sea $k \hookrightarrow K$ una extensión de Galois cíclica de grupo $G =< \sigma >$. La norma de $\alpha \in K$ es uno si y sólo si existe un $\beta \in K$ tal que $\alpha = \frac{\beta}{\sigma(\beta)}$.*

Demostración.

$$H^1(G, G_m(K)) =$$

$$= \left[\begin{array}{l}\text{Aplic. } f: G \to G_m(K) = K^*:\\ f(\sigma' \cdot \sigma'') = f(\sigma') \cdot \sigma'(f(\sigma''))\end{array}\right] \Big/ \left[\begin{array}{l} f \sim f' \Leftrightarrow \text{Existe } \alpha \in K^*:\\ f(\sigma') = \alpha \cdot f'(\sigma') \cdot \sigma'(\alpha)^{-1}\end{array}\right]$$

Las aplicaciones f están determinadas por $f(\sigma)$, con la única condición de que $f(\sigma^n) = N(f(\sigma)) = 1$. Por tanto,

$$0 = H^1(K/k, G_m) = H^1(G, G_m(K))$$
$$= \{\beta \in K \text{ tales que } N(\beta) = 1\}/\{\alpha \cdot \sigma(\alpha)^{-1}\}_{\alpha \in K^*}$$

que es el teorema 90 de Hilbert. □

4) Teorema 90 aditivo.

Una k-variedad algebraica X se dice que es un grupo algebraico si el haz de puntos $X^{\cdot}$, es un haz de grupos. Por ejemplo, $\mathrm{Spec}\, k[x,1/x]$ es un grupo algebraico, porque $(\mathrm{Spec}\, k[x,1/x])^{\cdot} = G_m$. Otro ejemplo, es la recta afín $\mathbb{A}_1 = \mathrm{Spec}\, k[x]$, pues $\mathbb{A}_1^{\cdot}(X) = \mathrm{Hom}(X, \mathrm{Spec}\, k[x]) = \Gamma(X, \mathcal{O}_X)$. Denotaremos $\mathbb{A}_1 = G_a$ y diremos que es el grupo aditivo, también denotaremos $\mathbb{A}_1^{\cdot} = G_a$.

Dado un grupo finito discreto G el funtor sobre la categoría de k-esquemas

$$F(Z) = \mathrm{Aplic}_{\mathrm{cont}}(Z, G)$$

es un haz de grupos. Si Z es conexo, entonces $F(Z) = G$. F es representable por $\mathrm{Spec}\, \mathrm{Aplic}(G, k)$, que por abuso de notación denotaremos G. Así pues,

$$\mathrm{Hom}_{\mathrm{esq}}(Z, G) = \mathrm{Aplic}_{\mathrm{cont}}(Z, G)$$

y G es un grupo algebraico.

4. Teorema: *Si $k \hookrightarrow K$ es una extensión, entonces $H^1(K/k, G_a) = 0$.*

Demostración. Se deduce de que $k \to K \rightrightarrows K \underset{k}{\otimes} K \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; K \underset{k}{\otimes} K \underset{k}{\otimes} K$ es una sucesión exacta y G_a es el funtor identidad. □

5. Corolario: *Sea $k \to K$ una extensión cíclica de grado $p = car\ k$ y grupo $G = <\sigma>$. La traza de $\alpha \in K$ es cero si y solo si existe un $\beta \in K$ tal que $\alpha = \beta - \sigma(\beta)$.*

Demostración. La demostración es la misma que el teorema 90 de Hilbert, sustituyendo G_m por G_a y recordando que $H^1(K/k, G_a) = 0$.

□

5) Teoría de Kummer y Artin-Schreier: extensiones cíclicas.

6. Teorema: *Sea k un cuerpo y p un número primo:*

1. *Si* $\mathrm{car}\, k \neq p$ *y k contiene una raíz p-ésima primitiva de la unidad, entonces*

$$\left[\begin{array}{l}\textit{Clases de isomorfía de}\\ \textit{extensiones cíclicas}\\ \textit{de } k \textit{ de grado } p\end{array}\right] = k^*/(k^*)^p \qquad \textit{(teoría de Kummer)}$$

2. *Si* $\mathrm{car}\, k = p$, *entonces*

$$\left[\begin{array}{l}\textit{Clases de isomorfía de}\\ \textit{extensiones cíclicas}\\ \textit{de } k \textit{ de grado } p\end{array}\right] = k/\{\lambda^p - \lambda : \lambda \in k\} \qquad \textit{(teoría de Artin-Schreier)}$$

Demostración. Denotemos por $\overline{k}$ el cierre separable de k.

1. Consideremos la sucesión exacta

$$1 \to \mu_p \to G_m \xrightarrow{F} G_m \to 1$$

donde μ_p es el haz definido por $\mu_p(X) = \{s \in \Gamma(X, \mathcal{O}_X^*) \colon s^p = 1\}$, y F es el morfismo elevar a p. Si K es una extensión de cuerpos de k, entonces $\mu_p(K)$ son las raíces p-ésimas de la unidad de K y como k contiene a todas las raíces p-ésimas de la unidad, tendremos que $\mu_p(K) \simeq \mathbb{Z}/p\mathbb{Z}$. Así pues, para toda extensión finita separable $k \hookrightarrow K$, se cumple que $H^1(K/k, \mu_p) = H^1(K/k, \mathbb{Z}/p\mathbb{Z})$.

De la sucesión exacta larga de cohomología se obtiene que $H^1(\bar{k}/k, \mu_p) = k^*/(k^*)^p$. Por otra parte, $H^1(\bar{k}/k, \mathbb{Z}/p\mathbb{Z})$ clasifica los $\mathbb{Z}/p\mathbb{Z}$-álgebras sobre k (haz de k-álgebras sobre las que opera $\mathbb{Z}/p\mathbb{Z}$), tales que por cambio de base $\otimes_k \bar{k}$, son isomorfas a $\bar{k} \times \overset{p}{\ldots} \times \bar{k}$ (donde $\mu_p(\bar{k})$ opera cíclicamente en las componentes), porque $Aut_{\mathbb{Z}/p\mathbb{Z}}(k^p) = \mathbb{Z}/p\mathbb{Z}$.

2. En este caso es igual que el anterior sólo que considerando la sucesión exacta

$$0 \to \mathbb{Z}/p\mathbb{Z} \to G_a \xrightarrow{x^p - x} G_a \to 0$$

Con la que obtenemos $H^1(\overline{k}/k, \mathbb{Z}/p\mathbb{Z}) = k/\{\lambda^p - \lambda : \lambda \in k\}$. □

6) Teoría de grupos algebraicos afines:

Sea k un cuerpo perfecto, $k \hookrightarrow \bar{k}$ el cierre algebraico y sea G un grupo algebraico afín sobre k.

7. Teorema: *Si* $G \underset{\mathrm{Spec}\, k}{\times} \mathrm{Spec}\, \bar{k} \simeq G_{a,\bar{k}} = \mathrm{Spec}\, \bar{k}[t]$, *entonces* $G = G_a$.

Demostración. Si $G \underset{\mathrm{Spec}\, k}{\times} \mathrm{Spec}\, \bar{k} \simeq G_{a,\bar{k}}$, entonces esto también es cierto para una cierta extensión finita K de k (pues basta que la función t de $G_{a,\bar{k}}$ esté en el anillo de $G \underset{\mathrm{Spec}\, k}{\times} \mathrm{Spec}\, K$). Los grupos afines tales que $G \underset{\mathrm{Spec}\, k}{\times} \mathrm{Spec}\, K = G_{a,K} = \mathrm{Spec}\, K[x]$ están clasificados por $H^1(K/k, Aut(G_a))$. Ahora bien, se cumple que $\mathrm{Aut}_{\mathrm{Spec}\, K \otimes K}(G_{a,K\otimes K}) = G_m(K \otimes K)$ ya que $K \otimes K$ no tiene nilpotentes. Por tanto, $H^1(K/k, Aut(G_a)) = H^1(K/k, G_m) = 0$ y $G = G_a$.

□

7) Variedades de Brauer-Severi.

Supondremos k perfecto. Las variedades de Brauer-Severi son las k-variedades X que al cambiar de base al cierre algebraico $\bar{k}$ son isomorfas al espacio proyectivo, es decir:

$$X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, \bar{k} = \mathbb{P}_{n,\bar{k}}$$

Por tanto su clasificación es un problema de la teoría del descenso y ésta nos da

$$\left[\begin{array}{l}\text{Clases de isomorfía de}\\ \text{variedades de Brauer-}\\ \text{Severi sobre } k\end{array}\right] = H^1(\bar{k}/k, PGl_{n+1})$$

donde PGl_{n+1} es el funtor definido por $PGl_{n+1}(K) = \mathrm{Aut}_K(\mathbb{P}_{n,K})$, siendo K una k-álgebra finita separable.

Las álgebras de Azumaya son las k-álgebras A (no conmutativas) finitas simples y centrales ($Z(A) = k$). Dicho de otro modo, las álgebras de Azumaya son las k-álgebras A tales que $A \underset{k}{\otimes} \bar{k} = M_n(\bar{k})$. En conclusión, por la teoría del descenso se clasifican por:

$$\left[\begin{array}{l}\text{Clases de isomorfía de}\\ \text{álgebras de Azumaya sobre}\\ k \text{ de dimensión } n^2\end{array}\right] = H^1(\bar{k}/k, PGl_n)$$

por ser $\mathrm{Aut}(M_n(K)) = PGl_{n,K}$, ($K$ cualquier álgebra finita separable) por el teorema de Skolem-Noether (que no hemos visto).

De aquí que clasificar variedades de Brauer-Severi de dimensión n equivale a clasificar álgebras de Azumaya de dimensión $(n+1)^2$.

8. Ejemplo: Si $k = \mathbb{R}$, $\bar{k} = \mathbb{C}$ y $n = 1$, hay tantas variedades reales X, tales que $X \times_{\mathrm{Spec}\,\mathbb{R}} \mathrm{Spec}\,\mathbb{C} = \mathbb{P}_{1,\mathbb{C}}$, como álgebras de Azumaya de dimensión $2^2 = 4$. Por otra parte, cuerpos no conmutativos finitos sobre $\mathbb{R}$ no hay más que $\mathbb{R}$, $\mathbb{C}$ y Q (siendo Q los cuaterniones), por el teorema de Fröbenius (no visto). Como toda álgebra de Azumaya es un álgebra de matrices sobre un cuerpo no conmutativo, se concluye que de dimensión 4 no hay más que $M_2(\mathbb{R})$ y Q, de donde

$$\left[\begin{array}{l}\text{Clases de isomorfía de}\\ \text{variedades de Brauer-Severi}\\ \text{sobre } \mathbb{R} \text{ de dimensión 1}\end{array}\right] = \{\mathbb{P}_{1,\mathbb{R}}, \text{ la cónica imaginaria }\}$$

El hecho es recíproco, si conocemos esta clasificación resulta (sin suponer el teorema de Fröbenius) que

$$\left[\begin{array}{l}\text{Clases de isomorfía de}\\ \text{álgebras reales de Azumaya}\\ \text{de dimensión 4}\end{array}\right] = \{M_2(\mathbb{R}), Q\}$$

Por último, sin detallar las demostraciones, veamos que si $k \hookrightarrow K$ es una extensión cíclica de grupo $G = <\sigma>$, puede calcularse $H^1(K/k, PGl_n)$:

De la sucesión $1 \to G_m \to Gl_n \to PGl_n \to 1$ se deduce la inyección $H^1(K/k, PGl_n) \hookrightarrow H^2(K/k, G_m)$. Sea A una k-álgebra, $\pi\colon \mathrm{Spec}\,A \to \mathrm{Spec}\,k$ el morfismo inducido en los

espectros. Denotemos $G_{m,A} = \pi^* G_m$ el grupo multiplicativo sobre $\operatorname{Spec} A$, escribiremos también $G_{m,A} = \pi_* \pi^*(G_m)$. Consideremos la sucesión

$$1 \to G_m \to G_{m,K} \xrightarrow{\frac{1}{\sigma}} G_{m,K} \xrightarrow{N} G_{m,K} \xrightarrow{\frac{1}{\sigma}} G_{m,K} \cdots$$

donde $\frac{1}{\sigma}(a) = \frac{a}{\sigma(a)}$ y $N(a)$ es la norma de a. $H^1(G, G_m(A \otimes_k K)) = H^1(A \otimes_k K/A, G_{m,A}) = 0$ para toda k-álgebra semilocal A, pues este último grupo clasifica los A-módulos que por cambio de base $\otimes_A A \otimes_k K$ son libres de rango 1. Por tanto, obtendremos que tomando secciones en la sucesión anterior, sobre cualquier k-álgebra A finita separable, es exacta. Se verifica además que $\operatorname{Ker} \frac{1}{\sigma} = G_m$ y que $H^i(K/k, G_{m,K}) = 0$ para todo $i > 0$. Con todo, mediante cálculos cohomológicos, obtendremos que

$$H^i(K/k, G_m) = \begin{cases} 0 & \text{i impar} \\ k^*/N(K^*) & \text{i par mayor que cero} \end{cases}$$

Así pues $H^1(K/k, PGl_n) \hookrightarrow k^*/N(K^*)$.

Ahora ya, se demuestra fácilmente el teorema de Fröbenius.

18.8. Descenso en otras topologías: Extensiones de módulos y de álgebras

En este capítulo, dado un esquema Y, hemos dicho que $X \to Y$ es un recubrimiento si es un morfismo fielmente plano. Después hemos probado que las estructuras, que son localmente isomorfas a una estructura N dada en Y, están clasificadas por el $H^1(X/Y, Aut(N))$.

Si en vez de considerar como recubrimientos los morfismos fielmente planos, consideramos otro tipo de morfismos, podremos desarrollar de modo equivalente otra teoría de descenso ("en otras topologías de Grothendieck"). Pongamos un par de ejemplos.

Clasificación de las extensiones de módulos de M por N

Sean M y N dos A-módulos. Dada una sucesión exacta de A-módulos

$$0 \to N \to E \to M \to 0$$

diremos que E es una extensión de A-módulos de M por N. Un ejemplo de extensión, es la extensión trivial, $E = N \oplus M$, con los morfismos obvios $N \hookrightarrow N \oplus M$, $N \oplus M \to M$.

Dadas dos extensiones $0 \to N \to E \to M \to 0$, $0 \to N \to E' \to M \to 0$, diremos que un morfismo de A-módulos $\phi\colon E \to E'$ es un morfismo de extensiones si se tiene el

diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow \phi & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Diremos que $\phi\colon E \to E'$ es un isomorfismo de extensiones si existe un morfismo de extensiones $\phi'\colon E' \to E$ de modo que $\phi \circ \phi' = \mathrm{Id}$ y $\phi' \circ \phi = \mathrm{Id}$.

Queremos clasificar las extensiones de módulos de M por N, módulo isomorfismos.

Sea $\mathscr{C}_M$ la categoría de A-módulos sobre M, es decir, la categoría cuyos objetos son A-módulos R, dotados de un morfismo $R \to M$ y los morfismos entre dos objetos $R \to M$ y $R' \to M$ son los morfismos de A-módulos $f : R \to R'$ que hacen el diagrama

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & R' \\ & \searrow \quad \swarrow & \\ & M & \end{array}$$

conmutativo.

Dados $P, R \in \mathscr{C}_M$ diremos que un morfismo $P \to R$ es un recubrimiento si es epiyectivo. Diremos que un funtor contravariante aditivo F sobre $\mathscr{C}_M$ es un haz si para todo recubrimiento $P \to R$, la sucesión

$$F(R) \to F(P) \rightrightarrows F(P \times_R P)$$

es exacta y $F(0) = 0$ (que equivale a decir que F es exacto por la izquierda). Dado un epimorfismo $P \to M$, tenemos la sucesión exacta

$$\cdots \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; P \times_M P \times_M P \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; P \times_M P \rightrightarrows P \to M$$

Denotemos por $P^{\cdot}$ el complejo diferencial recién definido. Definimos $H^{\cdot}(P/M, F)$ como la cohomología $H^{\cdot}(F(P^{\cdot}))$.

1. Proposición: *Sea $P \to M$ un recubrimiento, siendo P un módulo proyectivo. Entonces, $H^1(P/M, F)$ coincide con el primer funtor derivado de F en M.*

Demostración. Consideremos el complejo $P^{\cdot} \to M$ recién definido. Resolvamos este complejo por proyectivos, $P'(P^{\cdot}) \to P'(M)$. El bicomplejo $F(P'(P^{\cdot}))$ tiene la primera fila y la primera columna acíclica y F es exacto por la izquierda. Por tanto,

$$H^1(P/M, F) = H^1(F(P'(P^{\cdot}))) = R^1F(M)$$

□

Dado un objeto $R \in \mathscr{C}_M$, $\tilde{R} := \mathrm{Hom}_{\mathscr{C}_M}(-,R)$ es un haz sobre $\mathscr{C}_M$. Dado un morfismo $f : P \to M$, y un haz F en $\mathscr{C}_N$ definimos f^*F en $\mathscr{C}_P$, por $f^*F(Q) := F(Q)$. Se cumple que $f^*\tilde{R} = \tilde{R_P}$, con $R_P = R \times_M P$.

Dar una extensión E de M por N, es dar $E \in \mathscr{C}_M$, con $E \to M$ epiyectivo y donde fijamos el núcleo N del morfismo $E \to M$. Si $P \to M$ es un recubrimiento, siendo P un módulo proyectivo, entonces $E_P = N \oplus P$ es trivial.

Los automorfismos de $E = N \oplus M$, que dejan fijo N, se identifican con $\mathrm{Hom}_A(M,N)$ (compruébese). En general, los automorfismos de E_R, que dejan fijo N, se identifican con $\mathrm{Hom}_A(R,N)$. En conclusión, $\mathrm{Aut}_N(\tilde{E}) = \mathrm{Hom}_A(-,N)$. Por tanto, $H^1(P/M, \mathrm{Aut}_{\tilde{N}}(\tilde{E})) = Ext^1_A(M,N)$ si P es un módulo proyectivo.

2. Teorema : *Hay tantas extensiones de módulos de M por N, módulo isomorfismos, como elementos de $Ext^1_A(M,N)$.*

Clasificación de las extensiones de álgebras de A por el módulo I

Sea A una k-álgebra no necesariamente conmutativa (k incluida en el centro de A). Diremos que M es un A-módulo por la izquierda y por la derecha, si tenemos definido $a \cdot m \cdot b = (a \cdot m) \cdot b = a \cdot (m \cdot b)$, para todo $a, b \in A$ y $m \in M$, cumpliendo las propiedades obvias. Con mayor precisión, sea A^o el conjunto A, con la suma de A y el producto $*$ definido por $a * b := b \cdot a$, que dotan a A^o de estructura de anillo. Si M es un $A \otimes_k A^o$-módulo entonces es un A-módulo por la derecha y por la izquierda: $a \cdot m \cdot b := (a \otimes b) \cdot m$. Recíprocamente, si M es un A-módulo por la izquierda y la derecha entonces es un $A \otimes_k A^o$-módulo: $(a \otimes b) \cdot m := a \cdot m \cdot b$.

Sean E y A k-álgebras (no necesariamente conmutativas) y $E \to A$ un epimorfismo de k-álgebras, de modo que el núcleo es un ideal I, tal que $I^2 = 0$ (y por tanto, I es un A-módulo por la izquierda y la derecha, es decir, un $A \otimes A^o$-módulo). Tenemos pues la sucesión exacta

$$0 \to I \to E \to A \to 0$$

y decimos que E es una extensión de álgebras de A por el $A \otimes_k A^o$-módulo I. Un ejemplo de extensión de álgebras de A por I, es $E = A \oplus I$, donde $(a,i) \cdot (a',i') := (aa', ai' + ia')$, que llamaremos extensión trivial.

Si E' es otra extensión de álgebras de A por I, diremos que un morfismo de k-álgebras $\phi : E \to E'$ es de extensiones de álgebras si se tiene un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \\ & & \| & & \downarrow \phi & & \| & & \\ 0 & \longrightarrow & I & \longrightarrow & E' & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Diremos que ϕ es isomorfismo si tiene inverso.

Diremos que $D \in \mathrm{Hom}_k(A,I)$ es una derivación de una k-álgebra A en un $A\otimes A^0$-módulo I si $D(ab) = (Da)b + b(Da)$, para todo $a,b \in A$. Denotaremos $\mathrm{Der}_k(A,I)$ al conjunto de todas las derivaciones de A en I.

3. Proposición: *Sea Δ el núcleo del morfismo $A\otimes A \to A$, $a\otimes b \mapsto ab$. Se tiene*

$$\mathrm{Der}_k(A,I) = \mathrm{Hom}_{A\otimes A^0}(\Delta, I)$$

Demostración. Recordemos que Δ está generado como $A = A\otimes 1$-módulo por los elementos $da = a\otimes 1 - 1\otimes a$. Dado una derivación $D\colon A\to I$, entonces $A\otimes A \to I$, $a\otimes b \mapsto (Da)\cdot b$, restringida a Δ es un morfismo de $A\otimes A^o$-módulos (compruébese), que explícitamente es $\Delta \to I$, $adb \mapsto aDb$.

El morfismo $d\colon A\to \Delta$, $a\mapsto da := a\otimes 1 - 1\otimes a$ es una derivación. Dado un morfismo de $A\otimes A^0$-módulos $\phi\colon \Delta \to I$, entonces $\phi\circ d\colon A\to I$, $a\mapsto \phi(da)$ es una derivación.

Ambas asignaciones son inversas entre sí. □

4. Proposición: *Sea E una extensión de álgebras de A por el $A\otimes A^o$-módulo I. Entonces,*

$$Aut_{ext.alg}(E) = \mathrm{Der}_k(A,I)$$

Demostración. Las asignaciones $\mathrm{Der}_k(A,I) \to Aut_{ext.alg}(E)$, $D\mapsto \mathrm{Id}+D$, donde $(\mathrm{Id}+D)(e) = e + D(\bar{e})$, (siendo $\bar{e}$ la imagen de e en A) y $Aut_{ext.alg}(E) \to \mathrm{Der}_k(A,I)$, $\phi\mapsto D_\phi$, donde $D_\phi(\bar{e}) = e - \phi(e)$ son inversas entre sí. □

5. Proposición: *Denotemos por Δ_E el núcleo del morfismo $E\otimes E\to E$, $e\otimes e'\mapsto e$ y Δ_A el núcleo del correspondiente morfismo $A\otimes A\to A$. Dada la extensión de álgebras $0\to I\to E\to A\to 0$ se tiene la sucesión exacta de diferenciales*

$$0 \to I \xrightarrow{d} \Delta_E \otimes_{E\otimes E^0} (A\otimes A^0) \to \Delta_A \to 0$$

donde $di := \overline{i\otimes 1 - 1\otimes i}$ para todo $i\in I$.

Demostración. Si tomamos $\mathrm{Hom}_{A\otimes A^0}(-,M)$ se obtiene la sucesión exacta

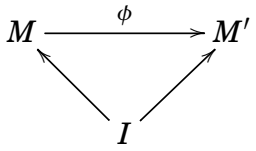
$$0\to \mathrm{Der}_k(A,M) \to \mathrm{Der}_k(E,M) \to \mathrm{Hom}_{A\otimes A^0}(I,M).$$

Por tanto, sólo falta probar que d es inyectivo: Sea $s\colon A\to E$ una sección de k-espacios vectoriales del epimorfismo $\pi\colon E\to A$. La aplicación $\Delta_E\otimes_{E\otimes E^0}(A\otimes A^0)\to I$, $\overline{\sum_i e_i\otimes e_i'} \mapsto \sum_i (e_i - s(\pi(e_i)))\cdot e_i'$ es una sección de d. □

Dar un isomorfismo de E en la extensión trivial equivale a dar una derivación $D: E \to I$ de modo que D sobre I sea el morfismo identidad. Si I es un $A \otimes A^0$-módulo inyectivo y tomamos $\mathrm{Hom}_{A\otimes A^0}(-,I)$ en la sucesión exacta de diferenciales de la proposición anterior, entonces el morfismo $\mathrm{Der}_k(E,I) \to \mathrm{Hom}_{A\otimes A^0}(I,I)$ es epiyectivo y existe una derivación $D: E \to I$ de modo que D sobre I es el morfismo identidad. En conclusión, si I es un $A \otimes A^0$-módulo inyectivo entonces E es isomorfa a la extensión trivial.

Queremos clasificar las extensiones de álgebras de A por el $A \otimes A^o$-módulo I, módulo isomorfismos.

Sea $\mathscr{C}_I$ la categoría de $A \otimes A^o$-módulos que contiene a I, es decir, la categoría cuyos objetos son $A \otimes A^o$-módulos M, dotados de un morfismo de $A \otimes A^o$-módulos $I \to M$. Dados dos objetos $I \to M$, $I \to M'$, los morfismos de $\mathscr{C}_I$ de M en M', son los morfismos de $A \otimes A^o$-módulos $\phi: M \to M'$ que hacen el diagrama siguiente



conmutativo.

Dado un $A \otimes A^o$-módulo $Q \in \mathscr{C}_I$, diremos que un morfismo $R \to Q$ es un recubrimiento de R si el morfismo es inyectivo. Un funtor covariante aditivo F de C_I diremos que es un haz si para todo recubrimiento $R \to Q$, la sucesión

$$F(R) \to F(Q) \rightrightarrows F(Q \oplus_R Q)$$

es exacta. Dado un morfismo inyectivo $R \hookrightarrow Q$ tenemos la sucesión exacta

$$R \to Q \rightrightarrows Q \oplus_R Q \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; Q \oplus_R Q \oplus_R Q \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots$$

Denotemos por $Q^{\cdot}$ el complejo diferencial recién definido. Definimos $H^{\cdot}(Q/R,F) := H^{\cdot}(F(Q^{\cdot}))$.

Dado un morfismo de $A \otimes A^o$-módulos $\phi: I \to R$, tenemos el morfismo $\mathscr{C}_I \to \mathscr{C}_R$, $M \mapsto M_R = R \oplus_I M$. Dada una extensión de álgebras E de A por I, entonces E_R es una extensión de álgebras de A por R.

Sea $\tilde{E}$ el haz de álgebras en C_I definido por $\tilde{E}(R) := E_R$, que contiene el haz de ideales $\tilde{I}$, definido por $\tilde{I}(R) = R$, cuyo conúcleo es el haz de álgebras constante A. El haz de automorfismos de álgebras $\tilde{E}$, $Aut(\tilde{E})$, que son la identidad sobre $\tilde{I}$ e A, coincide con $\mathrm{Der}_k(A,-) = \mathrm{Hom}_{A\otimes A^o}(\Delta,-)$. Por tanto, dado un módulo inyectivo Q y una inyección $I \hookrightarrow Q$, tenemos que $H^1(Q/I, Aut(\tilde{E})) = Ext^1_{A\otimes A^o}(\Delta,I) = Ext^2_{A\otimes A^o}(A,I)$ (donde la última igualdad se deduce de tomar $\mathrm{Hom}_{A\otimes A^o}(-,I)$, en la sucesión exacta $0 \to \Delta \to A \otimes A \to A \to 0$). Ahora ya tenemos el siguiente teorema.

6. Teorema : *Hay tantas extensiones de álgebras de A por I, módulo isomorfismos, como elementos de $Ext^2_{A\otimes A^o}(A,I)$.*

Demostración. Si $Q = \mathrm{Hom}_k(A\otimes A^o, I)$ entonces es un $A\otimes A^o$-módulo inyectivo, porque $\mathrm{Hom}_{A\otimes A^o}(-,Q) = \mathrm{Hom}_k(-,I)$. Además toda extensión B de álgebras de A por Q es trivial: Dar un isomorfismo de extensiones de álgebras de B en la extensión trivial equivale a dar una derivación de B en Q, que sobre Q sea la identidad. Veamos que tal derivación existe. Consideremos la sucesión exacta

$$0 \to Q \to B \to A \to 0$$

y sea la sucesión exacta de diferenciales asociada

$$0 \to Q \to \Delta_B \otimes_{B\otimes B^o} (A\otimes A^o) \to \Delta_A \to 0$$

Si tomamos $\mathrm{Hom}_{A\otimes A^o}(-,Q) = \mathrm{Hom}_k(-,I)$ en esta sucesión exacta obtenemos el epimorfismo

$$\mathrm{Hom}_{A\otimes A^o}(\Delta_B \otimes_{B\otimes B^o} (A\otimes A^o), Q) = \mathrm{Der}_k(B,Q) \to \mathrm{Hom}_{A\otimes A^o}(Q,Q)$$

que prueba la existencia de la derivación buscada.

Con todo, sea E la extensión trivial,

$$\{\text{Extensiones de } A \text{ por } I, \text{ módulo isomorfismos}\} = H^1(Q/I, Aut(\tilde{E})) = Ext^2_{A\otimes A^o}(A,I)$$

□

Capítulo 19

Esquema de Hilbert y de Picard

19.1. Introducción

Hablemos sin rigor. Sea X un esquema proyectivo. Nos proponemos dotar al conjunto $\mathrm{Hilb}(X)$ de los subesquemas cerrados de X de estructura de esquema algebraico. Definiendo una inmersión cerrada $X \hookrightarrow \mathbb{P}_n(k)$, es fácil ver que si construimos el Hilbert de cerrados de $\mathbb{P}_n(k) = \operatorname{Proj} k[x_0,\dots,x_n]$, el Hilbert de cerrados de X es un cerrado del Hilbert de cerrados de $\mathbb{P}_n(k) = \operatorname{Proj} k[x_0,\dots,x_n]$.

En este capítulo damos una construcción elemental del esquema de Hilbert de cerrados de una variedad proyectiva, usando únicamente la teoría de módulos graduados y los criterios estándar de platitud. Consideremos el morfismo de proyectivización $\pi\colon \mathbb{A}^{m+1}\setminus\{0\} \to \mathbb{P}^m$, cada cerrado $C \subseteq \mathbb{P}^m$ define una variedad homogénea de $\mathbb{A}^{m+1}$, el cierre esquemático de $\pi^{-1}(C)$. El esquema de Hilbert de cerrados de $\mathbb{P}^m$ es unión de componentes del esquema de Hilbert de subvariedades homogéneas de $\mathbb{A}^{m+1}$. Basta construir éste último (19.2.10), lo cual es un problema esencialmente afín, donde no aparecen los grupos de cohomología superiores.

Grothendieck construyó el esquema de Hilbert de cerrados de una variedad proyectiva en [11]. El punto central de la construcciones estándar de tal esquema se basa en una versión de Serre's Vanishing Theorem.

Teorema 1: Sea $p(n) \in \mathbb{Q}[n]$. Existe un $r \in \mathbb{N}$, de modo que para todo subesquema cerrado $C \subset \mathbb{P}^m$ de polinomio de Hilbert $p(n)$, se verifica que

1. $H^i(\mathbb{P}^m, \mathscr{O}_C(n)) = 0$ y $H^i(\mathbb{P}^m, \mathfrak{p}_C(n)) = 0$, para todo $i > 0$ y $n \geq r$.

2. Los morfismos de multiplicación

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(n)) \times H^0(\mathbb{P}^m, \mathscr{O}_C(r)) \to H^0(\mathbb{P}^m, \mathscr{O}_C(n+r))$$

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(n)) \times H^0(\mathbb{P}^m, \mathfrak{p}_C(r)) \to H^0(\mathbb{P}^m, \mathfrak{p}_C(n+r))$$

son epiyectivos, para todo $n \geq 0$.

3. $\mathfrak{p}_C(r)$ está generado por sus secciones globales.

Teorema que es probado con la herramienta de los haces m-regulares [20], o directamente en una demostración elaborada en [34]. Para nosotros el teorema central (19.2.6) será:

Teorema 2: Sea $p(n) \in \mathbb{Q}[n]$. Existe un $r \in \mathbb{N}$, de modo para todo ideal homogéneo $I \subseteq k[x_0,\ldots,x_n]$ tal que $k[x_0,\ldots,x_n]/I$ es un anillo de polinomio de Samuel $p(n)$ (en el origen), se verifica que

1. I está generado por los elementos homogéneos de grado menor que r.

2. $\dim_k[k[x_0,\ldots,x_n]/I + (x_0,\ldots,x_n)^m] = p(m)$, para $m \geq r$.

Teorema que es de demostración casi inmediata y no hace uso de los grupos de cohomología superiores.

Finalmente damos dos líneas de construcción del esquema de Hilbert de subesquemas homogéneos cerrados de $\mathbb{A}^{m+1}$ de función de Samuel $p(n)$. La primera lo construye , como el límite proyectivo de las Grasmannianas de ideales homogéneos I de $k[x_0,\ldots,x_m]/(x_0,\ldots,x_m)^{n+1} = R$, tales que $dim_k R/I = p(n)$ (límite que estabiliza para $n >> 0$, luego se tienen las ecuaciones del esquema de Hilbert de subesquemas homogéneos). La segunda, al modo clásico, lo construye como el subesquema de la Grassmanniana de subespacios vectoriales de $\bigoplus_{i=0}^{r} k[x_0,\ldots,x_m]_i$ de codimensión $p(r)$, que se anulan sobre un cerrado homogéneo de $\mathbb{A}^{m+1}$ de función de Samuel $p(n)$. Para ello es necesaria la "flatenning stratification" de Grothendieck. Nosotros damos un ligera generalización, Teorema 19.3.2, que probamos de modo casi inmediato, usando sólo la teoría de módulos graduados y los criterios de platitud estándar.

Una vez que hemos dotado al conjunto de cerrados de una variedad proyectiva de estructura de esquema, podremos dotar de estructura de esquema:

1. Al conjunto de homomorfismos entre dos variedades proyectivas, X e Y pues será el subconjunto de cerrados que son gráficas en el conjunto de todos los cerrados de $X \times Y$.

2. Al conjunto cociente de una variedad X por una relación de equivalencia, pues será el subconjunto de cerrados que son clases en el conjunto de todos los cerrados de X.

3. Al conjunto de divisores de un variedad.

4. Al conjunto de haces de línea de una variedad, pues es el conjunto cociente de la variedad de divisores de una variedad, por la relación de equivalencia lineal.

Un problema fundamental en Geometría Algebraica es la clasificación de todas las curvas. Es decir, la construcción como esquema del conjunto de todas las curvas no singulares, salvo isomorfismos. Variedad que se denomina el móduli de curvas. Esta teoría necesita del Hilbert y los cocientes por relaciones de equivalencia, y de la teoría de invariantes (por grupos de automorfismos) por ello no la desarrollamos aquí.

La clasificación de variedades abelianas (variedades propias con estructura de grupo) es algorítmicamente factible. Por tanto, la clasificación de las curvas lisas puede abordarse a través de la clasificación de las variedades jacobianas (variedad abeliana que parametriza los haces de línea de una curva de grado g, módulo la equivalencia lineal) y la caracterización de las variedades abelianas que son jacobianas (problema de Schottky). Por ello, procederemos al estudio de la jacobiana de una curva. En primer lugar probaremos, como parece obvio, que $S^nC := C^n/S_n$ (donde el grupo simétrico S_n opera en C^n de modo natural permutando los factores) parametriza los divisores de grado n de la curva C. Probamos que el morfismo de contracción de Abel $A : S^gC \to J_C$, que asigna a cada divisor de grado g el haz de línea asociado, es un morfismo birracional, que se obtiene como explosión a lo largo de la subvariedad de haces de línea especiales. Probamos que el espacio vectorial de las secciones del dualizante de S^nC se identifica con el álgebra exterior n del espacio vectorial de las secciones del dualizante de C, lo que nos permitirá demostrar que el morfismo de $S^{g-1}C$ en $\mathbb{P}^{g-1}$ definido por el dualizante ramifica en el dual de C. De aquí obtendremos el teorema de Torelli, que afirma esencialmente, que los automorfismo de J_C que dejan estable $A(S^{g-1}C)$ se identifican con los automorfismos de C. Además, quedan fundamentados los conocimientos básicos para la reconstrucción de la curva (S^gC y el morfismo de contracción de Abel) en términos de la variedad abeliana "'polarizada" J_C, $A(S^{g-1}C)$, lo cual permitirá resolver con éxito el problema de Schottky.

19.2. Esquema de Hilbert

Queremos probar la representabilidad de los funtores $Quot(F/X/S)$, que representan el conjunto de cocientes planos de un módulo coherente F, sobre un esquema proyectivo X sobre un esquema noetheriano S. Para simplificar notaciones, lo probaremos sólo para $F = \mathcal{O}_X$.

Sea A un anillo y $R = A[x_0,\dots,x_n]$. Dado un R-módulo graduado M denotaremos $[M]_n$ el A-submódulo de sus elementos homogéneos de grado n.

Cada ideal homogéneo $I \subset R$ define un subesquema cerrado $C_I = \mathrm{Proj}R/I$ de $\mathbb{P}^m_A$. Dos ideales homogéneos I e I' definen el mismo subesquema cerrado si y sólo si $[I]_n = [I']_n$ para todo $n \geq m$, para cierto m. Dos ideales homogéneos I e I' definen el mismo subesquema cerrado si y sólo si $I_{x_i} = I'_{x_i}$ para todo i. Diremos que los ideales

homogéneos que definen el mismo subesquema cerrado son equivalentes, y llamaremos saturado al mayor de todos, también diremos que este último es el ideal generado por todas las funciones homogéneas que se anulan en el cerrado de marras.

1. Proposición: *Un ideal homogéneo de $k[x_0,\dots,x_m]$ es saturado si y sólo si el ideal irrelevante no es una componente sumergida de su descomposición primaria.*

Demostración. Sea I un ideal homogéneo e $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{q}$ una descomposición primaria reducida por ideales primarios homogéneos y supongamos que el radical de $\mathfrak{q}$ es $(x_0,\dots,x_n)$. I' es un ideal homogéneo equivalente a I si y sólo si $I' = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{q}'$, donde el radical de $\mathfrak{q}'$ es $(x_0,\dots,x_n)$ o bien $\mathfrak{q}'$ no aparece en la descomposición primaria, porque I es equivalente a I' si y sólo si $I_{x_i} = I'_{x_i}$, para todo i. Por tanto, el ideal saturado equivalente a I es $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, que es el que cumple que el ideal irrelevante no es una componente sumergida. □

La descomposición primaria de un ideal localiza. Por tanto, dado un subesquema cerrado de un esquema noetheriano podemos hablar de las componentes sumergidas y las no sumergidas.

Dado un ideal homogéneo I saturado y una descomposición primaria reducida $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$,por ideales homogéneos primarios, tenemos que $[I_{x_i}]_0 = [\mathfrak{q}_{1x_i}]_0 \cap \ldots \cap [\mathfrak{q}_{nx_i}]_0$. Por tanto, las componentes sumergidas o no de $C_I = \mathrm{Proj}\, R/I$ son las proyectivizaciones de las componentes (sumergidas o no) del "cono" $\mathrm{Spec}\, R/I$.

2. Definición: Sea $I \subset R$ un ideal homogéneo saturado, que define el cerrado C_I. Diremos que el anillo de funciones homogéneas de C_I es R/I. Dada una función homogénea $f \in R$ diremos que la hipersuperficie que define $H_f = \mathrm{Proj}\, R/(f)$ corta transversalmente a C_I, si f no es divisor de cero en R/I.

Sea $A = k$ cuerpo e I un ideal homogéneo saturado. Una hipersuperficie H_f corta transversalmente a C_I si y sólo si H_f no pasa por ninguna de las componentes (sumergidas o no) de C_I. Si k contiene infinitos elementos existe un hiperplano que corta transversalmente a C_I.

3. Definición: Dado un ideal homogéneo $I \subset k[x_0,\dots,x_m] = R$ diremos que $p(n) = \dim_k [R/I]_n$ (resp. $\sum_{i=0}^{n-1} p(i)$) es la función de Hilbert (resp. de Samuel) de I. Si $C \subset \mathbb{P}_n$ es una subvariedad proyectiva, diremos que el polinomio de Samuel (resp. de Hilbert) de C es el polinomio de Samuel del ideal homogéneo de todas las funciones que se anulan en C.

El grado del polinomio de Hilbert de I coincide con la dimensión de la variedad proyectiva definida por I. Todos los ideales homogéneos equivalentes tienen el mismo polinomio de Hilbert.

4. Definición: Diremos que la función de Samuel de I, p(n) es polinomio a partir de m si coincide con el polinomio de Samuel, para todo $n \geq m$.

Igualmente podemos hablar de cuándo la función de Hilbert es polinomio. La función de Samuel es polinomio a partir de m si y sólo si la función de Hilbert es polinomio a partir de m.

5. Lema de Nakayama graduado: *Si M es un $k[x_0,\dots,x_n]$-módulo graduado finito generado y $\mathfrak{m} = (x_0,\dots,x_n)$, entonces $\mathfrak{m}M = M$ si y sólo si $M = 0$.*

Demostración. Si $\mathfrak{m}M = M$ y $m \in M$ es un elemento no nulo homogéneo de grado mínimo es claro que $m \notin \mathfrak{m}M = M$. En conclusión, $M = 0$.

□

6. Teorema: *Sea $p(n) \in \mathbb{Q}[n]$. Existe un $r \in \mathbb{N}$, de modo que para todo ideal homogéneo $I \subset k[x_0,\dots,x_n] = R$ de polinomio de Samuel $p(n)$, se verifica*

1. *I está generado por sus elementos homogéneos de grado menor o igual que r. Equivalentemente, todas las funciones homogéneas de grado $m > r$ están generadas por las de grado r.*

2. *La función de Samuel de I es polinomio a partir de r.*

Demostración. Por cambio de cuerpo base, podemos suponer que k es algebraicamente cerrado. Vamos a proceder por inducción sobre el grado del polinomio de Samuel. Si I es de polinomio de Samuel constante 0, el teorema es obvio.

Así que vamos a suponer como hipótesis de inducción que el teorema es cierto para I saturado cuyo polinomio de Samuel es de grado menor o igual que $s-1$.

Supongamos I de polinomio de Samuel $p(n)$ de grado s. Sea I' el ideal homogéneo saturado equivalente a I, cuyo polinomio de Samuel es $p(n)-a$, con $a \geq 0$ y cuyo polinomio de Hilbert es $p(n)-p(n-1)$.

Sea H_f un hiperplano que corte transversalmente a $C_{I'}$. Consideremos el diagrama

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I' & \xrightarrow{f.} & I' & \longrightarrow & I'/fI' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R & \xrightarrow{f.} & R & \longrightarrow & R/(f) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R/I' & \xrightarrow{f.} & R/I' & \longrightarrow & R/(I',f) & \longrightarrow & 0
\end{array}$$

cuya tercera columna es exacta por el lema de la serpiente, aplicado sobre las dos primeras columnas.

(*) De la fila exacta inferior, obtenemos que el polinomio de Samuel de (I', f) es el polinomio de Hilbert de I'. Por hipótesis de inducción, sabemos que existe un r', de modo que (I', f) está generado por sus elementos de grado menor o igual que r' y su función de Samuel es polinomio a partir de r'. Luego, I' está generado por sus elementos de grado menor o igual que r' (por el Lema de Nakayama graduado aplicado a la fila exacta superior) y su función de Samuel es polinomio a partir de r'.

Observemos que $0 \leq p(r') - a$, luego $0 \leq a \leq p(r')$. Como $\dim_k I'/I = a$, no puede ocurrir que $[I]_{r'+i} \subsetneq [I']_{r'+i}$ para todo $0 \leq i \leq p(r')$. En conclusión, $[I]_{r'+p(r')} = [I']_{r'+p(r')}$, luego I está generado por sus elementos de grado menor o igual que $r = r' + p(r')$ (determinado por $p(n)$) y su función de Samuel es polinomio a partir de $r = r' + p(r')$. □

7. Proposición: *Sea $p(n) \in \mathbb{Q}[n]$. Existe un $r \in \mathbb{N}$, de modo que para todo ideal homogéneo saturado $I' \subset k[x_0, \ldots, x_m]$ de polinomio de Hilbert $p(n)$, se verifica*

1. *I' está generado por sus elementos homogéneos de grado menor o igual que r.*
2. *La función de Hilbert de I' es polinomio a partir de r.*

Demostración. Arguméntese como en (*) de la demostración de 19.2.6, cambiando la expresión "por hipótesis de inducción" por "por 19.2.6". □

8. Observación: Observemos que el número r de 19.2.6 y 19.2.7 es el mismo y que el número asignado al polinomio $p(n)$ es mayor que el asignado al polinomio $p(n) - p(n-1)$.

9. Definición: Sea R una A-álgebra $\mathbb{N}$-graduada de tipo finito. Diremos que $\operatorname{Spec} R$ es una variedad homogénea afín sobre $\operatorname{Spec} A$. Sea S un esquema y R una $\mathcal{O}_S$-álgebra $\mathbb{N}$-graduada de tipo finito. Diremos que el esquema obvio $\operatorname{Spec} R$, es una variedad homogénea sobre S (X localmente sobre los abiertos afines de S es una variedad homogénea afín).

10. Teorema: *Sea S un esquema localmente noetheriano y consideremos una variedad homogénea X sobre S. El funtor*

$$\underline{\operatorname{Hilbhom}}_{X/S} : \left[\begin{array}{c} S\text{-esquemas localmente} \\ \text{noetherianos} \\ T \end{array} \right] \begin{array}{l} \rightsquigarrow \text{ Conjuntos} \\ \rightsquigarrow \text{ Subesquemas homogéneos cerrados} \\ \quad \text{de } X_T \text{ planos sobre } T \end{array}$$

es representable por un esquema que es unión disjunta de esquemas localmente proyectivos sobre S.

Demostración. Como $\underline{\mathrm{Hilbom}}_{X/S}$ es un haz puede suponerse que $S = \mathrm{Spec}\, A$ (siendo A un anillo noetheriano) y que $X = \mathrm{Spec}\, R$ (siendo R una A-álgebra $\mathbb{N}$-graduada de tipo finito). Podemos pensar X como subvariedad homogénea de $\mathbb{A}^{m+1} = \mathrm{Spec}\, A[x_0,\dots,x_m]$. Basta probar que $\underline{\mathrm{Hilbom}}_{\mathbb{A}^{m+1}/S}$ es representable porque $\underline{\mathrm{Hilbom}}_{X/S}$ es un subfuntor cerrado de $\underline{\mathrm{Hilbom}}_{\mathbb{A}^{m+1}/S}$.

$\underline{\mathrm{Hilbom}}_{\mathbb{A}^{m+1}/S} = \coprod_{\varphi(n)} \underline{\mathrm{Hilbom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$, donde $\underline{\mathrm{Hilbom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$ es el funtor de los subesquemas homogéneos cerrados de $\mathbb{A}^{m+1}$ de función de Samuel $\varphi(n)$. Veamos que este último funtor es representable. Sea el $r \in \mathbb{N}$ del teorema 19.2.6. Demos dos demostraciones.

1. Sea $B_n = A[x_0,\dots,x_m]/(x_0,\dots,x_m)^{n+1}$ y para $i \le n$ sea R_i los elementos homogéneos de grado i y escribamos $\phi(n) = \varphi(n) - \varphi(n-1)$. Consideremos la sucesión de epimorfismos naturales $\cdots \to B_{n+1} \to B_n \to \cdots \to B_r$. En cada R_i consideremos la Grassmannianna de subespacios vectoriales de codimensión $\phi(i)$, $G_\phi(R_i)$. Sea $G'(B_n)$ el subesquema cerrado de la Grassmanniana de B_n, $\prod_{i=0}^{n} G_\phi(R_i)$. Sea $G''(B_n)$ la Grassmannianna de ideales de B_n, que es un cerrado de la Grassmanniana de B_n. Sea $G(B_n) = G'(B_n) \cap G''(B_n)$, la Grassmanniana de ideales homogéneos de B_n, tal que la codimensión de los elementos homogéneos de grado i en R_i es $\phi(i)$.

Tenemos la sucesión obvia de morfismos (propios, pues la variedades lo son)

$$\cdots \to G(B_{n+1}) \to G(B_n) \to \cdots \to G(B_r)$$

El límite proyectivo de los $G(B_n)$ es el funtor que queremos probar que es representable.

Sean $C_i \subseteq G(B_i)$, la intersección de todas las imágenes esquemáticas de los morfismos $G(B_n) \to G(B_i)$, que por noetherianidad es la imagen esquemática de un $G(B_n)$, para $n >> 0$.

El límite proyectivo de los $G(B_n)$ coincide con el de los C_n.

Como meros conjuntos, C_{i+1} se epiyecta en C_i. Cada punto geométrico de C_i, con $i \ge r$ "levanta a un único punto geométrico del Hilbert homogéneo": Dado un punto geométrico de C_i existe un punto geométrico de C_{i+1} en la fibra, de nuevo existe un punto geométrico de C_{i+2} en la fibra del punto geométrico de C_{i+1}, así sucesivamente construimos un punto del límite proyectivo, es decir un ideal homogéneo $\bigoplus_{s\ge 0} I_s \subset k[x_0,\dots,x_m]$, que está generado por I_r.

Por tanto, los puntos geométricos de C_{i+1} coinciden con los de C_i, para $i \ge r$. Los morfismos de funtores $C_{i+1} \to C_i$ son inyectivos, para $i \ge r$ (pues los elementos de grado $i+1$ de cada ideal están generados por los elementos de grado i, porque así es en fibras).

Por el Main Theorem de Zariski (13.8.14 o [14] III. 11.5) $C_{i+1} = C_i$ para todo $i \ge r$ y coinciden con el límite proyectivo.

Observación 1: Para $n >> 0$ tenemos un epimorfismo $G(B_n) \to C_r$, de nuevo el morfismo entre los funtores de puntos es inyectivo y $G(B_n) = C_r$. Por tanto, $\underline{\mathrm{Hilhom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$ es representable por $G(B_n)$.

2. Sea G_i la Grassmanniana de subespacios vectoriales de $A[x_0,\dots,x_m]_i$, de codimensión $\phi(i)$. Sea $G = \prod_{i=0}^{r} G_i$, $\mathscr{O}_G$ el haz de anillos de G y $I \subset \bigoplus_{i=0}^{r} \mathscr{O}_G[x_0,\dots,x_m]_i$ el subespacio universal, definido por el morfismo identidad $\mathrm{Id}\colon G \to G$. Sea $(I) \subset \mathscr{O}_G[x_0,\dots,x_m]$ el haz de ideales generado por I. Sea $R = \mathscr{O}_G[x_0,\dots,x_m]/(I)$. Pues bien, el funtor F de 19.3.2, coincide con el esquema de Hilbert homogéneo que queremos representar.

Observación 2: De nuevo, usando 19.3.2 (*) obtenemos la observación 1 anterior.

□

Desafortunadamente el anillo de funciones homogéneas B de un subesquema cerrado C de $\mathbb{P}^m_A$ no cambia de base, si el morfismo de cambio de base $A \to A'$ no es plano. El anillo de funciones homogénea de $C_{A'} = C \times_A A'$ es un cociente de $B \otimes_A A'$.

Dado un morfismo de esquemas $X \to Y$, y un punto cerrado $y = \mathrm{Spec}\, k$ de Y, denotamos $X_y = X \times_Y y$ la fibra de y. El lector que conozca los teoremas de anulación de Grauert y Serre (13.10.5 y 13.6.9, o [14] III. 8.8, 12.11), sólo necesita leer en la demostración de la proposición que sigue el apartado 2.

11. Proposición : *Sea A un anillo local noetheriano y $x \in \mathrm{Spec} A$ el punto cerrado. Sea $p(n)$ un polinomio de coeficientes números racionales y r el número natural de la proposición 19.2.7.*

Un subesquema cerrado $C \subseteq \mathbb{P}^m_A$, tal que el polinomio de Hilbert de C_x es $p(n)$, es plano sobre $\mathrm{Spec} A$ $\iff$ *el A-módulo de las funciones homogéneas de grado n de C es libre de rango $p(n)$, para todo $n \geq r$.*

Demostración. Por cambio de base fielmente plano podemos suponer que el cuerpo residual de x tiene infinitos elementos.

Sea I el ideal homogéneo saturado de funciones que se anulan en C. Sea $B = \oplus_n B_n$ el anillo de funciones homogéneas de C.

$\Rightarrow$) 1. Sea H_f un hiperplano de $\mathbb{P}^m_A$ que corte transversalmente a C_x. El subesquema cerrado $C' = C \cap H_f$ es plano sobre A y f/x_i es no divisor de cero en los abiertos $C - H_{x_i}$, por los criterios de platitud (7.7.10 o [18] theorem 22.5) Se cumple que f no es divisor de cero en B: si $f \cdot p_n = 0$ entonces $\frac{f}{x_i} \cdot \frac{p_n}{x_i^n} = 0$, luego $\frac{p_n}{x_i^n} = 0$ y $p_n = 0$.

El polinomio de Hilbert de C'_x es $p(n) - p(n-1)$. Sea B' el anillo de funciones homogéneas de C'. Procedemos por inducción sobre el grado de $p(n)$. Por hipótesis de inducción B'_n son módulos localmente libres de rango $p(n) - p(n-1)$, para $n \geq r$. B' es un cociente de B/fB y para todo $n > s$ ($s >> 0$), $B'_n = [B/fB]_n$.

Consideremos, para $n > s$, las sucesiones exactas,

$$0 \to B_n \xrightarrow{f.} B_{n+1} \to [B/fB]_{n+1} \to 0$$

escinden, luego $B_{n+1} = f[B]_n \oplus [B/fB]_{n+1}$ y $\frac{B_{n+1}}{f^{n+1}} = \frac{B_n}{f^n} \oplus [B/fB]_{n+1}$.

Denotemos $U = C - H_f$ y $\mathcal{O}_C$ el haz de funciones de C. Tenemos que $\mathcal{O}_C(U) = \varinjlim_{n>s} \frac{B_n}{f^n} \simeq \varinjlim_{n\geq t} \frac{B_n}{f^n} \simeq \frac{B_t}{f^t} \oplus (\bigoplus_{n>t} [B/fB]_n)$, para $t > s$. $\mathcal{O}_C(U)$ es un A-módulo plano, luego $\frac{B_t}{f^t} \simeq B_t$ es un A-módulo libre. B_t es un módulo libre de rango $p(t)$, para $t >> 0$, como se observa calculando su dimensión al pasar a la fibra en x.

2. Probemos que B_n es libre de rango $p(n)$, para $n \geq r$, por inducción descendente:

Sea B^x el anillo de las funciones homogéneas de C_x. La dimensión de B^x_n es $p(n)$, para $n \geq r$. Denotemos por B'^x el anillo de funciones homogéneas de C'_x. La dimensión de B'^x_n es $p(n) - p(n-1)$, para $n \geq r$.

Consideremos las sucesiones de filas exactas, para $n \geq r$,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B_n & \xrightarrow{f.} & B_{n+1} & \longrightarrow & B_{n+1}/fB_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B^x_n & \xrightarrow{f.} & B^x_{n+1} & \longrightarrow & B^x_{n+1}/fB^x_n & \longrightarrow & 0 \end{array}$$

Suponemos que B_{n+1} es libre de rango $p(n+1)$, luego $B_{n+1} \otimes_A k(x) = B^x_{n+1}$ (donde $k(x)$ es el cuerpo residual de x). Por tanto, si tensamos la fila exacta superior por $\otimes_A k(x)$, obtenemos que $(B_{n+1}/fB_n) \otimes_A k(x)$ coincide con B^x_{n+1}/fB^x_n, que es de dimensión $p(n+1) - p(n)$. Luego B_{n+1}/fB_n coincide con el módulo libre cociente B'_{n+1} y B_n es libre de rango $p(n)$.

$\Leftarrow$) Sea H_f un hiperplano que corte transversalmente a C_x.

Para $m \geq r$, B_m es un A-módulo libre de rango $p(m)$, además la función de Hilbert a partir de r es polinomio, luego $B_m \otimes_A k(x)$ coincide con las funciones homogénea de grado m de C_x. Para $m \geq r$ los morfismos $B_m \xrightarrow{f.} B_{m+1}$ son inyectivos, porque es inyectivo en la fibra de x. Denotemos $U = C - H_f$. Tenemos que $\mathcal{O}_C(U) = \varinjlim_{m>r} \frac{B_m}{f^m} \simeq \varinjlim_{m>r} B_m$, luego es plano. Como los abiertos U (variando f) recubren, concluimos que C es plano sobre $\operatorname{Spec} A$.

□

12. Teorema: *Sea S un esquema localmente noetheriano y $X \to S$ un morfismo local-*

mente proyectivo. El funtor de Hilbert

$$\underline{\mathrm{Hilb}}_{X/S}: \begin{bmatrix} S\text{-esquemas localmente} \\ \text{noetherianos} \\ T \end{bmatrix} \begin{array}{l} \rightsquigarrow \text{ Conjuntos} \\ \rightsquigarrow \text{ Subesquemas cerrados de } X_T \\ \quad \text{planos sobre } T \end{array}$$

es representable por un esquema que es unión disjunta de esquemas localmente proyectivos sobre S.

Demostración. Como el funtor de Hilbert es haz, puede suponerse que $S = \operatorname{Spec} A$ es afín noetheriano conexo y $X \to S$ es un morfismo proyectivo. Consideremos una inmersión cerrada $X \hookrightarrow \mathbb{P}^m_A$.

Basta demostrar que el Hilbert de subesquemas cerrados de $\mathbb{P}^m_A$ es representable, porque el Hilbert cerrados de X es un cerrado del de $\mathbb{P}^m_A$.

$\underline{\mathrm{Hilb}}_{\mathbb{P}^m_A/S} = \coprod_{p(n)} \underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m_A/S}$, donde $\underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m_A/S}$ es el funtor de los subesquemas cerrados de $\mathbb{P}^m_A$ de polinomio de Hilbert $p(n)$.

Sea $r \in \mathbb{N}$ de 19.2.7. Sea $\phi(n) = 0$ si $n < r$ y $\phi(n) = p(n)$ si $n \geq r$. Sea $\varphi(n) = \sum_{i=0}^{n-1} \phi(n)$.

Tenemos un morfismo natural $\pi: \underline{\mathrm{Hilhom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S} \to \underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m/S}$, que asigna a cada variedad homogénea su proyectivización, o equivalentemente, a cada ideal homogéneo su variedad proyectiva. El morfismo $\underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m/S} \to \underline{\mathrm{Hilhom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$ que asigna a cada subvariedad proyectiva C, el ideal homogéneo I, tal que $I_n = H^0(X, \mathfrak{p}_C(n))$ para $n \geq r$ y $I_n = 0$ para $n < r$, es el inverso de π. En conclusión, $\underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m/S}$ es representable puesto que lo es $\underline{\mathrm{Hilhom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$. □

En observación 1 y 2 de 19.2.10 hemos obtenido las ecuaciones de $\underline{\mathrm{Hilhom}}^{\varphi(n)}_{\mathbb{A}^{m+1}/S}$, por tanto, tenemos las ecuaciones de $\underline{\mathrm{Hilb}}^{p(n)}_{\mathbb{P}^m/S}$, resultado que puede encontrarse en [6]

19.3. Estratificación plana de Grothendieck

1. Lema: *Sea A un anillo noetheriano y R una A-álgebra $\mathbb{N}$-graduada de tipo finito. Si $M = \bigoplus_{n\in\mathbb{N}} M_n$ es un R-módulo finito generado graduado, entonces $U := \{x \in \operatorname{Spec} A : M_x$ es un A_x-módulo plano$\}$ es un abierto de* $\operatorname{Spec} A$.

Demostración. Tenemos que probar que U satisface las dos condiciones del criterio topológico de Nagata (7.7.13 o [18] theorem 24.2):

1. Estabilidad por generalizaciones: $\bar{x}\cap U\neq\emptyset\Rightarrow x\in U$ (denotamos por $\bar{x}$ el cierre de x en $\operatorname{Spec}A$).

2. Si $x\in U$ entonces $\bar{x}\cap U$ es un entorno abierto de $x\in\bar{x}$.

Obviamente U es estable por generalizaciones. Veamos que U satisface 2. Sea $x\in U$ e $y\in\bar{x}$. Sea $\mathfrak{p}_x$ el ideal de A definido por x y sea $\bar{A}=A/\mathfrak{p}_x$. Entonces,

M_y es un A_y-módulo plano $\iff$ $(M_n)_y$ es un A_y-módulo plano para todo $n\in\mathbb{N}$ $\iff$ $\operatorname{Tor}_1((M_n)_y,\bar{A})=0$ y $(M_n)_y/\mathfrak{p}_x(M_n)_y$ es un $\bar{A}$-módulo plano para todo $n\in\mathbb{N}$ $\iff$ $\operatorname{Tor}_1(M_y,\bar{A})=0$ y $M_y/\mathfrak{p}_xM_y$ es un $\bar{A}$-módulo plano.

Ahora, $\operatorname{Tor}_1(M,\bar{A})_x=\operatorname{Tor}_1(M_x,\bar{A})=0$, por lo que es cero en un entorno de x (porque $\operatorname{Tor}_1(M,\bar{A})$ es un R-módulo finito generado). Además, $M/\mathfrak{p}_xM$ es un $\bar{A}$-módulo plano en un entorno de x en $\bar{x}$ por el lema de platitud genérica (7.7.14 o [18] theorem 24.1). Hemos terminado. □

Dados dos aplicaciones $\phi_1,\phi_2\colon\mathbb{N}\to\mathbb{N}$, diremos que $\phi_1<\phi_2$, si existe un $n\in\mathbb{N}$, de modo que $\phi_1(n)<\phi_2(n)$ y $\phi_1(m)\leq\phi_2(m)$, para todo $m>n$. En el conjunto de las aplicaciones, que para $n>>0$ son polinómicas, esta relación de orden es total.

2. Teorema : *Sea A un anillo noetheriano y R una A-álgebra, $\mathbb{N}$-graduada, de tipo finito. Sea $\phi\colon\mathbb{N}\to\mathbb{N}$ una aplicación. El funtor sobre los anillos (o esquemas afines) definido por*

$$F(S):=\{\operatorname{Spec}S\to\operatorname{Spec}A:\ [R\otimes_A S]_n \text{ es loc. libre de rango } \phi(n), \text{ para cada } n\}$$

es representable por un subesquema (un cerrado de un abierto) de $\operatorname{Spec}A$.

Existen sólo un número finito de aplicaciones $\phi_1<\phi_2<\cdots<\phi_m$, de modo que los funtores asociados a cada ϕ_i, F_{ϕ_i}, son no vacíos. Además, los funtores F_{ϕ_i} están representados por subesquemas X_{ϕ_i}, de modo que existe una filtración de cerrados $\operatorname{Spec}A=C_0\supset C_1\supset\cdots\supset C_m=\emptyset$, de modo que topológicamente $X_{\phi_i}=C_{i-1}-C_i$, para todo i.

(*) Para $s>>0$ el funtor

$$F_s(S):=\{\operatorname{Spec}S\to\operatorname{Spec}A:\ [R\otimes_A S]_n \text{ es loc. libre de rango } \phi(n), \text{ para cada } n\leq s\}$$

coincide con el funtor F.

Demostración. Sea $\varphi\colon\operatorname{Spec}S\to\operatorname{Spec}A$, perteneciente a $F(S)$. Sea $F_{\phi(n)-1}(R_n)$ el ideal de Fitting $(\phi(n)-1)$-ésimo de R_n. Se cumple que $F_{\phi(n)-1}(R_n)=0$ en S. Sea el cerrado $C=\bigcap_n(F_{\phi(n)-1}(R_n))_0\subseteq\operatorname{Spec}A$. Por la teoría de los ideales de Fitting, es fácil demostrar que φ valora en C. Podemos restringirnos a este cerrado, que seguiremos llamando

$\operatorname{Spec} A$. Si $x \in \operatorname{Im}\varphi$, entonces $x \in \operatorname{Spec} A - (F_{\phi(n)}(R_n))_0$, para todo n; por la teoría de los ideales de Fitting, $(R_n)_x$ es un A_x-módulo plano. Por el lema anterior, existe un entorno abierto de x, que podemos suponer conexo, en el que R_x es un A_x-módulo plano. En todos los puntos de este entorno conexo los R_n son localmente libres del mismo rango, $\phi(n)$. En conclusión, el conjunto de puntos de $\operatorname{Spec} A$, donde cada R_n es localmente libre de rango $\phi(n)$, es un abierto, el cual representa a F.

Para cada punto $x \in \operatorname{Spec} A$, cerrado o no, si consideramos la función $\phi_x(n) = \dim_{k(x)} R_n \otimes_A k(x)$, tendremos que $x \in X_{\phi_x}$. Por la noetherianidad de $\operatorname{Spec} A$ existen $\phi_1, \ldots, \phi_m$, de modo que $\operatorname{Spec} A = \coprod_i X_{\phi_i}$. Reordenando, podemos escribir $\phi_1 < \ldots < \phi_m$. Existe $m_i \in \mathbb{N}$, de modo que $\phi_1(m_i) < \phi_i(m_i)$. Así pues, dado $x \in X_{\phi_1}$ existen entornos U_i, de modo que $U_i \cap X_{\phi_i} = \emptyset$. Por tanto, X_{ϕ_1} es un abierto. Sea $C_1 = \operatorname{Spec} A - X_{\phi_1}$. Restringiéndonos a C_1, del mismo modo construiremos C_2, etc.

Probemos la existencia de s. Tenemos que $\operatorname{Spec} A = X_{\phi_1} \coprod \overset{m}{\ldots} \coprod X_{\phi_m}$. Si ϕ es distinta de todos los ϕ_i, existe un s de modo que ϕ es distinta a todos los ϕ_i sobre $\{0, 1, \ldots, s\}$. Entonces $F_s = \emptyset = F$. En otro caso, denotemos por X_t el subesquema de $\operatorname{Spec} A$ que representa al funtor, F_t, $t \in \mathbb{N}$. Sea r tal que las funciones $\{\phi_1, \ldots, \phi_m\}$ sean distintas sobre $\{0, 1, \ldots, r\}$. Tenemos la cadena de subesquemas $X_r \supseteq X_{r+1} \supseteq X_{r+2} \supseteq \cdots$, de modo que topológicamente son el morfismo identidad. Por noetherianidad, para un $s >> 0$ estabiliza, luego $X_\phi = X_s$ y $F = F_s$.

□

3. Corolario : *Sea* $\operatorname{Spec} A$ *noetheriano reducido y conexo, y* $C \subseteq \mathbb{P}^n_A$ *un subesquema cerrado. Entonces,* C *es plano sobre* $\operatorname{Spec} A$ *si y sólo si el polinomio de Hilbert de* $C_x = C \times_A A/\mathfrak{m}_x$ *no depende del punto cerrado* $x \in \operatorname{Spec} A$.

Demostración. Sea R la A-álgebra de funciones homogéneas de C, $\phi_1 < \ldots < \phi_m$ las aplicaciones del teorema anterior y $\operatorname{Spec} A = C_0 \supset C_1 \supset \cdots \supset C_m = \emptyset$, la estratificación plana asociada.

$\Rightarrow$) Podemos suponer que $\operatorname{Spec} A$ es irreducible (y reducido). Por la proposición 19.2.11, para cada punto cerrado $x \in \operatorname{Spec} A$, existe un n_x de modo que $(R_n)_x$ es libre, para todo $n \geq n_x$. Dado $x \in C_{m-1}$ y $n \geq n_x$, en un entorno abierto de x, R_n es libre de rango de $\phi_m(n)$ y en el abierto $\operatorname{Spec} A - C_1$ es localmente libre de rango $\phi_1(n)$. Como $\operatorname{Spec} A$ es irreducible, estos dos abiertos no son disjuntos y $\phi_1(n) = \phi_m(n)$. Luego, $\phi_1(n) = \ldots = \phi_m(n)$, para todo $n \geq n_x$. Luego, B_n es localmente libre de rango constante para cada $n \geq n_x$ y el polinomio de Hilbert no depende del punto x considerado.

$\Leftarrow$) Existe n' de modo que $\phi_1(n) = \cdots = \phi_m(n)$, para todo $n > n'$. Entonces, $\dim_{A/\mathfrak{m}_x} R_n \otimes_A A/\mathfrak{m}_x$ no depende de x, para $n > n'$. Entonces, B_n es localmente libre, para $n > n'$, por 0.9.9. Por 19.2.11, C es plano sobre A. □

19.4. Estudio infinitesimal del esquema de Hilbert

Dado un esquema X, denotaremos por $X[\epsilon] = X \times_{\mathbb{Z}} \operatorname{Spec}\mathbb{Z}[x]/(x^2)$. Obviamente X y $X[\epsilon]$ son topológicamente isomorfos y el morfismo $\mathbb{Z}[x]/(x^2) \to \mathbb{Z}$, $\bar{x} \mapsto 0$, define un morfismo natural $i : X \to X[\epsilon]$. $X[\epsilon]$ debe ser entendido geométricamente como "el conjunto de puntos de X, junto con un vector infinitesimal en cada punto".

1. Definición: Llamaremos funtor tangente del S-esquema X, al funtor $T_{X/S}$, definido por

$$T_{X/S}(S') := \left\{ \begin{array}{l} (x,\phi) \in X^{\cdot}(S') \times X^{\cdot}(S'[\epsilon]) : \text{ de modo que el diagrama} \\ \begin{array}{ccc} S'[\epsilon] & \xrightarrow{\phi} & X \\ & {\scriptstyle i}\nwarrow \quad \nearrow{\scriptstyle x} & \\ & S' & \end{array} \quad \text{sea conmutativo} \end{array} \right.$$

Por definición de $T_{X/S}$ tenemos una proyección natural $\pi : T_{X/S} \to X^{\cdot}$ y para cada punto $x : S' \to X$, se verifica que

$$\pi^{-1}(x) = \operatorname{Der}_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{O}_{S'}) = \operatorname{Hom}_{\mathcal{O}_X}(\Omega_{X/S}, \mathcal{O}_{S'})$$

Pues dada $D \in \operatorname{Der}_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{O}_{S'})$ define el morfismo de álgebras $\mathcal{O}_X \to \mathcal{O}_{S'}[\epsilon]$, $a \mapsto a(x) + D(a)\epsilon$, y así es todo morfismo perteneciente a $\pi^{-1}(x)$. Por tanto, $T_{X/S}$ coincide con el funtor de puntos sobre la categoría de X-esquemas del fibrado asociado a $\Omega^*_{X/S}$, es decir, $\operatorname{Proj} S^{\cdot}_X \Omega_{X/S}$.

Denotaremos $\pi^{-1}(x) = T_{X/S,x}$. Si S es el espectro de un cuerpo y $S' = S$, entonces $T_{X/S,x} = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$, donde $\mathfrak{m}_x$ es el ideal maximal de las funciones de X que se anulan en x.

2. Teorema: *Sea S un esquema localmente noetheriano y $X \to S$ un morfismo localmente cuasiproyectivo plano. Sea $x : S \to \operatorname{Hilb}_{X/S}$ el punto correspondiente a un cerrado $C \hookrightarrow X$ propio y plano sobre S. Se cumple que*

$$T_{\operatorname{Hilb}_{X/S},x} = (I/I^2)^*$$

donde I el haz de ideales de las funciones de X que se anulan en C y $*$ el dual como $\mathcal{O}_C$-módulo.

Demostración. Por la definición de funtor tangente y $\operatorname{Hilb}_{X/S}$, $T_{\operatorname{Hilb}_{X/S},x}$ coincide con los cerrados $C' \hookrightarrow X[\epsilon]$ propios y planos sobre $S[\epsilon]$, que por cambio de base $S \hookrightarrow S[\epsilon]$ coinciden con C. En términos de ideales, buscamos los ideales $I' \subset \mathcal{O}_X[\epsilon]$, planos sobre $\mathcal{O}_S[\epsilon]$, tales que $(I', \epsilon) = (I, \epsilon)$. En particular tenemos que $I' \cdot \epsilon = I \cdot \epsilon$. Además, $I' \cap (0 \oplus \mathcal{O}_X \cdot$

$\epsilon) \stackrel{*}{=} I\cdot\epsilon$: Si tensamos la sucesión exacta $\mathscr{O}_S[\epsilon] \xrightarrow{\epsilon\cdot} \mathscr{O}_S[\epsilon] \xrightarrow{\epsilon\cdot} \mathscr{O}_S[\epsilon]$ por $\otimes_{\mathscr{O}[\epsilon]} I'$, obtendremos la sucesión exacta $I' \xrightarrow{\epsilon\cdot} I' \xrightarrow{\epsilon\cdot} I'$ y

$$I' \cap (0 \oplus \mathscr{O}_X \cdot \epsilon) = \operatorname{Ker}\epsilon\cdot = \operatorname{Im}\epsilon\cdot = I'\cdot\epsilon = I\cdot\epsilon$$

Si $a + b\cdot\epsilon \in I'$, entonces $a \in I$. Además fijado a, b es único módulo I, por $*$. En conclusión, existe una (única) $w\colon I \to \mathscr{O}_X/I$, de modo que

$$I'/I\cdot\epsilon = \{a + w(a)\cdot\epsilon \subset \mathscr{O}_X \oplus \mathscr{O}_X/I\cdot\epsilon \mid a \in I\}$$

Recíprocamente dada $w \in \operatorname{Hom}_{\mathscr{O}_X}(I, \mathscr{O}_X/I) = (I/I^2)^*$, podemos reconstruir un ideal I' (para la $\mathscr{O}_S[\epsilon]$-platitud de I' pruébese que $\operatorname{Tor}_1^{\mathscr{O}_S[\epsilon]}(\mathscr{O}_S, I') = 0$ y úsese el criterio local de platitud 7.7.2).

□

19.5. El esquema de homomorfismos

Vamos a ver que el conjunto de morfismos de una variedad proyectiva en otra variedad forman una variedad algebraica. Dar un morfismo $f\colon X \to Y$ equivale a dar su gráfica $\Gamma_f \subseteq X \times Y$. Nos bastará ver que el conjunto de gráficas de $X \times Y$ es un abierto del Hilbert de cerrados de $X \times Y$.

1. Definición: Sean X e Y dos S-esquemas. Se define el funtor de homomorfismos de X en Y sobre la categoría de S-esquemas por la fórmula

$$Hom_S(X,Y)(T) = \operatorname{Hom}_T(X_T, Y_T)$$

2. Teorema: *Sea $X \to S$ un morfismo localmente proyectivo plano e $Y \to S$ un morfismo cuasiproyectivo. Se cumple que el morfismo*

$$\begin{array}{ccc} Hom_S(X,Y) & \to & \underline{\operatorname{Hilb}}_{X\times_S Y/S} \\ f & \mapsto & \Gamma_f \end{array}$$

es una inmersión abierta. Por tanto, $Hom_S(X,Y)$ es representable por un abierto del Hilbert de cerrados de $X \times_S Y$.

Demostración. Tenemos que probar que dado un morfismo $Z^\cdot \to \underline{\operatorname{Hilb}}_{X\times_S Y/S}$, es decir, un subesquema V cerrado de $(X\times_S Y)\times_S Z = X_Z \times_Z Y_Z$ propio y plano sobre Z, entonces

$$F := Hom_S(X,Y) \times_{\underline{\operatorname{Hilb}}_{X\times_S Y/S}} Z^\cdot \to Z^\cdot$$

es una inmersión abierta. $F(T) = \{(f,g)/f\colon X_T \to Y_T$ es el único morfismo (si existe), tal que $\Gamma_f = V \times_Z T\}$. Ahora bien, $V \times_Z T$ es la gráfica de un morfismo si y sólo si la

composición $V \times_Z T \subset (X \times_S Y) \times_S T \to X \times_S T$ es un isomorfismo. Un morfismo entre T-esquemas planos es isomorfismo si y sólo si lo es en fibras sobre T. Tendremos $V \times_Z T \to X \times_S T$ es isomorfismo si y sólo si T valora en el conjunto de puntos de Z, sobre los que $V \to X \times_S Z$ es isomorfismo. Sea $C \subset V$ el cerrado de puntos de V donde el morfismo anterior no sea localmente un isomorfismo, sea $\pi\colon V \to Z$ el morfismo natural. Pues bien, T ha de valorar en el abierto $U = Z - \pi(C)$. Podemos suponer que $Z = U$. En este caso, las fibras del morfismo $V \to X \times_S Z$ son discretas y finitas (no vacías). Sea $U' \subseteq X_Z$ el abierto de puntos cuyas fibras en V sean de un sólo punto y $\pi'\colon X_Z \to Z$ el morfismo natural. Pues bien, $F = (Z - \pi'(X_Z - U'))^{\cdot}$.

□

19.6. Cociente por una relación de equivalencia plana

Todos los esquemas considerados lo son sobre un esquema localmente noetheriano base S.

1. Definición: Sea P un prehaz (es decir, un funtor contravariante en la categoría de los S-esquemas). Diremos que un subhaz $R \hookrightarrow P \times P$ es una relación de equivalencia en P, si para cada S-esquema T, $R(T) \hookrightarrow F(T) \times F(T)$ es una relación de equivalencia de conjuntos.

El prehaz P', $P'(T) := P(T)/R(T)$, cumple que la sucesión de prehaces $R \rightrightarrows P \to P'$ es exacta y $R = P \times_{P'} P$.

2. Definición: Sea F un haz para la topología fielmente plana, sobre la categoría de los S-esquemas. Diremos que un subhaz $R \hookrightarrow F \times F$ es una relación de equivalencia en F, si para cada S-esquema T, $R(T) \hookrightarrow F(T) \times F(T)$ es una relación de equivalencia de conjuntos.

En la categoría de haces para la topología fielmente plana, el cociente de un haz por una relación de equivalencia existe y coincide con el haz asociado al prehaz cociente: Sea el prehaz

$$\bar{F}(S) :\, = \varinjlim_{T \overset{\text{f. plano}}{\to} S} \left[x \in F(T)\colon \pi_1^*(x) R\, \pi_2^*(x)\right]/R(T)$$

donde $\pi_1, \pi_2\colon T \times_S T \to T$ son las proyecciones naturales, y observemos en el límite inductivo que dados dos morfismos $f_1, f_2\colon T' \to T$ y $x \in F(T)$ tales que $\pi_1^*(x) R\, \pi_2^*(x)$ entonces de la composición $T' \overset{(f_1,f_2)}{\to} T \times_S T \overset{\pi_i}{\to} T$, se deduce que $f_1^*(x) R\, f_2^*(x)$. Pues bien, se verifica que $\bar{F}$ es un haz para la topología fielmente plana y que

$$\mathrm{Hom}_{\mathrm{Prehaces}}(F', G) = \mathrm{Hom}_{\mathrm{Haces}}(\bar{F}, G)$$

donde $F'(T) := F(T)/R(T)$ y G es un haz para la topología fielmente plana. Además, el morfismo natural $F' \to \bar{F}$ es inyectivo, la sucesión de haces $R \rightrightarrows F \to \bar{F}$ es exacta y $F \times_{\bar{F}} F = R$.

3. Definición: Un subesquema $R \hookrightarrow X \times_S X$ es una relación de equivalencia en el S-esquema X, si induce una relación de equivalencia en el funtor de puntos, esto es, si para cada S-esquema T, $R^\cdot(T) \hookrightarrow X^\cdot(T) \times X^\cdot(T)$ es una relación de equivalencia de conjuntos.

4. Definición: Diremos que la relación de equivalencia es efectiva (en la topología fielmente plana) si el haz cociente de $X^\cdot$ por la relación de equivalencia $R^\cdot$ es el funtor de puntos de un esquema.

Si denotamos por Z el esquema cociente, entonces la sucesión de conjuntos $\mathrm{Hom}_S(Z,T) \to \mathrm{Hom}_S(X,T) \rightrightarrows \mathrm{Hom}_S(R,T)$ es exacta para todo S-esquema T y $R = X \times_Z X$ ("las fibras del morfismo de paso al cociente $X \to Z$ son las clases de equivalencia").

5. Teorema: *Sea S un esquema noetheriano y $f: X \to S$ un morfismo cuasiproyectivo o proyectivo. Una relación de equivalencia $R \hookrightarrow X \times_S X$ propia y plana sobre X por la segunda proyección es efectiva. El esquema cociente Z es cuasiproyectivo sobre S y el morfismo $X \to Z$ de paso al cociente es propio y plano.*

Demostración. Expongamos primero la línea argumental de la demostración. Sea H el esquema de Hilbert de X y $W \hookrightarrow X \times_S H$ el "cerrado universal", es decir, el cerrado de $X \times_S H$ definido por el morfismo $\mathrm{Id}: H \to H$, o equivalentemente el conjunto de puntos (x,h) de $X \times_S H$, tales que x es un punto del cerrado definido por h. Tenemos un morfismo natural $X \hookrightarrow W$, $x \mapsto (x,[x])$, donde $[x]$ es la clase de equivalencia de x por la relación R, es decir, $[x]$ es la fibra de x en la segunda proyección $R \to X$. En W tenemos una relación de equivalencia R': $R' = W \times_H W \hookrightarrow W \times_S W$, es decir, dos puntos de W están relacionados si tienen la misma imagen en H. H es justamente el cociente de W por esta relación de equivalencia. Las clases de equivalencia de cada punto de X por R', son las mismas que por R. En esta situación, el cociente de X por R existe, y es el subconjunto cerrado de H formado por las clases de equivalencia de R.

Considérese la segunda proyección $p_2: R \to X$. Como X es noetheriano los polinomios de Hilbert de las fibras distintos son un número finito. Luego si H es la unión de los esquemas de Hilbert $\mathrm{Hilb}^{p(n)}_{X/S}$, donde $p(n)$ recorre ese conjunto finito de polinomios, R define un morfismo

$$g: X \to H,\ x \mapsto [x] = R_x$$

de modo que si $W \hookrightarrow X \times_S H$ es el "cerrado universal" entonces $R = X \times_H W$. La gráfica de g, $X \hookrightarrow X \times_S H$, $x \mapsto (x,[x])$, factoriza a través de W. Por tanto, $X \hookrightarrow W$, $x \mapsto (x,[x])$, es un subesquema cerrado.

$W \to H$ es un morfismo fielmente plano y tenemos un subesquema cerrado $X \hookrightarrow W$, de modo que $X \times_H W \simeq W \times_H X$, $(x,(x',h)) \mapsto ((x,h),x')$ [1] (que consideradas las inclusiones obvias $X \times_H W \subseteq W \times_H W$ y $W \times_H X \subseteq W \times_H W$ es la restricción del morfismo $\mathrm{Id}\colon W \times_H W = W \times_H W$). Por la teoría de descenso fielmente plano 18.4.4, X desciende a un subesquema cerrado Z de H, de modo que $X = Z \times_H W$, por lo que $X \to Z$ es un morfismo propio y plano. Z es el esquema cociente buscado: $X \times_Z X = (Z \times_H W) \times_Z X = X \times_H W = R$ y como el funtor de puntos de un esquema es un haz para la topología fielmente plana (por 18.3.3), Z es el conúcleo de las dos proyecciones de $R = X \times_Z X$ sobre X. □

19.7. Esquema de Picard

Hablemos sin rigor. Sea $X \to S$ un morfismo proyectivo plano. Nos proponemos dotar de estructura de esquema al grupo de Picard, $\mathrm{Pic}X$, de las clases de isomorfía de haces de línea en X, o equivalentemente, al grupo de los divisores de Cartier módulo la equivalencia lineal. Demostraremos que existe el esquema $\mathrm{Div}X$ que representa a los de divisores de Cartier efectivos de X, probando que es un abierto del esquema de Hilbert de los cerrados de X.

Consideremos la aplicación natural

$$\mathrm{Div}X \to \mathrm{Pic}X,\ D \mapsto \mathscr{L}_D$$

conocida como contracción de Abel. Podemos pensar $\mathrm{Pic}X$ como el cociente de $\mathrm{Div}X$, por la relación de equivalencia $R \subset \mathrm{Div}X \times \mathrm{Div}X$, cuyas clases de equivalencia son las fibras del morfismo de Abel. La fibra de la contracción de Abel sobre un haz de línea $\mathscr{L}_D$ es el conjunto de los divisores efectivos linealmente equivalentes a D. Es decir, la fibra de $\mathscr{L}_D$ es $\mathbb{P}(\Gamma(X,\mathscr{L}_D))$. Así pues, los divisores equivalentes a D se identifican con $\mathbb{P}(\Gamma(X,\mathscr{L}_D))$. Relativizando este resultado, si consideramos haz de línea $\mathscr{P}$ universal en $X \times_k \mathrm{Div}X$, demostraremos que $R = \mathbb{P}(\Gamma(X,\mathscr{P}))$, que es un fibrado proyectivo sobre $\mathrm{Div}X$. Por la sección anterior, tendremos que el esquema cociente de $\mathrm{Div}X$ por la equivalencia lineal, existe y coincide con $\mathrm{Pic}X$.

19.7.1. Esquema de divisores

1. Lema: *Sea $\pi\colon X \to H$ un morfismo de esquemas. Sea $\mathscr{M}$ un haz coherente en X, plano sobre H (i.e., para todo $x \in X$, $\mathscr{M}_x$ es un $\mathscr{O}_{H,\pi(x)}$-módulo plano). Se cumple que $\mathscr{M}$ es un $\mathscr{O}_X$-plano $\iff$ $\mathscr{M}_{|\pi^{-1}(h)}$ es un $\mathscr{O}_{\pi^{-1}(h)}$-módulo plano para todo punto $h = \mathrm{Spec}\mathscr{O}_{H,h}/\mathfrak{p}_h \in H$.*

[1] Aquí estamos usando que si $h = [x] = \{y \text{ de } X\colon xRy\}$ y x' es un punto de $[x]$ entonces $[x] = [x']$, es decir, que R es una relación de equivalencia.

Demostración. Sea $x \in X$ un punto cerrado y $\phi\colon L \to \mathscr{M}_x$ un epimorfismo de $\mathscr{O}_{X,x}$-módulo libre L en $\mathscr{M}_x$, de modo que $\bar{\pi}\colon L/\mathfrak{m}_x L \simeq \mathscr{M}/\mathfrak{m}_x\mathscr{M}$. Consideremos la sucesión exacta

$$0 \to \operatorname{Ker}\phi \to L \to \mathscr{M}_x \to 0$$

Como $\mathscr{M}_x$ es un $\mathscr{O}_{H,\pi(x)}$-módulo plano, tensando por $\otimes_{\mathscr{O}_{H,\pi(x)}}\mathscr{O}_{H,\pi(x)}/\mathfrak{p}_{\pi(x)}$, obtenemos la sucesión exacta

$$0 \to \operatorname{Ker}\phi/\mathfrak{p}_{\pi(x)}\operatorname{Ker}\pi \to L/\mathfrak{p}_{\pi(x)}L \to \mathscr{M}/\mathfrak{p}_{\pi(x)}\mathscr{M} \to 0$$

Ahora ya,

$$\begin{aligned} \mathscr{M}_x/\mathfrak{p}_{\pi(x)}\mathscr{M}_x \text{ es } \mathscr{O}_{X,x}\big/\mathfrak{p}_{\pi(x)}\mathscr{O}_{X,x}\text{-plano} &\overset{\text{Nak}}{\iff} \operatorname{Ker}\phi/\mathfrak{m}_x\operatorname{Ker}\phi = 0 \\ &\overset{\text{Nak}}{\iff} \operatorname{Ker}\phi = 0 \iff \mathscr{M}_x \text{ es } \mathscr{O}_{X,x} \text{ plano} \end{aligned}$$

□

2. Teorema: *Sea $\pi\colon X \to S$ un morfismo proyectivo plano. El funtor*

$$\underline{\operatorname{Div}}_{X/S}(T) := \{\textit{Divisores de Cartier efectivos de } X_T\textit{, planos sobre } T\}$$

es representable por un abierto del Hilbert de cerrados de X.

Demostración. Sea $H = \operatorname{Hilb}_{X/S}$ y $F = \underline{\operatorname{Div}}_{X/S}$. Tenemos que probar que F es un subfuntor abierto de H.

Un cerrado D de X_T plano sobre T, es un divisor efectivo de Cartier si y sólo si el ideal $\mathfrak{p}_D \subset \mathscr{O}_{X_T}$ de funciones que se anulan en D es un $\mathscr{O}_{X_T}$-módulo plano, o equivalentemente por el lema anterior, si y sólo si $\mathfrak{p}_{D_t} \subset \mathscr{O}_{X_t}$ es un $\mathscr{O}_{X_t}$-módulo plano, para todo $t \in T$.

Dado un morfismo $T \to H$, tenemos que ver que $F \times_H T$ es un abierto de T. Es decir, dado subesquema cerrado D de X_T plano sobre T, tenemos que ver que un morfismo $Z \to T$, cumple que D_Z es un divisor efectivo de Cartier de X_Z si y sólo si factoriza a través de un abierto U de T. Pues bien, si V es el abierto de puntos donde $\mathfrak{p}_{D_T}$ es un $\mathscr{O}_{X_T}$-módulo plano y $C = X_T - V$, entonces $U = T - \pi_T(C)$, por el párrafo anterior.

□

Denotaremos por $\operatorname{Div}_{X/S}$ al representante del funtor $\underline{\operatorname{Div}}_{X/S}$. Igualmente al representante del funtor de los divisores de Cartier de X de polinomio de Hilbert $p(n)$ lo denotaremos $\operatorname{Div}^{p(n)}_{X/S}$.

19.7.2. Efectividad de la equivalencia lineal

Queremos probar que el conjunto $\mathrm{Pic}X$ de haces de línea de un esquema X, módulo isomorfismos, es un esquema. Sobre $X \times \mathrm{Pic}X$ tendremos definido el haz de línea universal $\mathscr{P}$, de modo que $\mathscr{P}_{|X\times p}$ es justamente el haz de línea definido en X por $p \in \mathrm{Pic}X$. Así pues, dado un morfismo $f : Y \to \mathrm{Pic}X$, tenemos que $f^*\mathscr{P}$ es un haz de línea en X_Y, de modo que $(f^*\mathscr{P})_{|X\times y}$ es el haz de línea definido por $f(y)$. Podemos, pues, aventurar que $\mathrm{Pic}X$ representa al funtor $PicX(Y) :=$ {Haces de línea de X_Y, módulo isomorfismos}. Sólo surge una pequeña dificultad. Si $PicX$ fuese representable, sería un haz para la topología de Zariski, es más, para la topología fielmente plana. Así, si $\pi : X_Y \to Y$ es la proyección natural, $\mathscr{L}$ es un haz de línea sobre X_Y y $\mathscr{N}$ es un haz de línea sobre Y, tendremos que identificar $\mathscr{L}$ con $\mathscr{L} \otimes \pi^*\mathscr{N}$, porque localmente sobre Y son isomorfos. Esto nos empujará a considerar, en vez de $PicX$, su hacificado $\underline{\mathrm{Pic}}X$ y probaremos que este último es representable.

Una k-variedad algebraica X se dice que es geométricamente íntegra si para todo cambio de cuerpo base $k \hookrightarrow K$, X_K lo es.

3. Proposición: *Sea $\pi : X \to S$ un morfismo proyectivo plano, cuyas fibras sean variedades algebraicas geométricamente íntegras. Se cumple que $\pi_*\mathscr{O}_X = \mathscr{O}_S$.*

Demostración. El problema es local en S, luego podemos suponer que $S = \mathrm{Spec}A$ es afín. Para cada punto cerrado $s = \mathrm{Spec}A/\mathfrak{m}_s \in S$, denotemos $X_s = \pi^{-1}(s)$. Sabemos que $H^0(X_s, \mathscr{O}_{X_s})$ es un $A/\mathfrak{m}_s$-álgebra finita. Por hipótesis, por cambio de cuerpo base $H^0(X_s, \mathscr{O}_{X_s})$ es íntegra, por tanto, $H^0(X_s, \mathscr{O}_{X_s}) = A/\mathfrak{m}_s$. Por el teorema de Grauert 13.11.9, $\pi_*\mathscr{O}_X$ es un $\mathscr{O}_S$-módulo localmente libre de rango 1, luego el morfismo $\mathscr{O}_S \to \pi_*\mathscr{O}_X$ es isomorfismo.

□

4. Proposición: *Sea $\pi : X \to S$ un morfismo proyectivo plano, cuyas fibras sean variedades algebraicas geométricamente íntegras. Sea $f : S' \to S$ un morfismo fielmente plano y $f' : X' = X \times_S S' \to X$ el morfismo natural. Si $\mathscr{L}$ es un haz de línea en X, tal que $f'^*\mathscr{L} \simeq \mathscr{O}_{X'}$ entonces $\mathscr{L} \simeq \pi^*\mathscr{N}$, donde $\mathscr{N}$ es un haz de línea de S.*

Demostración. Empecemos probando que $\mathscr{L}$ es trivial localmente sobre S. Para probar esto, podemos suponer que $S = \mathrm{Spec}A$, $S' = \mathrm{Spec}A'$ con A y A' anillos locales. Por el teorema de cambio de base fielmente plano 13.4.6, tenemos que

$$\Gamma(X, \mathscr{O}_X) \otimes_A A' = \Gamma(X', \mathscr{O}_{X'}) = \Gamma(X', f'^*\mathscr{L}) = \Gamma(X, \mathscr{L}) \otimes_A A'$$

Como $A \to A'$ es un morfismo fielmente plano, $\Gamma(X, \mathscr{L})$ es un $\Gamma(X, \mathscr{O}_X)$-módulo libre de rango 1. Dado un generador $e \in \Gamma(X, \mathscr{L})$, tendremos que $e \otimes 1$ es un generador de

$\Gamma(X', f'^*\mathscr{L})$. Por tanto, el morfismo inducido $e \otimes 1 \colon \mathscr{O}_{X'} \to f'^*\mathscr{L}$, es isomorfismo, luego el morfismo $e \colon \mathscr{O}_X \to \mathscr{L}$ es isomorfismo.

Así pues, podemos construir un recubrimiento $\{U_i\}$ de S e isomorfismos $\mathscr{L}_{|\pi^{-1}(U_i)} \simeq \mathscr{O}_{\pi^{-1}(U_i)}$. Tendremos que $\pi_*\mathscr{L}$ es un haz de línea en S, porque $(\pi_*\mathscr{L})_{|U_i} = \pi_*(\mathscr{L}_{|\pi^{-1}U_i}) = \pi_*(\mathscr{O}_{|\pi^{-1}U_i}) = \mathscr{O}_{U_i}$ por la proposición anterior.

Por último, el morfismo natural $\pi^*\pi_*\mathscr{L} \to \mathscr{L}$ es un isomorfismo, como se comprueba localmente en los U_i.

□

En esta sección supondremos que $\pi \colon X \to S$ es un morfismo proyectivo plano de fibras geométricamente íntegras.

5. Definición: Definamos el funtor sobre la categoría de los S-esquemas

$$Pic_{X/S}(T) = \{\text{Haces de línea sobre } X_T\}/\sim$$

donde decimos que $\mathscr{L} \sim \mathscr{L}'$ si existe un haz de línea $\mathscr{N}$ en T tal que $\mathscr{L} \simeq \mathscr{L}' \otimes_{\mathscr{O}_T} \pi'^*\mathscr{N}$, siendo $\pi' \colon X_T \to T$ la proyección natural.

Denotemos $\underline{\mathrm{Pic}}_{X/S}$ el hacificado de $Pic_{X/S}$ en la topología fielmente plana.

6. Teorema: *Sea $\pi \colon X \to S$ un morfismo proyectivo plano, cuyas fibras sean variedades algebraicas geométricamente íntegras.*

1. *El morfismo natural $Pic_{X/S} \to \underline{\mathrm{Pic}}_{X/S}$ es inyectivo.*
2. *Si π tiene una sección s, el morfismo $Pic_{X/S} \to \underline{\mathrm{Pic}}_{X/S}$ es isomorfismo.*

Demostración. 1. Tenemos que ver que si $\mathscr{L}$ es un haz de línea en X_T tal que localmente en la topología plana es equivalente a $\mathscr{O}_{X_T}$ entonces $\mathscr{L}$ es equivalente a $\mathscr{O}_{X_T}$. Ahora bien, sea $f \colon T' \to T$ un morfismo fielmente plano y $\pi' \colon X_{T'} \to T'$, $f' \colon X_{T'} \to X$ los morfismos inducidos, si $f'^*\mathscr{L} \sim \pi'^*\mathscr{O}_{T'}$, sustituyendo T' por un recubrimiento suyo por la topología de Zariski, podemos suponer que $f'^*\mathscr{L} \simeq \pi'^*\mathscr{O}_{T'}$; entonces $\mathscr{L}$ es equivalente a $\mathscr{O}_{X_T}$ por la proposición anterior.

2. Para probar que $Pic_{X/S} \to \underline{\mathrm{Pic}}_{X/S}$ es isomorfismo nos falta ver: si $T' \to T$ es un S-morfismo fielmente plano, $f' \colon X_{T'} \to X_T$ el morfismo natural y $\mathscr{L}'$ es un haz de línea en $X_{T'}$ tal que $f'^*_1\mathscr{L}' \sim f'^*_2\mathscr{L}'$, siendo $f'_1, f'_2 \colon X_{T' \times_T T'} \to X_{T'}$ las dos proyecciones naturales, entonces existe un haz $\mathscr{L}$ en X_T de modo que $f'^*\mathscr{L} \sim \mathscr{L}'$. Veámoslo.

Cambiando de base $T \to S$, podemos suponer que $T = S$.

Dado un haz de línea $\mathscr{L}$ en X, la restricción, s^*, del haz de línea $\mathscr{L} \otimes_{\mathscr{O}_X} \pi^*s^*\mathscr{L}^{-1}$ a S, es $\mathscr{O}_S$. Como $\mathscr{L} \sim \mathscr{L} \otimes_{\mathscr{O}_X} \pi^*s^*\mathscr{L}^{-1}$ podremos suponer que la restricción de $\mathscr{L}$ a S es $\mathscr{O}_S$. Si $\mathscr{L}_1, \mathscr{L}_2$ son dos haces de línea en X equivalentes, cuyas restricciones a S

son $\mathscr{O}_S$, entonces $\mathscr{L}_1 \simeq \mathscr{L}_2$, pues $\mathscr{L}_1 \simeq \mathscr{L}_2 \otimes \pi^* \mathscr{N}$ y restringiéndonos a S tenemos que $\mathscr{N} = \mathscr{O}_S$.

En conclusión, podemos suponer que la restricción de $\mathscr{L}'$ a T' es $\mathscr{O}_{T'}$ y que ${f'}_1^* \mathscr{L}' \simeq {f'}_2^* \mathscr{L}'$. Podemos suponer que la restricción de este isomorfismo, llamémoslo θ, a $T' \times_T T'$ es la identidad. Por teoría de descenso fielmente plano, basta probar que θ, verifica la condición de cociclo $\theta_2^{-1} \circ \theta_1 \circ \theta_3 = \mathrm{Id}$, donde si ${f'}_i \colon X_{T' \times_T T' \times_T T'} \to X_{T' \times_T T'}$ es olvidar la componente i de $T' \times_T T' \times_T T'$, entonces $\theta_i = {f'}_i^* \theta$. Observemos que $\theta_2^{-1} \circ \theta_1 \circ \theta_3 \in \Gamma(X_{T' \times_T T' \times_T T'}, \mathscr{O}^*_{X_{T' \times_T T' \times_T T'}}) = \Gamma(T' \times_T T' \times_T T', \mathscr{O}^*_{T' \times_T T' \times_T T'})$. Luego $\theta_2^{-1} \circ \theta_1 \circ \theta_3 = \mathrm{Id}$ si y sólo si lo es su restricción a $T' \times_T T' \times_T T'$, y así sucede.

□

7. Lema: *El subfuntor de $U_r \subseteq Pic_{X/S}$ definido por*

$$U_r(T) = \{\mathscr{L} \in Pic_{X/S}(T) \colon h^0(X_t, \mathscr{L}^{-1}(r)) > 0 \text{ y } h^i(X_t, \mathscr{L}^{-1}(r)) = 0 \text{ para } i > 0, \text{ para todo } t \in T\}$$
$$= \{\mathscr{L} \in Pic_{X/S}(T) \colon \pi_{T*} \mathscr{L}^{-1}(r) \text{ es loc. libre de rango } > 0 \text{ y } R^i \pi_{T*} \mathscr{L}^{-1}(r) = 0 \text{ para } i > 0\}$$

es un subfuntor abierto de $Pic_{X/S}$.

Demostración. Dado un morfismo $T \to Pic_{X/S}$, tenemos que probar que $U_r \times_{Pic_{X/S}} T$ es un abierto de T. Es decir, dado un haz de línea $\mathscr{L}$ de X_T, tenemos que probar que un morfismo $Z \to T$, cumple que $h^0(X_z, \mathscr{L}^{-1}(r)) \geq 0$ y $h^i(X_z, \mathscr{L}^{-1}(r)) = 0$ para $i \geq 0$, para todo $z \in Z$, si y sólo si factoriza a través de un abierto U de T. Efectivamente, denotemos $\mathscr{M} = \mathscr{L}^{-1}(r)$, basta probar que el conjunto U de puntos t de T, tales que $h^0(X_t, \mathscr{M}) > 0$ y $h^i(X_t, \mathscr{M}) = 0$ para $i > 0$, es un abierto. La condición, $h^i(X_t, \mathscr{M}) = 0$ para $i > 0$, equivale a que $R^i \pi_{T*} \mathscr{M} \otimes k(t) = 0$, por 13.11.11. Si se cumple esta condición entonces $\pi_{T*} \mathscr{M} \otimes k(t) = H^0(X_t, \mathscr{M})$ y $\pi_{T*} \mathscr{M}$ es localmente libre en T, por 13.11.10 y 13.11.9 b. Luego U es el conjunto de puntos donde $R^i \pi_{T*} \mathscr{M} = 0$ para $i > 0$, y $\pi_{T*} \mathscr{M}$ tiene rango mayor que cero. Luego U es un abierto.

□

Siempre que diga "la representabilidad de un funtor" me referiré a "la representabilidad del haz asociado al funtor".

Dado un haz de línea $\mathscr{L}$ en X_T sabemos por 13.6.9 que existe un r tal que $\mathscr{L} \in U_r(T)$. Por tanto, $\{U_r\}_{r \in \mathbb{N}}$ es un recubrimiento de $Pic_{X/S}$. Para probar que $Pic_{X/S}$ es un funtor representable basta ver que los U_r son representables.

Dado un haz de línea $\mathscr{L}$ en X y $s \in S$, se dice que

$$p(n) = \chi(X_s, \mathscr{L}(n))$$

es el polinomio de Hilbert de $\mathscr{L}$. Este polinomio no depende del punto $s \in S$, por 13.10.5, y es estable por cambios de la base S. Si definimos

$$Pic^{q(n)}_{X/S}(Y) := \coprod_{T\to Y} \{\text{Haces de línea sobre } X_T \text{ de polinomio de Hilbert } q(n)\}/\sim$$

tenemos que $Pic_{X/S} = \coprod Pic^{q(n)}_{X/S}$.

Consideremos el isomorfismo $Pic^{q(n)}_{X/S} \simeq Pic^{q(n+m)}_{X/S}$, $\mathscr{L} \mapsto \mathscr{L}(m)$. Para la representabilidad de $Pic^{q(n)}_{X/S}$, podremos considerar $Pic^{q(n+m)}_{X/S}$, en vez de $Pic^{q(n)}_{X/S}$, cuando nos convenga.

Con todo, basta probar la representabilidad de $U_r \cap Pic^{q(n)}_{X/S}$. Basta probar la representabilidad de $U_0 \cap Pic^{q(n-r)}_{X/S}$. Dado $\mathscr{L} \in U_0 \cap Pic^{q(n-r)}_{X/S}(T)$, tendremos que $\mathscr{L}$ es un haz de línea en X_T y localmente en T existe un morfismo $\mathscr{O}_{X_T} \to \mathscr{L}^{-1}$ inyectivo en fibras sobre T. Luego, $\mathscr{L}$ se inyecta en $\mathscr{O}_{X_T}$, es un ideal de $\mathscr{O}_{X_T}$, localmente sobre T. Por 19.2.11, existe un m que depende del polinomio $q(n-r)$, de modo que $\pi_{T*}(\mathscr{L}(m))$ es un $\mathscr{O}_T$-haz localmente libre de rango $q(m-r)$. Por tanto, si $\mathscr{L} \in U_m \cap Pic^{q(n+m-r)}_{X/S}(T)$, tendremos que $\pi_{T*}(\mathscr{L})$ es un $\mathscr{O}_T$-haz localmente libre de rango $p(m) = q(m-r)$. Además, dado un morfismo $f\colon T' \to T$ y el morfismo inducido $f'\colon X_{T'} \to X_T$, entonces $\pi_{T*}(\mathscr{L}) \otimes_{\mathscr{O}_T} \mathscr{O}_{T'} \overset{*}{=} \pi_{T'*}(f'^*\mathscr{L})$. Basta demostrar la representabilidad de $U = U_m \cap Pic^{q(n-r+m)}_{X/S}$.

Consideremos el morfismo

$$A\colon \underline{\mathrm{Div}}_{X/S} \to Pic_{X/S},\ D \mapsto \mathscr{L}_D$$

Diremos que dos divisores de Cartier $D, D' \in \mathrm{Div}^{p(n)}_{X/S}(T)$ son linealmente equivalentes sobre T, si los haces de línea $\mathscr{L}_D, \mathscr{L}_{D'}$ asociados son localmente, en la topología fielmente plana, isomorfos sobre T, es decir, $A(D) = A(D')$ en $\underline{\mathrm{Pic}}_{X/S}(T)$. Consideremos la restricción de la relación de equivalencia lineal de divisores de Cartier a $A^{-1}(U)$. Sea pues $R = A^{-1}(U) \times_U A^{-1}(U)$, el haz que define la relación de equivalencia lineal de divisores de Cartier de $A^{-1}(U)$.

El haz cociente de $A^{-1}(U)$ por la relación de equivalencia es el hacificado de U. Para demostrar que la relación de equivalencia lineal es efectiva, basta ver que la relación es representable y que es un fibrado proyectivo sobre $A^{-1}(U)$.

Sea $C \subset X \times \mathrm{Div}_{X/S}$ el divisor universal y $\mathfrak{p} \subset \mathscr{O}_{X\times \mathrm{Div}_{X/S}}$ el haz de ideales de funciones que se anulan en C. Sea $\mathscr{P} = Hom_{\mathscr{O}_{X\times \mathrm{Div}_{X/S}}}(\mathfrak{p}, \mathscr{O}_{X\times \mathrm{Div}_{X/S}})$ el haz de línea universal. Para cada punto $h \in \mathrm{Div}_{X/S}$ entonces $\mathscr{P}_{|X\times h}$ es el haz de línea en X asociado al divisor definido por h. Consideremos $\mathscr{P}_{|X\times A^{-1}(U)}$ y denotemos $\pi_{A^{-1}(U)}\colon X \times A^{-1}(U) \to A^{-1}(U)$, la proyección natural.

8. Proposición : *Sea $\pi\colon X \to S$ un morfismo proyectivo plano, de fibras geométricamente íntegras. Se cumple que $\mathbb{P}(\pi_{A^{-1}(U)*}\mathscr{P}_{|X\times_S A^{-1}(U)})$, representa la relación de equivalencia lineal de divisores de Cartier en $A^{-1}(U)$.*

Demostración. Sea T un $A^{-1}(U)$-esquema. Sea D el divisor de Cartier en X_T definido por el morfismo $T \to A^{-1}(U)$. Por $\overset{*}{=}$, $\mathbb{P}(\pi_{A^{-1}(U)*}\mathscr{P}_{|X\times_S A^{-1}(U)}) \times_{A^{-1}(U)} T$ se identifica con $\mathbb{P}(\pi_{T*}\mathscr{L}_D)$.

Por tanto,

$$\mathrm{Hom}_{A^{-1}(U)}(T, \mathbb{P}(\pi_{A^{-1}(U)*}\mathscr{P}_{|X\times_S A^{-1}(U)})) = \mathrm{Hom}_T(T, \mathbb{P}(\pi_{T*}\mathscr{L}_D))$$

que se identifica con el conjunto de los divisores de Cartier de X_T linealmente equivalentes a D, localmente sobre T.

□

9. Teorema : *Sea $X \to S$ un morfismo proyectivo plano, de fibras geométricamente íntegras.* $\underline{\mathrm{Pic}}_{X/S}$ *es representable, por un esquema que denotaremos* $\mathrm{Pic}_{X/S}$.

El funtor $Pic_{X/S}$ es un funtor de grupos abelianos, con la operación producto tensorial (de haces de línea). El elemento neutro, "el cero", es la clase del haz de línea $\mathscr{O}_X$.

10. Teorema: *Sea $X \to S$ un morfismo proyectivo. Se verifica que*

$$T_{Pic_{X/S},0} = H^1(X, \mathscr{O}_X)$$

Demostración. $T_{Pic_{X/S},0}$ coincide con los haces de línea en $X[\epsilon]$ (módulo subidas de haces de línea de $S[\epsilon]$) tales que su restricción a X sean isomorfos a $\mathscr{O}_X$ (módulo subidas de haces de línea de S). Dado un tal haz de línea $\mathscr{L}$ en $X[\epsilon]$, sea $\{U_i\}$ un recubrimiento de $X[\epsilon]$ (que coincide topológicamente con X) por abiertos afines de modo que existan isomorfismos $f_i : \mathscr{L}_{|U_i} \simeq \mathscr{O}_{U_i}[\epsilon]$. Tenemos que $f_i \circ f_j^{-1} : \mathscr{O}_{U_i\cap U_j}[\epsilon] \simeq \mathscr{O}_{U_i\cap U_j}[\epsilon]$ aplica el 1 en $1 + a_{ij}\epsilon$ y los $a_{ij} \in \mathscr{O}_X(U_i \cap U_j)$, verifican la condición de cociclo obvia. Por tanto, considerando la topología Cech, definen un elemento de $H^1(X, \mathscr{O}_X)$. Recíprocamente, dado un elemento del $H^1(X, \mathscr{O}_X)$, tendremos el cociclo $a_{ij} \in \mathscr{O}_X(U_i \cap U_j)$, que definirán en $X[\epsilon]$ el haz de línea $\mathscr{L}$, cuya restricción a X será isomorfo a $\mathscr{O}_X$. □

11. Ejercicio : Supóngase que X es una variedad íntegra y $S = k$. Úsese que $H^1(X, \mathscr{O}_X^*) = Pic_{X/k}(k)$ y la sucesión exacta

$$0 \longrightarrow \mathscr{O}_X \xrightarrow{exp} \mathscr{O}^*_{X[\epsilon]} \longrightarrow \mathscr{O}^*_X \longrightarrow 0$$

$$0 \longrightarrow f \longrightarrow 1 + f\epsilon$$

para probar el teorema anterior.

19.8. Variedades abelianas

1. Definición: Diremos que un S-esquema X es un S-esquema de grupos si el funtor $X^{\cdot}$ de puntos de X en la categoría de S-esquemas valora en la categoría de grupos.

X es un S-esquema de grupos si y sólo si existen morfismos de S-esquemas

$$X \times_S X \xrightarrow{+} X,\ S \xrightarrow{el.neut.} X,\ X \xrightarrow{inv.} X$$

verificando los diagramas obvios de la definición (por diagramas) de grupo.

2. Ejemplo: $\mathbb{A}^1 = \operatorname{Spec} k[x]$ es un k-esquema de grupos porque $\mathbb{A}^{1^{\cdot}} = G_a$, es decir, $\mathbb{A}^{1^{\cdot}}(T) = \operatorname{Hom}_k(T, \mathbb{A}^1) = \mathscr{O}_T(T)$, que es un grupo abeliano. La operación viene definida por el morfismo $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$, $(\alpha, \beta) \mapsto \alpha + \beta$, etc.

Si E es un k-espacio vectorial de dimensión finita, entonces $\mathbf{E} := \operatorname{Spec} S_k^{\cdot} E^*$ es un k-esquema de grupos conmutativo, pues $\mathbf{E}(T) = E \otimes_k \mathscr{O}_T(T)$.

El funtor $\mathbf{Aut_k E}(T) := \operatorname{Aut}_T(\mathbf{E}_T, \mathbf{E}_T)$ es representable por un abierto afín de $\mathbf{End_k}(\mathbf{E})$, que denotaremos por $\mathbf{Gl}(\mathbf{E})$, que es un k-esquema de grupos no abeliano si $\dim_k E > 1$.

Sea $\pi : X \to S$ un morfismo proyectivo plano, de fibras geométricamente íntegras. $\operatorname{Pic}_{X/S}$ es un S-esquemas de grupos conmutativo.

3. Definición: Diremos que una k-variedad algebraica X es una k-variedad abeliana si es propia y geométricamente conexa y reducida (es decir, reducido y conexo al cambiar de base al cierre algebraico de k) y es k-esquema de grupos.

4. Proposición: *Si X es una k-variedad abeliana entonces es una variedad de grupos conmutativos, lisa.*

Demostración. Por ser X propia y geométricamente reducida y conexa $\mathscr{O}_X(X) = k$. Para ver que X es un grupo conmutativo, tenemos que ver que dado un punto racional g de X, el automorfismo de X conjugar por g es el morfismo identidad. Sea e el elemento neutro de X y $I_e \subset \mathscr{O}_{X,e}$ el ideal de gérmenes de funciones que se anulan en e. Para todo m, tenemos un morfismo $\tau : X \to \mathbf{Aut_k}(\mathscr{O}_{\mathbf{X,e}}/\mathbf{I_e^m})$, $g \mapsto \tau_g$, donde τ_g es el automorfismo inducido en $\mathscr{O}_{X,e}/I_e^m$, por la conjugación por g. Ahora bien, $\mathbf{Aut_k}(\mathscr{O}_{\mathbf{X,e}}/\mathbf{I_e^m})$ es una variedad afín, luego

$$\begin{aligned}\operatorname{Hom}_{k-esq}(X, \mathbf{Aut_k}(\mathscr{O}_{\mathbf{X,e}}/\mathbf{I_e^m})) &= \operatorname{Hom}_{k-esq}(\operatorname{Spec}\mathscr{O}_X(X), \mathbf{Aut_k}(\mathscr{O}_{\mathbf{X,e}}/\mathbf{I_e^m})) \\ &= \operatorname{Hom}_{k-esq}(\operatorname{Spec} k, \mathbf{Aut_k}(\mathscr{O}_{\mathbf{X,e}}/\mathbf{I_e^m}))\end{aligned}$$

Por tanto, $\tau(g) = \tau(e) = \mathrm{Id}$ para todo g. Luego, el endomorfismo inducido en el completado de $\mathscr{O}_{X,e}$ por la conjugación por g, es la identidad. En conclusión, la conjugación por g induce la identidad en $\mathscr{O}_{X,e}$, luego en un entorno de e es la identidad, y por ser X separado e irreducible es la identidad en X.

Veamos la lisitud. Por cambio de base al cierre algebraico podemos suponer que el cuerpo base es algebraicamente cerrado. Por las condiciones impuestas X es una variedad íntegra. El conjunto de puntos donde es lisa es un abierto no vacío. Abierto que es estable por traslaciones, luego ha de ser todo X.

□

5. Teorema: *Sea X una variedad abeliana. Si T es un isomorfismo de esquemas de X que deja fijo el elemento neutro de X, entonces T es un automorfismo de grupos de X. Es decir, salvo traslaciones todo isomorfismo de X es un automorfismo de grupos.*

Demostración. Tenemos que probar que $T(x+y)-T(x)-T(y)=0$ para todo par de puntos x,y de X. Consideremos el morfismo de esquemas $T_y\colon X\to X$, $T_y(x):=T(x+y)-T(x)-T(y)$. Tenemos que probar que $T_y=0$ para todo y. Para cada m, sea $\tau\colon X\to \mathbf{End_k}(\mathscr{O}_{\mathbf{X},\mathbf{e}}/\mathbf{I_e^m})$, donde $\tau(y)$ es el morfismo inducido por T_y en $\mathscr{O}_{X,e}/I_e^m$. Basta probar que $\tau(y)=0$ para todo y. Ahora bien, $\mathbf{End_k}(\mathscr{O}_{\mathbf{X},\mathbf{e}}/\mathbf{I_e^m})$ es una variedad afín, luego

$$\begin{aligned}\mathrm{Hom}_{k-esq}(X,\mathbf{End_k}(\mathscr{O}_{\mathbf{X},\mathbf{e}}/\mathbf{I_e^m})) &= \mathrm{Hom}_{k-esq}(\mathrm{Spec}\,\mathscr{O}_X(X),\mathbf{End_k}(\mathscr{O}_{\mathbf{X},\mathbf{e}}/\mathbf{I_e^m}))\\ &= \mathrm{Hom}_{k-esq}(\mathrm{Spec}\,k,\mathbf{End_k}(\mathscr{O}_{\mathbf{X},\mathbf{e}}/\mathbf{I_e^m}))\end{aligned}$$

Por tanto, $\tau(y)=\tau(0)=0$ para todo y.

□

19.9. Esquema simétrico

Sea $\pi\colon X\to S$ un morfismo cuasiproyectivo de esquemas. Se define el esquema simétrico relativo a S como el cociente del producto directo $X\times_S \overset{n}{\ldots}\times_S X$ por la acción natural del grupo simétrico S_n operando por permutación de los factores, esquema que denotaremos por $S^n_S X$, o simplemente por S^nX. Si $\{U_i=\mathrm{Spec}A_i\}$ es un recubrimiento de X por abiertos afines, de modo que $\pi(U_i)\subset V_i=\mathrm{Spec}B_i$ y $\{U_i\times_S \overset{n}{\ldots}\times_S U_i\}$ sea un recubrimiento de $X\times_S \overset{n}{\ldots}\times_S X=:X^n$ entonces

$$\{(U_i\times_S \overset{n}{\ldots}\times_S U_i)/S_n=\mathrm{Spec}(A_i\otimes_{B_i}\overset{n}{\ldots}\otimes_{B_i}A_i)^{S_n}\}$$

es un recubrimiento por abiertos afines de S^nX (téngase en cuenta 3.3.38).

Obviamente el morfismo $X^n\to S^nX$ es finito.

Por 2.5.4, los invariantes por la acción de un grupo finito cambian de base por cambios de base plano. En característica cero, los invariantes por la acción de un grupo finito cambian de base, porque el morfismo $M^G\hookrightarrow M$ tiene como sección $\frac{1}{\#G}\sum_{g\in G} g$. Además, si M es un A-módulo plano entonces M^G es un A-módulo plano y la toma de invariantes es exacta.

1. Proposición: *Sea $X \to S$ un esquema y $G \subset \mathrm{Aut}_S X$ un grupo finito que opera sobre un recubrimiento por abiertos afines de X. Supongamos que X es un $\mathbb{Q}$-esquema. Si $X \to S$ es de Cohen-Macaulay entonces $X/G \to S$ es de Cohen-Macaulay.*

Demostración. La proposición es local en X, luego podemos suponer que $X = \mathrm{Spec} B$, $S = \mathrm{Spec} A$ y $G \subseteq \mathrm{Aut}_A B$. Podemos suponer que A es un cuerpo y B es de Cohen-Macaulay. Tenemos que probar que B^G es de Cohen-Macaulay. Podemos suponer que $\dim B^G > 0$. Consideremos un punto $y \in X/G$ no aislado y sea $x \in X$ no aislado que se proyecte en y. Sea $f \in \mathfrak{p}_x$ que no sea divisor de cero en B. Entonces $N(f) = \prod_{g \in G} g(f)$ es no divisor de cero en B y $N(f) \in \mathfrak{p}_y$. Como $B^G/N(f) = (B/N(f))^G$ y $B/N(f)$ es de Cohen-Macaulay, por inducción sobre la dimensión de Krull $B^G/N(f)$ es de Cohen-Macaulay y B^G es de Cohen-Macaulay. □

2. Teorema: *Si $X \to S$ es plano, entonces*

1. *El morfismo $S^n X \to S$ es un morfismo plano.*
2. *El producto simétrico cambia de base, es decir, $S^n_S X \times_S S' = S^n_{S'}(X \times_S S')$*

Demostración. En efecto, basta ver que si M es un A-módulo plano entonces $S^n_A M := (M \otimes_A \overset{n}{\ldots} \otimes_A M)^{S_n}$ es un A-módulo plano y que $S^n_A M \otimes_A B = S^n_B(M \otimes_A B)$. Si M fuese un A-módulo libre finito generado entonces sería obvio. Como por el Teorema de Lazard 0.11.22, M es límite inductivo de módulos libres finito generados y la toma de invariantes conmuta con límites inductivos, concluimos. □

3. Teorema: *Si $C \to S$ es un morfismo cuasiproyectivo plano de fibras curvas lisas, entonces $S^n C \to S$ es liso. Además, el morfismo $C^n \to S^n C$ es plano.*

Demostración. Dado que $S^n C$ es plano sobre S y cambia de base, basta demostrar la proposición cuando $S = \mathrm{Spec} k$ es el espectro de un cuerpo, que podremos suponer algebraicamente cerrado.

Sea $(x_1, \ldots, x_n) \in C \times_k \ldots \times_k C$ un punto cerrado y denotemos por $x_1 + \ldots + x_n$ la clase de $(x_1, \ldots, x_n)$ en $S^n C$. Sea $U = \mathrm{Spec} A$ un abierto afín que contenga a todos los x_i. Denotemos por $B = (A \otimes_k \overset{n}{\ldots} \otimes_k A)^{S_n}$ y $B' = A \otimes_k \overset{n}{\ldots} \otimes_k A$.

La compleción de B' en $x = (x_1, \ldots, x_n)$ es isomorfo a $k[[t_1, \ldots, t_n]]$.

Para demostrar la proposición basta probar que la compleción, $\widehat{B}$, de B en el punto $x_1 + \ldots + x_n$ es un anillo de series formales. Se verifica que $(B' \otimes_B \widehat{B})^{S_n} = \widehat{B}$ y

$$B' \otimes_B \widehat{B} = \varprojlim_n \prod_{\bar{\sigma} \in S_n/I_x} (A \otimes_k \ldots \otimes_k A)/\mathfrak{m}^n_{(x_{\sigma(1)}, \ldots, x_{\sigma(n)})} = \prod_{\bar{\sigma} \in S_n/I_x} k[[t_1, \ldots, t_n]]$$

donde I_x es el subgrupo de isotropía de x. Dado $(p_{\bar{\sigma}}(t_1,\dots,t_n)) \in B' \otimes_B \widehat{B}$ y $\tau \in S_n$, entonces $\tau((p_{\bar{\sigma}}(t_1,\dots,t_n)) = (p_{\overline{\tau\sigma}}(t_{\tau(1)},\dots,t_{\tau(n)})$. En conclusión, hemos reducido la proposición al caso en el que $C = \mathbb{A}^1_k$. En tal caso, $S^n_k\mathbb{A}^1 \simeq \mathbb{A}^n_k$ por el teorema fundamental de las funciones simétricas.

El morfismo $C^n \to S^n C$ es plano, porque por 7.6.17 todo morfismo finito entre variedades lisas es plano. □

19.9.1. Dualizante de los esquemas simétricos

En esta sección supondremos que $X \to S$ es un morfismo proyectivo liso, de modo que las fibras son curvas lisas o bien S es un $\mathbb{Q}$-esquema.

Consideremos el morfismo $\pi\colon X^n \to S^n X$. Por ser π finito, dado un módulo cuasicoherente $\mathscr{M}$ en X^n, escribiremos $\pi_*\mathscr{M} = \mathscr{M}$.

Se cumple que el morfismo $\mathscr{O}_{S^nX} \hookrightarrow \mathscr{O}_{X^n}$ tiene localmente sección, es decir, el morfismo natural $\mathscr{O}^*_{X^n} = \underline{\mathrm{Hom}}_{\mathscr{O}_{S^nX}}(\mathscr{O}_{X^n},\mathscr{O}_{S^nX}) \to \mathscr{O}^*_{S^nX} = \mathscr{O}_{S^nX}$, $w \mapsto w(1)$, es epiyectivo. En efecto, en característica cero, la sección es $\frac{1}{\#G}\sum_{g\in G} g$; si X es una curva lisa sobre S, el morfismo $\mathscr{O}_{S^nX} \hookrightarrow \mathscr{O}_{X^n}$ es fielmente plano, luego por cambio de base fielmente plano tiene sección, luego el morfismo $\mathscr{O}^*_{X^n} = \underline{\mathrm{Hom}}_{\mathscr{O}_{S^nX}}(\mathscr{O}_{X^n},\mathscr{O}_{S^nX}) \to \mathscr{O}^*_{S^nX} = \mathscr{O}_{S^nX}$, $w \mapsto w(1)$, es epiyectivo por cambio de base fielmente plano, luego antes también.

Si G es un grupo finito y M es un módulo en el que opera G, denotaremos $\mathrm{Tr}_M\colon M \to M$, el morfismo definido por $\mathrm{Tr}_M(m) = \sum_{g\in G} g(m)$.

4. Proposición: *Sea $\mathscr{M}$ un $\mathscr{O}_{S^nX}$-módulo coherente libre de torsión en fibras sobre S y plano sobre S. Sea $\bar{\mathscr{M}} = \underline{\mathrm{Hom}}_{\mathscr{O}_{S^nX}}(\mathscr{O}_{X^n},\mathscr{M})$, el morfismo*

$$\phi\colon \mathscr{M} \to \bar{\mathscr{M}},\ \phi(m)(b) := \mathrm{Tr}(b)\cdot m$$

establece un isomorfismo $\mathscr{M} \simeq \mathrm{Tr}(\bar{\mathscr{M}})$.

Demostración. La proposición es local en S^nX. Veamos que ϕ es inyectivo: Sea L un módulo $\mathscr{O}_{S^nX}$-módulo libre que se epiyecte en $\mathscr{O}_{X^n}$ y consideremos la composición $\mathscr{M} \to \bar{\mathscr{M}} \hookrightarrow \mathrm{Hom}_{\mathscr{O}_{S^nX}}(L,\mathscr{M})$. La composición es un morfismo que en fibras sobre S es inyectiva, luego por 7.7.9 es inyectiva. Luego ϕ es inyectiva.

$\mathrm{Tr}(w)(b) = \sum_{g\in G} w(g(b)) = w(\mathrm{Tr}(b)) = \mathrm{Tr}(b)\cdot w(1) = \phi(w(1))(b)$. Por tanto, $\mathrm{Tr}(\bar{\mathscr{M}}) \subseteq \phi(\mathscr{M})$. Por último, dado $w' \in \mathrm{Hom}_{\mathscr{O}_{S^nX}}(\mathscr{O}_{X^n},\mathscr{O}_{S^nX})$, tal que $w'(1) = 1$ y $w \in \bar{\mathscr{M}}$ definida por $w(b) := w'(b)\cdot m$, se tiene que $\mathrm{Tr}(w)(b) = \mathrm{Tr}(b)\cdot m = \phi(m)(b)$, luego $\phi(\mathscr{M}) \subseteq \mathrm{Tr}(\bar{\mathscr{M}})$ y $\phi(\mathscr{M}) = \mathrm{Tr}(\bar{\mathscr{M}})$. □

5. Teorema : *El dualizante de S^nX es canónicamente isomorfo a la imagen por la traza del dualizante de X^n, es decir,*

$$\mathrm{Tr}(w_{X^n}) \simeq w_{S^nX}$$

Demostración. Por dualidad $w_{X^n} = \underline{\mathrm{Hom}}_{\mathscr{O}_{S^nX}}(\mathscr{O}_{X^n}, w_{S^nX})$. Por tanto,

$$\mathrm{Tr}(w_{X^n}) \simeq w_{S^nX}$$

□

6. Corolario:

$$w_{S^nX} \simeq \begin{cases} \Lambda^n_S w_X & \textit{si } \dim_S X \textit{ es impar} \\ S^n_S w_X & \textit{si } \dim_S X \textit{ es par (y } S \textit{ es un } \mathbb{Q}\textit{-esquema)} \end{cases}$$

Demostración. Si d es la dimensión de las fibras del morfismo $X \to S$, el dualizante de X^n es

$$w_{X^n} = \Lambda^{nd}\Omega_{X^n} = \Lambda^{nd}(\Omega_X \oplus \overset{n}{\ldots} \oplus \Omega_X) = \Lambda^d\Omega_X \otimes_{\mathscr{O}_S} \overset{n}{\ldots} \otimes_{\mathscr{O}_S} \Lambda^d\Omega_X = w_X \otimes_{\mathscr{O}_S} \overset{n}{\ldots} \otimes_{\mathscr{O}_S} w_X$$

cada permutación de S_n opera permutando los factores y multiplicando por el signo de la permutación considerada elevado a d. Por el teorema anterior

$$w_{S^nX} \simeq \mathrm{Tr}(w_X \otimes_{\mathscr{O}_S} \overset{n}{\ldots} \otimes_{\mathscr{O}_S} w_X)$$

y se concluye fácilmente. □

Si $\dim_S X = 1$, la característica de $\mathscr{O}_S$ es distinta de 2 y hacemos operar S_n en $w_X \otimes_S \ldots \otimes_S w_X$ permutando lo factores y multiplicando por el signo de la permutación, tenemos que $(w_X \otimes_S \ldots \otimes_S w_X)^{S_n} = w_{S^nX}$.

Sea $f\colon C \to S$ un morfismo proyectivo, liso y cuyas fibras sean curvas geométricamente conexas y de género g. Sea $s \in S$ un punto cerrado. El morfismo $(f_*\mathscr{O}_C) \otimes_{\mathscr{O}_S} k(s) \to H^0(C_s, \mathscr{O}_{C_s}) = k(s)$ es claramente epiyectivo, luego por el teorema de Grauert, 13.11.9, $f_*\mathscr{O}_C$ es un $\mathscr{O}_S$-módulo localmente libre de rango 1, de modo que el morfismo $\mathscr{O}_S \to f_*\mathscr{O}_C$ es un isomorfismo. De nuevo por Grauert, $R^1f_*\mathscr{O}_C$ es localmente libre de rango g.

Por dualidad, $f_*w_C = (R^1f_*\mathscr{O}_C)^*$, luego es localmente libre de rango g. Se cumple que $f_*w_C \otimes_{\mathscr{O}_S} \mathscr{O}_S/\mathfrak{m}_s = H^0(C_s, w_{C_s})$ y de nuevo por Grauert $R^1f_*w_C$ es localmente libre de rango 1.

Por la fórmula de Künneth (Problema 5 del capítulo 13), si denotamos $f'\colon C \times_S \ldots \times_S C \to S$ el morfismo natural, se cumple que

$$f'_*(w_C \otimes_S \ldots \otimes_S w_C) = f_*(w_C) \otimes_S \ldots \otimes_S f_*(w_C)$$

7. Corolario: *Sea $f: C \to S$ un morfismo proyectivo, liso y cuyas fibras sean curvas geométricamente conexas y de género g. Denotemos $\bar{f}: S^nC \to S$ el morfismo natural. Se verifica un isomorfismo canónico*

$$\bar{f}_* w_{S^nC} = \Lambda^n_S f_* w_C$$

y además éstos son haces coherentes sobre S localmente libres de rango $\binom{g}{n}$.

19.9.2. Simétrico de una curva. Morfismo determinante

Sea $C \to S$ una curva lisa proyectiva. Consideremos el subesquema cerrado de $C^n \times_S C^n$, $F_\sigma = \{(x, \sigma(x)) \in C^n \times C^n, x \in C^n\}$, $\sigma \in S_n$ y F la unión de "las diagonales" F_σ. Se verifica que $F = C^n \times_{S^nC} C^n$: Como F_σ es un subesquema cerrado de $C^n \times_{S^nC} C^n$ entonces $F \subseteq C^n \times_{S^nC} C^n$. Sea A el anillo de funciones en un entorno afín U de C^n estable por S_n, $B = A^{S^n}$. Si I_σ es ideal de funciones de $U \times U$, que se anulan en $F_\sigma \cap U \times U$ entonces el anillo de funciones $F \cap U \times U$ es $A' = (A \otimes A)/\bigcap_{\sigma \in S_n} I_\sigma$. La imagen del morfismo $\phi: A \otimes_B A \to \prod_{\sigma \in S_n} A$, $\phi(a \otimes a') := (a \cdot \sigma(a'))_\sigma$ es A'. Basta ver que ϕ es inyectivo. Basta verlo en fibras sobre S, por 7.7.9. Podemos suponer que S es un cuerpo, luego que A es un anillo íntegro. El morfismo ϕ es un morfismo entre A-módulos localmente libres y localizando en el punto genérico de A es un isomorfismo por la teoría de Galois. Por tanto ϕ es inyectivo.

Así pues, S^nC es el cociente de C^n por la relación de equivalencia F. Advirtamos que $F^\cdot \neq \bigcup_{\sigma \in S_n} F^\cdot_\sigma$, aunque coincidan tomando valores sobre esquemas íntegros.

Probemos que el esquema simétrico n de una curva lisa representa los divisores de grado n de la curva.

Consideremos en $C \times_S C^n$ el subesquema cerrado $\mathscr{D} = \{(x, x_1, \ldots, x_n) \colon x = x_i \text{ para algún } i\}$. Dado el morfismo

$$\begin{array}{ccc} C \times_S C^n & \xrightarrow{\mathrm{Id} \times \pi_i} & C \times_S C \\ (x, x_1, \ldots, x_n) & \longmapsto & (x, x_i) \end{array}$$

el ideal Δ de la diagonal de $C \times C$ y $\Delta_i = (\mathrm{Id} \times \pi_i)^* \Delta$, el ideal de funciones que se anulan en $\mathscr{D}$ es $\mathfrak{p}_D = \bigcap_{i=1}^n \Delta_i$. Dado un punto cerrado $x \in X_1 \times X_2$ cuyas proyecciones en cada factor sean x_1, x_2, escribiremos $x = (x_1, x_2)$. Observemos que los Δ_i son ideales localmente principales, ya que Δ lo es. Si $(\Omega_{C/S})_x = \langle dt \rangle$, entonces $\Delta_{(x,x)} = (t \otimes 1 - 1 \otimes t)$. Denotemos $t = t \otimes (1 \overset{n}{\otimes} \ldots \otimes 1)$ y $t_i = 1 \otimes (1 \overset{i}{\otimes} \ldots \otimes t \otimes \ldots \otimes 1)$, entonces $\Delta_i = (t - t_i)$ localmente en el punto $(x, x_1, \overset{i}{\ldots}, x, \ldots, x_n)$. Además, la sucesión $\{t - t_1, \ldots, t - t_i\}$ forman una sucesión regular en el punto $(x, x, \overset{i}{\ldots}, x, x_{i+1}, \ldots, x_n)$, porque generan el ideal de funciones que se anulan

en la subvariedad lisa $C \times {}^{n-i}\pi C = \{(x,x,\ldots,x,x_{i+1},\ldots,x_n)\}$. Como consecuencia tendremos que $\mathfrak{p}_{\mathscr{D}} = \Delta_1 \cdot \ldots \cdot \Delta_n$. Así pues, $\mathscr{D}$ es un divisor de Cartier. Dado un punto cerrado $y = (x,x_1,\ldots,x_n) \in D$ y t una función en un entorno de $\{x_1,\ldots,x_n\}$, que genere $\mathfrak{m}_x\mathscr{O}_{C,x}$ y que no se anule en los $x_i \neq x$, tendremos que $\mathfrak{p}_{\mathscr{D}} = ((t-t_1)\cdot \ldots \cdot (t-t_n))$ en un entorno de y. Además, $\mathscr{D} \to C^n$ es un morfismo finito, porque es propio y de fibras finitas, y es un morfismo plano de grado n, como se comprueba de modo inmediato y explícito. Por otra parte, $(t-t_1)\cdot \ldots \cdot (t-t_n)$ es un polinomio en t con coeficientes funciones invariantes por S^n, por tanto pertenece a $\mathscr{O}_{C\times S^nC,(x,x_1+\ldots+x_n)}$. En conclusión, existe un divisor de Cartier $\tilde{\mathscr{D}} \subset C \times S^nC$, finito, plano y de grado n sobre S^nC, de modo que su imagen inversa por el morfismo $C \times C^n \to C \times S^nC$ es $\mathscr{D}$.

Supongamos que C es una curva lisa sobre un cuerpo algebraicamente cerrado. Dado un punto cerrado $x = x_1 + \ldots + x_n \in S^nC$, veamos cómo podemos reconstruir el divisor $D = x_1 + \ldots + x_n$. Consideremos laa inclusiones obvias $f : x \hookrightarrow S^nC$ y por $\mathrm{Id} \times f : C \times x \hookrightarrow C \times S^nC$. Se cumple que $(\mathrm{Id} \times f)^*(\tilde{\mathscr{D}}) = D$:

$$\mathscr{O}_{(\mathrm{Id}\times f)^*(\tilde{\mathscr{D}})} = \mathscr{O}_{C\times S^nC}/(\mathfrak{p}_{\tilde{\mathscr{D}}}, \mathfrak{m}_{x_1+\ldots+x_n}) = \mathscr{O}_{C\times C^n}/(\mathfrak{p}_{\mathscr{D}}, \mathfrak{m}_{(x_1,\ldots,x_n)})$$

como localmente $\mathfrak{p}_{\mathscr{D}} = ((t-t_1)\cdot \ldots \cdot (t-t_n))$ y $\mathfrak{m}_{(x_1,\ldots,x_n)} = (t_1 - t_1(x_1), \ldots, t_n - t_n(x_n))$, entonces se verifica que $\mathscr{O}_{C\times C^n}/(\mathfrak{p}_{\mathscr{D}}, \mathfrak{m}_{(x_1,\ldots,x_n)}) = \mathscr{O}_C/((t-t(x_1))\cdots,(t-t(x_n))) = \mathscr{O}_D$ y hemos concluido.

Dado un divisor $D = x_1 + \cdots + x_n$ de grado n en C, veamos cómo podemos definir el punto $x_1 + \ldots + x_n$ de S^nC. En los anillos queremos definir la composición

$$\begin{array}{cccc} & & \mathscr{O}_{S^nC} & \hookrightarrow \mathscr{O}_{C^n} \to \quad \mathscr{O}_{C^n}/\mathfrak{m}_{(x_1,\ldots,x_n)} = k \\ (*) & \sum_{\sigma\in S_n} 1\otimes\ldots\otimes \underset{\sigma(1)}{b} \otimes\ldots\otimes \underset{\sigma(i)}{b} \otimes\ldots\otimes 1 & |----> & \sum_{\sigma\in S_n} b(x_{\sigma(1)})\cdot\ldots\cdot b(x_{\sigma(i)}) \end{array}$$

Sea $A \hookrightarrow B$ un morfismo de anillos de modo que B sea un A-módulo finito generado localmente libre. Denotemos por $\otimes^n_A B$ el producto tensorial n-ésimo de B sobre A y por $S^n_A B = (\otimes^n_A B)^{S_n}$. Sea $I = \langle b_1 \otimes \ldots \otimes b \otimes b \ldots \otimes b_n \rangle_{A-mod}$. Recordemos que $\Lambda^n_A B = (\otimes^n_A B)/I$. $S^n_A B$ opera en $\otimes^n_A B$ por multiplicación y deja estable I, por tanto opera en $\Lambda^n_A B$. Si B es un A-módulo localmente libre de rango n, entonces $\Lambda^n_A B$ es localmente isomorfo a A y cada elemento s de $S^n_A B$ que opera en $\Lambda^n_A B$, es una homotecia por un elemento, que denotaremos $\det s$. Tenemos un morfismo[2]

$$\det : S^n_A B \to A$$

[2]De otro modo: Sea $Det : B \to A$ el morfismo que asigna a cada función $b \in B$ el determinante de la homotecia de factor b en B. El morfismo Det es una n-forma simétrica, es decir, $Det \in S^nB^*$. La imagen de Det por el morfismo natural $S^nB^* \to \mathrm{Hom}_k((\otimes^n_A B)^{S_n}, A)$ es el morfismo det que hemos definido.

que llamaremos morfismo determinante. Si denotamos, $s_i(b) = \sum_{\sigma\in S_n} 1\otimes\ldots\otimes \underset{\sigma(1)}{b}\otimes\ldots\otimes \underset{\sigma(i)}{b}\otimes\ldots\otimes 1$, tenemos que

$$\det(s_i(b)) = \begin{cases} \text{Coeficiente del término de grado } n-i \\ \text{del polinomio característico de } B \xrightarrow{b\cdot} B \end{cases}$$

En espectros tenemos $\operatorname{Spec} A \xrightarrow{\det^*} S^n(\operatorname{Spec} B)$. Si $B = \mathscr{O}_D = \mathscr{O}_C/\mathfrak{p}_D$ y $A = k$, es una comprobación inmediata que la composición de los morfismos $\mathscr{O}_{S^nC} \to \mathscr{O}_{S^nD} = S^n_k\mathscr{O}_D \xrightarrow{\det} k$ es el morfismo $(*)$ antes definido.

Denotemos $\underline{\operatorname{Div}}^n_{C/S}$ el funtor definido por

$$\underline{\operatorname{Div}}^n_{C/S}(T) := \{\text{Divisores efectivos de Cartier de } C\times_S T \text{ finitos y planos de grado } n \text{ sobre } T\}$$

que es representable por 19.7.2 por $\operatorname{Div}^n_{C/S}$. Sean los morfismos

$$\begin{array}{rcl} \phi\colon (S^nC)^{\cdot}(T) & \longrightarrow & \underline{\operatorname{Div}}^n_{C/S}(T) \\ T\xrightarrow{f} S^nC & \longmapsto & (\mathrm{Id}\times f)^*\tilde{\mathscr{D}}\subset C\times_S T \end{array}$$

$$\begin{array}{rcl} \varphi\colon \underline{\operatorname{Div}}^n_{C/S}(T) & \longrightarrow & (S^nC)^{\cdot}(T) \\ D\subset C_T & \longmapsto & T\xrightarrow{\det^*} S^n_T D\to S^n_T(C_T)\to S^nC \end{array}$$

8. Teorema: *Los morfismos ϕ y φ son inversos entre sí, es decir,*

$$(S^nC)^{\cdot} = \underline{\operatorname{Div}}^n_S C$$

Demostración. $\varphi\circ\phi$ define un morfismo $I\colon S^nC\to S^nC$ que en fibras sobre la base S es topológicamente el morfismo identidad, luego I es topológicamente el morfismo identidad, en particular es un morfismo finito. Para probar que I es esquemáticamente el morfismo identidad basta probarlo localmente y tras compleciones, en tal caso podemos suponer que C es la recta proyectiva. Además podemos suponer que $S = \operatorname{Spec}\mathbb{Z}$, porque el morfismo I lo obtenemos por cambio de la base $\mathbb{Z}$. Ahora, el único automorfismo de un anillo de polinomios con coeficientes en $\mathbb{Z}$, que en espectros es topológicamente la identidad es el morfismo identidad. Por tanto, $I = \mathrm{Id}$.

El morfismo $\phi\circ\varphi$ define un morfismo $H\colon \operatorname{Div}^n_{C/S}\to\operatorname{Div}^n_{C/S}$, que en fibras sobre S es topológicamente el morfismo identidad. Por tanto, H es un morfismo finito. Ahora bien, como $\varphi\circ\phi = \mathrm{Id}$, entonces $H^2 = H$, que implica ya que $H = \mathrm{Id}$.

□

19.10. Morfismo canónico de la variedad de divisores

Sea $f: C \to S$ un morfismo proyectivo liso de fibras curvas geométricamente conexas de género g y $\bar{f}: S^g C \to C$ el morfismo natural. Sabemos que $\bar{f}_* w_{S^g C} = \Lambda^g_S f_* w_C$, es un haz de línea en S, lo cual afirma que $S^g C$ tiene un único divisor canónico, $K^g \hookrightarrow S^g C$.

El funtor sobre la categoría de los S-esquemas

$$G(Z) = \left\{ \begin{array}{l} \text{Divisores de grado } g,\ D \hookrightarrow C \times_S Z = C_Z, \\ \text{tales que } F_1^{\mathscr{O}_Z}(R^1 f_{Z,*}(w_C \otimes \mathscr{L}_{-D})) = 0 \end{array} \right.$$

donde $f_Z: C_Z \to Z$ es el morfismo natural y $F_1^{\mathscr{O}_Z}$ denota el primer haz de ideales de Fitting, es representable por el subesquema cerrado de $S^g C$, , que denotaremos por G^1_g y llamaremos el subesquema de los divisores especiales de grado g de C, definido por los ceros del ideal $F_1^{\mathscr{O}_{S^g C}}(R^1 f_{S^g C,*}(w_C \otimes \mathscr{L}_{-\tilde{\mathscr{D}}}))$. Si S es un cuerpo algebraicamente cerrado, los puntos cerrados de G^1_g, son aquellos divisores D de grado g de C, tales que $h^0(C, \mathscr{L}_D) = h^1(C, \mathscr{L}_{K-D}) > 1$.

En general, para $r \leq s \leq g$, los ceros del ideal $F_r^{\mathscr{O}_{S^s C}}(R^1 f_{S^s C,*}(w_C \otimes \mathscr{L}_{-\tilde{\mathscr{D}}}))$ diremos que es la subvariedad de divisores especiales de $S^s C$, de índice de especialidad mayor o igual que r y la denotaremos G^r_s.

Dado un divisor de Cartier efectivo $D \subset C$ de grado n sobre S, tenemos un epimorfismo natural $\mathscr{O}_C \to \mathscr{O}_D$. Tensando por w_C, tenemos un epimorfismo $w_C \to w_C \otimes \mathscr{O}_D$ y denotaremos $w \mapsto w(D)$. Tomando el álgebra exterior n, obtenemos un epimorfismo $\pi: \Lambda^n_S w_C \to \Lambda^n(w_C \otimes \mathscr{O}_D)$. Por otra parte, D es un punto de $S^n C$, denotemos $\mathscr{O}_{S^n C}(D)$, su anillo de funciones (o "cuerpo residual" si S es un cuerpo), tenemos un epimorfismo $\mathscr{O}_{S^n C} \to \mathscr{O}_{S^n C}(D)$. Tensando por $w_{S^n C}$, tenemos un epimorfismo $\pi': w_{S^n C} \to w_{S^n C}(D)$

1. Lema: *Existe un único isomorfismo $\Lambda^n_S w_C(D) = \mathscr{O}_{S^n C}(D)$, de modo que tenemos un diagrama conmutativo*

$$\begin{array}{ccc} \Lambda^n_S w_C & \xrightarrow{\pi} & \Lambda^n_S(w_C \otimes \mathscr{O}_D) \\ \| & & \| \\ w_{S^n C} & \xrightarrow{\pi'} & w_{S^n C}(D) \end{array}$$

Demostración. Como π y π' son epimorfismos, basta ver que $\operatorname{Ker}\pi = \operatorname{Ker}\pi'$. Basta verlo localmente. Sea $w = w_1 \wedge \ldots \wedge w_n$ un generador del $\mathscr{O}_{S^n C}$-haz de línea $w_{S^n C} = \Lambda^n_S w_C$. Dado $f \in \mathscr{O}_{S^n C}$, es fácil probar que $\pi(f \cdot w) = \det(f) \cdot \pi(w)$ y $\pi'(f \cdot w) = \det(f) \cdot \pi'(w)$. Como $\pi(w)$ y $\pi'(w)$ son generadores de los $\mathscr{O}_S$-módulos de línea $\Lambda^n_S(w_C \otimes \mathscr{O}_D)$, $\mathscr{O}_{S^n C}(D)$ concluimos. □

2. Teorema: *El subesquema de divisores especiales de grado g de C es precisamente el divisor canónico de S^gC.*

Demostración. Basta ver que ambos esquemas tienen el mismo funtor de puntos. Cambiando de base basta ver que ambos esquemas tienen los mismos puntos racionales. Sea $D \in (S^gC)^{\cdot}(S)$. De la sucesión exacta

$$0 \to w_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D} \to w_C \xrightarrow{h} w_C \otimes_{\mathscr{O}_C} \mathscr{O}_D \to 0$$

tomando imágenes directas se obtiene

$$f_* w_C \xrightarrow{h} w_C \otimes_{\mathscr{O}_C} \mathscr{O}_D \to R^1 f_*(w_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D}) \to R^1 f_*(w_C) \to 0$$

Por ser $R^1 f_*(w_C)$ un haz de línea se concluye que $F_1(R^1 f_*(w_C \otimes_{\mathscr{O}_C} \mathscr{L}_{-D}) = F_0(\mathscr{N})$, donde $\mathscr{N}$ es el conúcleo de h. Por tanto, $D \in G^1_g(S)$ si y sólo si $F_0(\mathscr{N}) = 0$, es decir, el morfismo

$$\Lambda^g(f_* w_C) = \bar{f}_* \Lambda^g w_C \to \Lambda^g(w_C \otimes_{\mathscr{O}_C} \mathscr{O}_D)$$

es nulo. Ahora bien, por el Lema 19.10.1 este morfismo es nulo si y sólo si el morfismo $\bar{f}_* w_{S^gC} \to w_{S^gC}(D)$ es nulo, es decir si y sólo si D es un punto del divisor canónico de S^gC.

□

Supongamos que C es una parametrización de curvas de género $g \geq 2$, no hiperelípticas. Consideremos el morfismo canónico

$$C \to \mathbb{P}_S((f_* w_C)^*) = \mathbb{P}^{g-1}$$

donde $\mathbb{P}^{g-1}$ denota un fibrado proyectivo sobre S de dimensión $g-1$. Por otra parte consideremos la transformación canónica

$$K : S^{g-1}C \dashrightarrow \mathbb{P}_S((\bar{f}_* w_{S^{g-1}C})^*)$$

Dado un divisor relativo de Cartier efectivo D de grado $g-1$ en C, no especial existe un único hiperplano en $\mathbb{P}^{g-1}$ que pasa por dicho divisor y por tanto se tiene un morfismo

$$G : S^{g-1}C \dashrightarrow \mathbb{P}^{g-1\,*} = \mathbb{P}(f_* w_C)$$

G está definido exactamente en el abierto de divisores no especiales, y lo llamaremos morfismo de Gauss.

3. Teorema: *El morfismo*

$$G\colon S^{g-1}C - - - > \mathbb{P}^{g-1\,*} = \mathbb{P}(f_* w_C)$$

que asigna a cada divisor efectivo de Cartier de grado $g-1$ y no especial, el único divisor canónico de C que pasa por él, coincide con el morfismo canónico

$$K\colon S^{g-1}C - - - > \mathbb{P}_S((\bar{f}_* w_{S^{g-1}C})^*)$$

Demostración. Basta ver que los morfismos inducidos sobre los funtores de puntos son los mismos. Cambiando de base si es necesario, basta verlo para los puntos racionales.

Sea $D \in (S^{g-1}C)^{\cdot}(S)$ un divisor no especial. Sea $\mathscr{L}_D$ el haz de línea en C asociado al divisor D. Se observa que por ser D no especial, para cada punto cerrado $s \in S$, $f_*(\mathscr{L}_D \otimes k(s)) = k(s)$, como $\mathscr{O}_S \subseteq f_*\mathscr{L}_D$, por el teorema de Grauert $f_*\mathscr{L}_D = \mathscr{O}_S$ y $R^1 f_* \mathscr{L}_D$ es un $\mathscr{O}_S$-módulo localmente libre de rango 1. Por dualidad se obtiene que $f_*(w_C \otimes \mathscr{L}_{-D})$ y $R^1 f_*(w_C \otimes \mathscr{L}_{-D})$ son localmente libres de rango 1.

Consideremos la sucesión exacta de haces

$$0 \to w_C \otimes \mathscr{L}_{-D} \to w_C \to w_C \otimes \mathscr{O}_D \to 0$$

y consideremos la sucesión exacta larga de cohomología

$$0 \to f_*(w_C \otimes \mathscr{L}_{-D}) \xrightarrow{i} f_* w_C \xrightarrow{h} f_*(w_C \otimes \mathscr{O}_D) \to 0$$

donde la epiyectividad de h se obtiene de que $R^1 f_*(w_C \otimes \mathscr{L}_{-D})$ y $R^1 f_* w_C$ son localmente libres de rango 1. $G(D)$ es i.

Por otro lado, h define la epiyección

$$\Lambda^{g-1}(f_* w_C) = \bar{f}_*(\Lambda^{g-1} w_C) \xrightarrow{\wedge h} \Lambda^{g-1}(f_*(w_C \otimes \mathscr{O}_D)) \to 0$$

Por el Lema 19.10.1, $K(D)$ es $\wedge h$.

Tensando, $\wedge h$ por $\Lambda^g(f_* w_C)$, basta ver que su transpuesto coincide con i. Lo cual es una simple comprobación del Álgebra Lineal.

□

Nuestro objetivo ahora es probar que el divisor de ramificación del morfismo canónico $S^{g-1}C \to \mathbb{P}^{g-1\,*}$ es precisamente el dual de la curva $C \hookrightarrow \mathbb{P}^{g-1}$ (que es un divisor irreducible del espacio proyectivo $\mathbb{P}^{g-1\,*}$) contado $\binom{2g-4}{g-3}$ veces.

El dual de C, C^* se define como el subesquema que parametriza los hiperplanos de $\mathbb{P}^{g-1}$ que son tangentes a C, es decir, aquellos tales que el divisor canónico que definen no es separable. Es decir, C^* es el cerrado de $\mathbb{P}^{g-1\,*}$ definido por el ideal de Fitting,

$F_0(\Omega_{\tilde{K}/\mathbb{P}^{g-1*}})$, donde $\tilde{K} = (C \times_S \mathbb{P}^{g-1*}) \cap \tilde{H}$, siendo $\tilde{H} \hookrightarrow \mathbb{P}^{g-1} \times_S \mathbb{P}^{g-1*}$ el hiperplano universal. Observemos que $\tilde{K}$ es el divisor universal de grado $2g-2$, $\tilde{D}_{2g-2} \subset C \times S^{2g-2}C$, restringido a $C \times \mathbb{P}^{g-1*}$.

Consideremos el diagrama cartesiano

$$\begin{array}{ccc} S^{g-1}C \times_S S^{g-1}C & \xrightarrow{s} & S^{2g-2}C \\ \uparrow & & \uparrow \\ \mathbb{H} = s^{-1}(\mathbb{P}^{g-1*}) & \xrightarrow{s} & \mathbb{P}^{g-1*} \end{array}$$

donde s es el morfismo "suma" de divisores y $\mathbb{P}^{g-1*} \hookrightarrow S^{2g-2}C$ es el subesquema cerrado de los divisores efectivos de grado $2g-2$ que son canónicos. Observemos que la primera proyección $\pi_1 \colon \mathbb{H} \to S^{g-1}C$ es un isomorfismo en el abierto complementario en $S^{g-1}C$ de los divisores especiales, de modo que sobre dicho abierto s coincide con el morfismo canónico, por 19.10.3. Por tanto, para calcular la ramificación del morfismo canónico basta calcular la ramificación del morfismo suma de divisores.

Recuérdese que la ramificación de un morfismo finito se define como el cerrado definido por el Fitting cero de las diferenciales relativas del morfismo.

4. Teorema: *El lugar de ramificación del morfismo suma*

$$s \colon S^m C \times_S S^r C \to S^{m+r} C$$

es el lugar de los divisores de grado $m+r$ singulares, es decir el cerrado de $S^{m+r}C$ definido por el Fitting cero del módulo de las diferenciales del divisor universal sobre $S^{m+r}C$, contado $\binom{m+r-2}{m-1}$-veces.

Demostración. Por ser el esquema simétrico el esquema de Hilbert de los cerrados finitos y planos sobre la base, se sabe por 19.4.2 que dado un punto racional $p \colon S \to S^n C$, entonces el espacio tangente a $S^n C$ en p es $T_p S^n C = (I/I^2)^*$, donde I es el haz de ideales de funciones de C que se anulan en el divisor de grado n definido por p. Considerando el punto identidad de $S^n C$, tenemos que el haz de módulos de las derivaciones de $S^n C$ es isomorfo a $(I_{\tilde{\mathscr{D}}_n}/I^2_{\tilde{\mathscr{D}}_n})^*$, donde $I_{\tilde{\mathscr{D}}_n}$ es el haz de ideales de las funciones de $C_{S^n C}$ que se anulan en el divisor universal de grado n, de C. Por tanto, $\Omega_{S^n C/S} = I_{\tilde{\mathscr{D}}_n}/I^2_{\tilde{\mathscr{D}}_n}$.

Escribamos $m+r=n$. Consideremos la sucesión exacta de diferenciales

$$\Omega_{S^n C} \otimes_{\mathscr{O}_{S^n C}} \mathscr{O}_{S^m C \times S^r C} \to \Omega_{S^m C \times S^r C/S} \to \Omega_{S^m C \times S^r C/S^n C} \to 0$$

Como $\Omega_{S^m C \times S^r C/S} = (\Omega_{S^m C} \otimes_{\mathscr{O}_{S^m C}} \mathscr{O}_{S^m C \times S^r C}) \oplus (\Omega_{S^r C} \otimes_{\mathscr{O}_{S^r C}} \mathscr{O}_{S^m C \times S^r C})$, simplificando notaciones, tenemos la sucesión exacta

$$(*) \qquad I_{\tilde{\mathscr{D}}_n}/I^2_{\tilde{\mathscr{D}}_n} \xrightarrow{f} I_{\tilde{\mathscr{D}}_m}/I^2_{\tilde{\mathscr{D}}_m} \oplus I_{\tilde{\mathscr{D}}_r}/I^2_{\tilde{\mathscr{D}}_r} \to \Omega_{S^m C \times S^r C/S^n C} \to 0$$

donde $I_{\tilde{\mathscr{D}}_n} = I_{\tilde{\mathscr{D}}_m} \cdot I_{\tilde{\mathscr{D}}_r}$ (en $\mathscr{O}_{C\times(S^mC\times S^rC)}$) y f es el morfismo inducido por los morfismos naturales de inclusión $I_{\tilde{\mathscr{D}}_n} \hookrightarrow I_{\tilde{\mathscr{D}}_m}$ y $I_{\tilde{\mathscr{D}}_n} \hookrightarrow I_{\tilde{\mathscr{D}}_r}$.

El morfismo f de $(*)$, es un morfismo de $B = \mathscr{O}_{S^mC\times S^rC}$-módulos localmente de rango n y por tanto $F_0^{\mathscr{O}_{S^mC\times S^rC}}(\Omega_{S^mC\times S^rC/S^nC})$ es el "determinante" de f, denotémoslo $\det_B f$. Del mismo modo $F_0^{\mathscr{O}_{S^n}}(\Omega_{S^mC\times S^rC/S^nC})$ es el determinante de f como $A = \mathscr{O}_{S^nC}$-módulo. Ahora bien,

$$\det_A f = \prod_{\sigma\in S_n/S_m\times S_r} \sigma(\det_B f)$$

Calculemos, pues, $\det_B f$. Siguiendo notaciones previas, localmente, el ideal de funciones que se anulan en $\tilde{\mathscr{D}}_n$ es $I_{\tilde{\mathscr{D}}_n} = ((t-t_1)\cdot\ldots\cdot(t-t_n) = p(t))$ y $I_{\tilde{\mathscr{D}}_n}/I^2_{\tilde{\mathscr{D}}_n} \simeq B[t]/(p(t))$. Escribamos $p_1(t) = (t-t_1)\cdot\ldots\cdot(t-t_r)$ y $p_2(t) = (t-t_{r+1})\cdot\ldots\cdot(t-t_n)$. El morfismo f es equivalente al morfismo

$$B[t]/(p(t)) \overset{p_2(t)\cdot\times p_1(t)\cdot}{\longrightarrow} B[t]/(p_1(t)) \times B[t]/(p_2(t))$$

Por tanto,

$$\det_B f = \prod_{\substack{0<i\le r\\ r<j\le n}} (t_i - t_j)$$

Luego,

$$F_0^{\mathscr{O}_{S^n}}(\Omega_{S^mC\times S^rC/S^nC}) = \prod_{\sigma\in S_n/S_m\times S_r} \prod_{\substack{0<i\le r\\ r<j\le n}} (t_{\sigma(i)} - t_{\sigma(j)})$$

Calculemos $F_0^{\mathscr{O}_{S^nC}}(\Omega_{\tilde{\mathscr{D}}_n/S^nC})$. Localmente, $\mathscr{O}_{\tilde{\mathscr{D}}_n} = \mathscr{O}_{S^nC}[t]/(p(t))$ y $\Omega_{\tilde{\mathscr{D}}_n/S^nC} = \mathscr{O}_{S^nC}[t]/(p(t), p'(t))$. Luego,

$$F_0^{S^nC}(\Omega_{\tilde{\mathscr{D}}_n/S^nC}) = \mathrm{Result}(p(t), p'(t)) = \prod_{i\neq j}(t_i - t_j)$$

Fácilmente se concluye el teorema. □

5. Teorema: *El divisor de ramificación de la trasformación canónica* $K\colon S^{g-1}C - - > \mathbb{P}^{g-1*}$ *es precisamente el dual de la curva C,* $C^* \hookrightarrow \mathbb{P}^{g-1*}$ *(que es un divisor irreducible del espacio proyectivo) contado* $\binom{2g-4}{g-3}$ *veces.*

19.11. Codimensión de las variedades de divisores especiales

En esta sección supondremos que C es una curva lisa conexa de género $g > 2$ no hiperelíptica, sobre un cuerpo algebraicamente cerrado.

Sea $C \hookrightarrow \mathbb{P}^{g-1}$ la inmersión canónica. Dados r puntos $p_1,\dots,p_r \in \mathbb{P}^{g-1}$ denotaremos $< p_1,\dots,p_r >$ a la mínima subvariedad lineal de $\mathbb{P}^{g-1}$ que pasa por dichos puntos.

Todo morfismo racional de una variedad normal en una variedad propia está definido en un abierto, cuyo complementario es un cerrado de codimensión mayor o igual que dos, porque sobre los puntos de codimensión uno está definido. En particular, todo morfismo racional de una curva en una variedad propia extiende a un morfismo global de la curva en la variedad.

1. Teorema: *La codimensión en $S^{g-1}C$ de la subvariedad G^1_{g-1} de los divisores especiales es mayor o igual que* 2.

Demostración. Supongamos por el contrario que $\mathrm{Codim}_{S^{g-1}C} G^1_{g-1} = 1$. Sea $r \le g-1$ mínimo tal que $G^1_r \subset S^r C$ es de codimensión 1. La imagen del morfismo suma $s' : G^1_{r-1} \times C \to G^1_r$ es un cerrado de codimensión mayor o igual que 1. Así pues, en general, si $D_r = p_1 + \cdots + p_r$ es un divisor especial, $D_r^{(i)} = p_1 + \cdots + \widehat{p}_i + \cdots + p_r$ no es especial. Luego, $< p_1,\dots,p_r >=< p_1,\dots,\widehat{p}_i,\dots,p_r >$ para cada $i \le r$. Se verifica que la imagen por el morfismo suma $s : G^1_r \times S^{g-1-r}C \to S^{g-1}C$ es de codimensión 1 y contenido en G^1_{g-1}. Por tanto, el morfismo de Gauss, G, está definido en un abierto de $\mathrm{Im}\, s$, pues G está definido fuera de un cerrado de codimensión mayor o igual que 2. Sea $D_{g-1} \in \mathrm{Im}\, s$ sobre el que está definido G, y de modo que $D_{g-1} = D_r + D_{g-1-r}$, con $D_r = p_1 + \cdots + p_r \in G^1_r$ y $D_r^{(i)}$ no especial.

Fijado el índice $i \le r$, consideremos C como curva en la variedad de divisores de grado $g-1$ de la forma:

$$\tilde{p} \mapsto D_{g-1}(\tilde{p}) = p_1 + \cdots + p_{i-1} + \tilde{p} + p_{i+1} + \cdots + p_r + D_{g-1-r}$$

Es claro que $D_{g-1}(p_i) = D_{g-1}$, luego el morfismo de Gauss está definido en un entorno de puntos $\tilde{p}$ de p_i. Ahora bien, por definición $G(D_{g-1}(\tilde{p}))$ es un hiperplano que pasa por $D_{g-1}(\tilde{p})$, luego en particular pasa por $p_1,\dots,\widehat{p}_i,\dots,p_r$ y, por tanto, por p_i, pues $< p_1,\dots,p_r >=< p_1,\dots,\widehat{p}_i,\dots,p_r >$. De aquí que:

$$G(D_{g-1}(\tilde{p})) \cap C = D_{g-1} + \tilde{p} + \overline{D}_{g-2}(\tilde{p})$$

para cierto divisor $\overline{D}_{g-2}(\tilde{p})$ de grado $g-2$ que depende de $\tilde{p}$. En particular, $G(D_{g-1}) \cap C = G(D_{g-1}(p_i)) \cap C = D_{g-1} + p_i + \overline{D}_{g-2}(p_i)$. Es decir, p_i aparece 2 veces en $G(D_{g-1}) \cap C$.

Variando $i = 1,\dots,r$ se concluye que $G(D_{g-1}) \cap C = 2D_r + D_{(g-1)-r} + D'_{g-1-r}$, para cierto divisor D'_{g-1-r} de grado $g-1-r$. Dicho de otro modo:

"El hiperplano $G(D_{g-1})$ es tangente a la curva en cada uno de los puntos $p_1,\dots,p_r$ de D_r".

Por otro lado, *dado un divisor D_{r-1} de grado $r-1$, existe un $p_r \in C$ tal que $D_{r-1}+p_r$ es especial*: si $s\colon S^{r-1}C \times C \to S^rC$ es el morfismo suma, entonces se trata de ver que si $s^{-1}G^1_r$ es la fibra de los divisores especiales, entonces la primera proyección $s^{-1}G^1_r \to S^{r-1}C$ es un epimorfismo. Pero por ser ambos esquemas propios de la misma dimensión, basta ver que es genéricamente de fibras finitas, lo cual es inmediato, pues genéricamente $D_{r-1} = p_1 + \cdots + p_{r-1}$ es no especial y, por tanto, $D_{r-1}+p_r$ es especial si y sólo si $p_r \in < p_1,\dots,p_{r-1} > \cap C$ y este último conjunto es finito por ser $C \hookrightarrow \mathbb{P}^{g-1}$ una curva alabeada.

Con todo, para todo punto $(p_1,\dots,p_{r-1},p_{r+1},\dots,p_{g-1})$ de un cierto abierto $U \subset C^{g-2}$, $p_1 + \dots + p_{r-1}$ no es especial, existe un un punto p_r de modo que $p_1 + \dots + p_r$ es especial y existe $G(p_1 + \cdots + p_{g-1})$. Así pues, para cada par de puntos (p_1,p_2) de un abierto de C^2 existe un abierto $V_{1,2}$ de puntos de C^{g-4} de modo que $(p_1,p_2) \times V_{12} \subset U$. Por tanto, para todo punto $(p_3,\cdots,p_{g-2}) \in V_{12}$, existe un hiperplano que pasa por p_i, $1 \le i \le g-2$ y es tangente a C en p_1 y p_2. Esto implica que las tangentes en p_1 y p_2 son co-2-planarias. Luego todas las tangentes de C pasan por un punto. Luego C es una "*strange curve*" y, en particular $g = 0$ (véase los comentarios previos a 14.9.28), lo cual es contradictorio. □

2. Corolario: *La codimensión en $S^{g-1}C$ del subesquema G^r_{g-1} de los divisores especiales con índice de especialidad $\ge r$ es:*

$$\operatorname{Codim}_{S^{g-1}C} G^r_{g-1} \ge r+1$$

($r \le g-1$).

Demostración. Supongamos por el contrario que $\operatorname{Codim}_{S^{g-1}C} G^r_{g-1} \le r$. Sea $n \le g-1$ mínimo tal que $\operatorname{Codim}_{S^nC} G^r_n \le r$ y, por tanto, $\operatorname{Codim}_{S^{n-1}C} G^r_{n-1} \ge r+1$.

Consideremos el morfismo finito suma:

$$s\colon S^{n-1}C \times C \to S^nC$$

y $\overline{G}^r_n = s^{-1}(G^r_n) - G^r_{n-1} \times C$ que es de codimensión $\le r$ en $S^{n-1}C \times C$.

La primera proyección:

$$\pi_1\colon \overline{G}^r_n \to S^{n-1}C$$

valora en G^{r-1}_{n-1}, pues al quitarle un punto a un divisor su índice de especialidad disminuye como mucho en 1. Además π_1 es de fibras finitas pues si $(D_{n-1},p) \in \overline{G}^r_n$, entonces

$D_{n-1} \notin G^r_{n-1}$ y $D_{n-1}+p \in G^r_n$, es decir, p pertenece al corte de la curva con la mínima subvariedad lineal (de $\mathbb{P}^{g-1}$) conteniendo a D_{n-1}, es decir, $p \in < D_{n-1} > \cap C$ y este subesquema es finito por ser $C \hookrightarrow \mathbb{P}^{g-1}$ alabeada.

En conclusión, $\pi_1(\overline{G}^r_n) \subset G^{r-1}_{n-1}$ tiene la misma dimensión que $\overline{G}^r_n$, es decir, la misma que G^r_n y, por tanto, $\mathrm{Codim}_{S^{n-1}C} G^{r-1}_{n-1} = \dim S^{n-1}C - \dim G^{r-1}_{n-1} \leq \dim S^n C - 1 - \dim G^r_n = \mathrm{Codim}_{S^nC} G^r_n - 1 \leq r-1$, luego

$$\mathrm{Codim}_{S^{g-1}C} G^{r-1}_{g-1} \leq r-1$$

ya que $G^{r-1}_{n-1} + S^{g-1-(n-1)}C \subset G^{r-1}_{g-1}$. Recurrentemente en r se obtiene la contradicción con el teorema anterior

$$\mathrm{Codim}_{S^{g-1}C} G^1_{g-1} \leq 1$$

□

Dado $D \in S^{g-1}C - G^1_{g-1}$, denotaremos por D^* al único divisor $D^* \in S^{g-1}C$ tal que $D+D^*$ es un divisor canónico. Observemos que $h^0(C,\mathscr{L}_D) = h^0(C,\mathscr{L}_{K-D})$, luego D^* no es especial. Obviamente el morfismo

$$S^{g-1}C - G^1_g \xrightarrow{*} S^{g-1}C - G^1_g$$

es un isomorfismo, que al cuadrado es el morfismo identidad.

3. Teorema: *El subesquema en S^gC de los divisores especiales de grado g es un divisor irreducible íntegro.*

Demostración. Veamos que es irreducible. Sabemos que G^1_g es el divisor canónico, luego es unión de cerrados irreducibles de codimensión 1. Por dimensiones tenemos que el complementario de la imagen del morfismo suma $C \times G^1_{g-1} \to G^1_g$ es un abierto U denso de G^1_g. Dado $D \in U$, tenemos que $D = p + D_{g-1}$, con D_{g-1} no especial. Así pues, el único divisor canónico que contiene a D_{g-1}, contiene a D. Por tanto, D^*_{g-1} contiene a p. Escribamos, $D^*_{g-1} = p + D'$, con $D' \in S^{g-2}C$. Tenemos que $D_{g-1} = D^{**}_{g-1} = (p+D')^*$ y $D = p + (p+D')^*$. En conclusión, sea $V = \{(p,D') \in C \times S^{g-2}C$, tales que $p+D'$ sea no especial$\}$, que es un abierto (irreducible) de $C \times S^{g-2}C$, la imagen, que es irreducible, del morfismo

$$V \to S^gC,\ (p,D') \mapsto p + (p+D')^*$$

contiene a U, luego sus cierres en S^gC coinciden y G^1_g es irreducible.

Por último, sea $D = p_1 + \ldots + p_{g-1}$ un divisor no especial, con $p_i \neq p_j$ si $i \neq j$. Sea $h: C \hookrightarrow S^gC$ definido por $h(p) = p + D^*$. Se tiene que $h^{-1}(G^1_g - G^2_g) = D$: Sea $f: C \to S$ el morfismo estructural. Un divisor $D' \in G^1_g - G^2_g$ si y sólo si $f_*\mathscr{L}_{K-D'}$ es localmente de rango 1 (y así sucede en fibras sobre S), que equivale a que existe un único divisor

canónico K que contiene a D' (y así sucede en fibras sobre S). D^* es no especial y existe un único canónico que lo contiene, $D+D^*$. Luego $p+D^* \in G^1_g - G^2_g$ si y sólo si $p \in D$ y hemos concluido. Si G^1_g no fuese íntegro, entonces D sería n-veces un divisor, con $n>1$, y por la elección de D esto no sucede.

□

19.12. Teorema de estructura del morfismo de Abel

Los morfismos lisos pueden ser caracterizados en términos del funtor de puntos. Puede demostrarse con tal caracterización la lisitud $\mathrm{Pic}_{C/S}$. Procedamos de otro modo.

Sea C una curva lisa sobre un cuerpo k, de género $g>0$. Consideremos la inmersión canónica $C \hookrightarrow \mathbb{P}(H^0(C,\mathscr{L}_{3K})^*)$. Para todo haz de línea $\mathscr{L}_D$,

$$\chi(C,\mathscr{L}_D(n)=\mathscr{L}_{D+3nK}) = (6g-6)n+(1-g+\mathrm{gr}\,D)$$

Por tanto, $\mathrm{Pic}_{C/S} = \coprod_m \mathrm{Pic}^m_{C/S}$, donde $\mathrm{Pic}^m_{C/S}$ representa los haces de línea asociados a divisores de grado m. Dado un haz de línea $\mathscr{L}'$ asociado a un divisor de grado r, define el isomorfismo

$$\mathrm{Pic}^m_{C/S} \simeq \mathrm{Pic}^{m+r}_{C/S}\,,\ \mathscr{L} \mapsto \mathscr{L}\otimes\mathscr{L}'$$

Denotaremos que $J^r_C = \mathrm{Pic}^r_{C/S}$ y diremos que es la jacobiana de C.

Al morfismo

$$A : S^r C \to J^r_C,\ D \mapsto \mathscr{L}_D$$

lo llamaremos morfismo de contracción de Abel, cuando $r=g$.

El morfismo de contracción de Abel es un morfismo birracional proyectivo. Todo morfismo birracional es la explosión a lo largo de un cerrado (Problema 7 del capítulo 13). El objetivo de esta sección es probar que el morfismo de Abel es la explosión de la Jacobiana de la curva a lo largo de los haces de línea especiales.

1. Teorema: *Sea $f: C \to S$ una curva relativa lisa conexa de género g y sea $\mathscr{L}$ un haz de línea. Se verifica que dar un divisor relativo de la serie lineal asociada a $\mathscr{L}$ equivale a dar un cociente de línea de $R^1 f_*(\omega_C \otimes \mathscr{L}^{-1})$ como $\mathscr{O}_S$-módulos. En particular,*

$$\mathrm{S}^r C \approx \mathrm{Proj}\, S^{\cdot}_{J^r C} R^1 \bar{f}_*(\omega_{C_{J^r C}} \otimes \tilde{\mathrm{L}}^{-1})$$

donde $\bar{f}: C_{J^r C} \to J^r C$ es la proyección natural y $\tilde{\mathrm{L}}$ es el haz de línea universal.

Demostración. Si $D \subset C$ es un divisor asociado a $\mathscr{L}$, e I_D es el haz de ideales que define D, entonces $\mathscr{L} = I_D^{-1} \otimes f^*\mathscr{N}$ para algún haz de línea $\mathscr{N}$ sobre la base S. De la sucesión exacta:

$$0 \longrightarrow I_D \longrightarrow \mathscr{O}_C \longrightarrow \mathscr{O}_D \longrightarrow 0$$

tensada por $\omega_C \otimes f^*\mathscr{N}^{-1}$ y considerando la sucesión larga de cohomología se obtiene una epiyección:

$$R^1f_*(\omega_C \otimes \mathscr{L}^{-1}) \to R^1f_*(\omega_C) \otimes \mathscr{N}^{-1} \to 0$$

que define un cociente de línea de $R^1f_*(\omega_C \otimes \mathscr{L}^{-1})$, por ser $R^1f_*(\omega_C) = \mathscr{O}_S$. Recíprocamente, dado un cociente de línea $R^1f_*(\omega_C \otimes \mathscr{L}^{-1}) \to \mathscr{M}$, tomando dual en $\mathscr{M}$ se obtiene por dualidad una inyección $0 \to \mathscr{L}^{-1} \otimes f^*\mathscr{M}^{-1} \to \mathscr{O}_C$, que lo sigue siendo para todo cambio de base $S' \to S$, luego el conúcleo $\mathscr{O}_D = \mathscr{O}_C/(\mathscr{L}^{-1} \otimes f^*\mathscr{M}^{-1})$ es de soporte finito en fibras sobre S y $Tor^1_{\mathscr{O}_S}(\mathscr{O}_D, k) = 0$, para cada cuerpo residual k de puntos cerrados de $\mathscr{O}_S$. Por tanto, D es un divisor de C plano sobre S y es de la serie lineal correspondiente a $\mathscr{L}$.

Por último, el morfismo $S^rC \to J^r_C$ es el morfismo de fibras para cada haz de línea en C (es decir, un punto de J^r_C) la serie lineal asociada al haz de línea, que es lo que dice el isomorfismo del enunciado. □

2. Corolario : *El morfismo de contracción de Abel es un morfismo birracional. Además, J^g_C es una variedad propia de dimensión g lisa.*

Demostración. Por el teorema anterior, $A : S^gC - G^1_g \to J^g_C - A(G^1_g)$ es un isomorfismo por el Main Theorem de Zariski, ya que las fibras de cada punto es un único punto. Además, el morfismo de Abel es epiyectivo, luego J^g_C es una variedad propia, de dimensión g. Por 19.7.10, el espacio tangente a J^g_C en el origen, es isomorfo a $H^1(C, \mathscr{O}_C)$, es decir de dimensión g, luego J^g_C es geométricamente regular en el origen, luego por traslaciones en todo punto, es decir, es lisa. □

Si $\tilde{Ł}$ es el haz de línea universal, para $r \le s \le g$, los ceros del ideal $F_r^{\mathscr{O}_{J^s_C}}(R^1f_{J^s_C,*}(w_C \otimes \tilde{Ł}))$ diremos que es la subvariedad de haces de línea especiales de J^sC, de índice de especialidad mayor o igual que r y la denotaremos W^r_s. Si $A : S^sC \to J^sC$, es el morfismo que asigna a cada divisor el haz de línea asociado, entonces $(\mathrm{Id} \times A)^*\tilde{Ł} = \mathscr{L}_{\mathscr{D}}$ (salvo subidas de haces de línea de S^sC) y por tanto, $A^*W^r_s = G^r_s$.

3. Corolario : *El morfismo $S^{g-1}C \to J^{g-1}_C$ que asigna a cada divisor el haz de línea asociado, establece un isomorfismo de $S^{g-1}C$ con su imagen esquemática, fuera de G^1_{g-1}.*

Demostración. El morfismo $A : S^{g-1}C - G^1_{g-1} \to J^{g-1}_C - W^1_{g-1}$ es un morfismo propio, de modo que la fibra (esquemática) de cada punto es un único punto. Por el Main Theorem de Zariski es un morfismo finito que ha de ser isomorfismo. □

4. Observación : Dado un punto racional $p \in C$, trasladando por el haz de línea $\mathscr{L}_p$, tenemos que $J^{g-1}_C \simeq J^g_C$. La imagen del morfismo natural inducido $S^{g-1}C \to J^g_C, D \mapsto$

$\mathscr{L}_{p+D}$ contiene a W_g^1, pues dado $\mathscr{L}_D \in W_g^1$, existe un $D' \in S^{g-1}C$ de modo que D es linealmente equivalente a $p+D'$.

Observemos que G_g^2 es de codimensión mayor o igual que uno en el esquema irreducible G_g^1, porque si no topológicamente tendríamos que $G_g^2 = G_g^1$, lo cual implicaría que el morfismo suma $C \times G_{g-1}^1 \to G_g^1$ es epiyectivo, y esto es falso por dimensiones. Por tanto, las fibras del morfismo $G_g^1 \to W_g^1$ son genéricamente de dimensión uno, lo que implica que $\dim W_g^1 = g-2$.

Dado un morfismo propio birracional $A\colon X \to Y$ entre variedades normales, el conjunto $U \subset Y$ de puntos de fibras finitas es un abierto y por el Main Theorem de Zariski $A^{-1}(U)$ es isomorfo a U. Denominemos $Y-U$ el locus excepcional.

5. Lema: *Sea $A\colon S \to J$ un morfismo birracional entre variedades lisas propias. Supongamos que el locus excepcional W y su fibra, $G = A^{-1}W$ son íntegros y que G es un divisor. Entonces*

1. *Si $D \subset J$ es un divisor que pasa por W, entonces*

$$A^*D = \overline{D} + m \cdot G$$

   siendo $\overline{D}$ la trasformada propia de D (el cierre de la fibra de D en el abierto $S-G$) y m es la multiplicidad de D a lo largo de W (es decir, la multiplicidad de D en el anillo local de J en el punto genérico de W).

2. *Si ν_W y ν_G son las valoraciones $\mathfrak{p}$-ádicas correspondientes a W y G respectivamente, entonces $\nu_W = \nu_G$.*

3. *Si $S = S^gC$, $J = J_C^g$ y A el morfismo de Abel entonces $A^*(A_*(p+S^{g-1}C)) = (p+S^{g-1}C) + G_g^1$*

Demostración. Es claro que los apartados 1 y 2 son equivalentes. Veamos el segundo. Sea $z \in G$, el punto donde centra ν_W y sea $\mathfrak{p}$ el ideal de W en $\mathscr{O}_{J,W}$ (anillo local de J en el punto genérico de W). Sea $f \in \mathscr{O}_{J,W}$ y $\nu_W(f) = m$, se verifica que $f \in \mathfrak{p}^m - \mathfrak{p}^{m+1}$. Si g es la ecuación local de G en z se verifica que $f = g^m \cdot h$, para alguna función $h \in \mathscr{O}_{S,z}$. Ahora $m = \nu_W(f) = m \cdot \nu_W(g) + \nu_W(h)$ y como $\nu_W(g) \geq 1$ (pues ν_W centra en z) y $\nu_W(h) \geq 0$, se concluye que $\nu_W(h) = 0$. Por tanto, h es invertible en $\mathscr{O}_{S,z}$, luego en $\mathscr{O}_{S,G}$ y $\nu_G(f) = m$.

Veamos el apartado 3: $A_*(p+S^{g-1}C)$ es regular en el punto genérico de W_g^1, porque este es un punto de codimensión 1 de $A_*(p+S^{g-1}C)$, el cual es regular en codimensión 1, por el corolario anterior. Por tanto, la multiplicidad de $A_*(p+S^{g-1}C)$ a lo largo de W_g^1 es 1 y concluimos por 1.

□

El divisor universal $\tilde{\mathscr{D}}$ en $C \times S^g C$ define el haz de línea $\mathscr{L}_{\tilde{\mathscr{D}}}$, que define el morfismo

$$A : S^g C \to J_C^g =: J_C,\ D \mapsto \mathscr{L}_D$$

que se denomina morfismo de Abel. Si $\tilde{\mathrm{L}}$ es un haz de línea universal, en $C \times J_C$, el morfismo de Abel viene caracterizado por $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}} = \mathscr{L}_{\tilde{\mathscr{D}}} \otimes f_{S^g C}^* \mathscr{N}$, donde $\mathscr{N}$ es un haz de línea en $S^g C$ y $f_{S^g C} : C \times S^g C \to S^g C$ la proyección natural. En general, denotemos $f_Z : C \times Z \to Z$ la proyección natural.

Por sencillez supongamos que el esquema base S es el espectro de un cuerpo.

6. Proposición: *Existe un único haz de línea universal* $\tilde{\mathrm{L}}$ *en* $C \times J_C$ *tal que su imagen inversa en* $C \times S^g C$ *es precisamente* $\mathscr{L}_{\tilde{\mathscr{D}}} \otimes w_{S^g C}$.

Demostración. Como sabemos $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}} = \mathscr{L}_{\tilde{\mathscr{D}}} \otimes f_{S^g C}^* \mathscr{N}$, donde $\mathscr{N}$ es un haz de línea en $S^g C$. Sea $U = S^g C - G_g^1 = J_C - W_g^1$. Existe un único haz de línea en $\mathscr{N}'$ en J_C cuya restricción a U es $\mathscr{N}$. Si tensamos $\tilde{\mathrm{L}}$ por $f_{J_C}^*(\mathscr{N}'^{-1})$, podemos suponer que $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}}$ es igual a $\mathscr{L}_{\tilde{\mathscr{D}}}$ sobre $C \times U$. Por tanto, $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}} = \mathscr{L}_{\tilde{\mathscr{D}}} \otimes \mathscr{L}_{n(C \times G_g^1)}$. Como $\mathscr{L}_{G_g^1} = w_{S^g C}$, simplificando notaciones tenemos que $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}} = \mathscr{L}_{\tilde{\mathscr{D}}} \otimes w_{S^g C}^n$. Basta probar que $n = 1$.

Cambiando de base, sea $p \in C$ un punto racional. Restringiendo $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}}$ y $\mathscr{L}_{\tilde{\mathscr{D}}}$ a $p \times S^g C$, se puede determinar n. En efecto:

$\mathscr{L}_{\tilde{\mathscr{D}}}$ restringe en $p \times S^g C$ en el haz de línea asociado a $\tilde{\mathscr{D}} \cap (p \times S^g C) = p \times (p + S^{g-1} C)$.

$\tilde{\mathrm{L}}$ restringe en $p \times U$ en el mismo haz de línea, es decir, en el asociado al divisor $A_*(p + S^{g-1} C - W_g^1)$. Por ser W_g^1 de codimensión 2, es claro que $\tilde{\mathrm{L}}$ restringido a $p \times J_C$ es el haz de línea asociado al divisor $A_*(p + S^{g-1})$. Por tanto, $(\mathrm{Id} \times A)^* \tilde{\mathrm{L}}$ restringe en el haz de línea asociado a $A^*(A_*(p + S^{g-1} C)) = (p + S^{g-1} C) + G_g^1$, igualdad que se debe al apartado 3 del lema anterior □

Consideremos el epimorfismo natural

$$R^1 f_{S^g C,*}(\omega_{C_{S^g C}} \otimes \mathscr{L}_{\tilde{\mathscr{D}}}^{-1}) \to R^1 f_{S^g C,*}(\omega_{C_{S^g C}}) = \mathscr{O}_{S^g C}$$

que es isomorfismo en el complementario de G_g^1.

Si $i : U = J_C - W_g^1 \hookrightarrow J_C$ es la inclusión natural, entonces teniendo en cuenta que:

1. A es un isomorfismo en U,
2. El primer funtor derivado R^1 cambia de base
3. la epiyección natural anterior,

se obtiene un isomorfismo $\varphi_U : R^1 f_{J_C,*}(\omega_{C_{J_C}} \otimes \tilde{\text{Ł}}^{-1})_{|U} \to \mathcal{O}_U$, de donde tomando i_* se obtiene un morfismo natural:

$$\varphi : R^1 f_{J_C,*}(\omega_{C_{J_C}} \otimes \tilde{\text{Ł}}^{-1}) \to \mathcal{O}_{J_C}$$

ya que $i_*\mathcal{O}_U = \mathcal{O}_{J_C}$, por ser $Codim_{J_C} W_g^1 = 2$. Además este morfismo es único con la condición de que $\varphi_{|U} = \varphi_U$.

Cambiando de base ϕ, por un morfismo birracional $g : Z \to J_C$, tal que $g_U : g^{-1}U \to U$ sea isomorfismo, obtenemos

$$\varphi_Z : R^1 f_{Z,*}(\omega_{C_Z} \otimes \tilde{\text{Ł}}_g^{-1}) \to \mathcal{O}_Z$$

siendo $\tilde{\text{Ł}}_g = (1 \times g)^* \text{Ł}$, único con la condición de que $\varphi_{Z|U} = \varphi_U$.

Por otro lado, por ser φ_Z un isomorfismo en U, se concluye que $\ker \varphi_Z$ es la torsión de $R^1 f_{Z,*}(\omega_{C_Z} \otimes \tilde{\text{Ł}}_g^{-1})$.

7. Lema : *Sea $g : Z \to J_C$ en las hipótesis de arriba y $\varphi_Z : R^1 f_{Z,*}(\omega_{C_Z} \otimes \tilde{\text{Ł}}_g^{-1}) \to \mathcal{O}_Z$ el morfismo definido. La condición necesaria y suficiente para que g factorice a través de $A : \mathrm{S}^g C \to J_C$ es que el ideal $\operatorname{Im} \varphi_Z \subset \mathcal{O}_Z$ sea localmente principal.*

Demostración. Si $\operatorname{Im} \varphi_Z$ es localmente principal, por ser $\varphi_Z : R^1 f_{Z,*}(\omega_{C_Z} \otimes \tilde{\text{Ł}}_g^{-1}) \to \operatorname{Im} \varphi_Z$ un epimorfismo, se concluye que $\tilde{\text{Ł}}_g$ admite un divisor (lema 19.12.1) y, por tanto, un morfismo $s : Z \to \mathrm{S}^g C$ tal que $A \circ s = g$. Recíprocamente, si g factoriza a través de A, entonces $\tilde{\text{Ł}}_g$ admite un divisor, es decir, un cociente de línea $R^1 f_{Z,*}(\omega_{C_Z} \otimes \tilde{\text{Ł}}_g^{-1}) \to \mathcal{N}$. Pero este epimorfismo factoriza a través del cociente por la torsión del primero, es decir, define un epimorfismo $\operatorname{Im} \varphi_Z \to \mathcal{N}$, luego un isomorfismo, ya que es genéricamente un isomorfismo y el núcleo sería de torsión, es decir, 0 ya que $\operatorname{Im} \varphi_Z \subset \mathcal{O}_Z$. □

En el caso $Z = \mathrm{S}^g C$ es $\tilde{\text{Ł}}_A = \mathscr{L}_{\mathscr{D}} \otimes_{\mathcal{O}_{\mathrm{S}^g C}} \mathscr{L}_{G_g^1}$ y, por tanto, es fácil ver que $\operatorname{Im} \varphi_{\mathrm{S}^g C} = \mathscr{L}_{G_g^1}^{-1} = \mathfrak{p}_{G_g^1}$ el haz de ideales que se anula en G_g^1.

8. Teorema : *$A : \mathrm{S}^g C \to J_C$ es el morfismo de explosión por el haz de ideales $\operatorname{Im} \varphi \subset \mathcal{O}_{J_C}$.*

Demostración. Sea $\tilde{J}_C \to J_C$ el morfismo de explosión en el haz de ideales $\operatorname{Im} \varphi$. Por el lema anterior este morfismo factoriza a través de $S^g C$. Por otra, parte la explosión de $S^g C$ en $(\operatorname{Im} \varphi) = \mathfrak{p}_{G_g^1} \subset \mathcal{O}_{S^g C}$ es $S^g C$. Luego tenemos el morfismo $S^g C \to \tilde{J}_C$. Con lo que concluimos. □

9. Teorema : *Sea C una curva lisa conexa de género $g > 2$ no hiperelíptica y sea $A : \mathrm{S}^g C \to J_C$ el morfismo de Abel. Se verifica que el morfismo de Abel es el morfismo de explosión con centro en el ideal primo correspondiente a la subvariedad de haces de línea especiales de grado g, $W_g^1 \subset J_C$.*

Demostración. Sea $I = \operatorname{Im}\varphi$. Usando el lema de estabilidad, se obtiene para $n \gg 0$ las inclusiones $\mathfrak{p}^n_{W^1_g} \supset I^n = A_*(I^n \cdot \mathscr{O}_{\mathrm{S}^g C}) = A_* \mathfrak{p}^n_{G^1_g} \supset \mathfrak{p}^n_{W^1_g}$, luego $\mathfrak{p}^n_{W^1_g} = I^n$. Ahora como la explosión por $I^n = \mathfrak{p}^n_{W^1_g}$ es la misma que por I y que por $\mathfrak{p}_{W^1_g}$, se concluye. □

19.13. Teorema de Torelli

1. Teorema: *Si denotamos* $K\colon \mathrm{S}^{g-1}C \dashrightarrow \mathbb{P}^{g-1*}$ *la trasformación canónica,* $q\colon S \to C$ *un punto racional y* $H_q \subset \mathbb{P}^{g-1*}$ *el hiperplano que éste define, entonces la fibra de este hiperplano por K rompe en dos componentes homólogas por la involución* $*\colon S^{g-1}C \dashrightarrow S^{g-1}C$*, es decir, se verifica que*

$$K^{-1}(H_q) = W_q \cup W_q^*$$

siendo W_q *el subesquema de divisores de grado* $g-1$ *tales que al sumarle q es un divisor especial, es decir,* $q + W_q = G^1_g \cap (\mathrm{S}^{g-1}C + q)$ *y* W_q^* *es el subesquema de divisores de grado* $g-1$ *que contienen a q, es decir,* $W_q^* = \mathrm{S}^{g-2}C + q$.

Demostración. Basta probar que ambos subesquemas cerrados de $\mathrm{S}^{g-1}C$ tienen los mismos puntos. Cambiando de base, basta ver que tienen los mismos puntos racionales para lo cual se puede suponer que S es conexo. Por otro lado, por ser todos los subesquemas del enunciado divisores de $\mathrm{S}^{g-1}C$ sobre S, basta probar la igualdad en el abierto $V = \mathrm{S}^{g-1}C - G^1_{g-1} - (2q + S^{g-3}C)$.

Dado un punto $p'\colon S \to K^{-1}(H_q) \cap V$ su imagen por K define un hiperplano $H_{p'} \hookrightarrow \mathbb{P}^{g-1}$ y éste a su vez un divisor canónico en la curva, $K_{p'} = H_{p'} \cap C$, que contiene a q (por construcción) y sus diferenciales son nulas a lo largo de este punto, luego q es una componente conexa de $K_{p'}$ y por tanto es $K_{p'} = q \coprod (K_{p'} - q)$.

Ahora bien, si $D_{p'}$ es el divisor que define el punto $p'\colon S \to \mathrm{S}^{g-1}C$, entonces, por construcción, está contenido en $K_{p'}$, es decir, $D_{p'} \hookrightarrow K_{p'}$, luego contiene a q o lo contiene su complementario $K_{p'} - D_{p'}$, es decir, es un divisor correspondiente a un punto de $\mathrm{S}^{g-2}C + q \subset \mathrm{S}^{g-1}C = W_q^*$ o es un divisor tal que al sumarle q es especial, es decir, se corresponde con un punto de $(\mathrm{S}^{g-1}C + q) \cap G^1_g = W_q$. □

Observemos que el morfismo $*\colon J^{g-1}_C \to J^{g-1}_C$, $\mathscr{L} \mapsto \mathscr{L}^{-1} \otimes \mathscr{L}_K$ es una involución, que hace conmutativo el diagrama

$$\begin{array}{ccc} S^{g-1}C & \overset{*}{\dashrightarrow} & S^{g-1}C \\ \downarrow & & \downarrow \\ J^{g-1}_C & \xrightarrow{\ *\ } & J^{g-1}_C \end{array}$$

2. Lema: *Sea C una curva lisa no hiperelíptica de género mayor que 2. El número de multitangentes de C, de su inmersión canónica en $\mathbb{P}^{g-1}$, es finito.*

Demostración. Si consideramos el morfismo de C en la grassmanniana de rectas de $\mathbb{P}^{g-1}$, que asigna a cada punto de C su recta tangente y el lema no se verifica, entonces el morfismo de C en su imagen no es puramente inseparable. Luego toda tangente sería multitangente, salvo para un número finito de tangentes.

Supongamos que g es par. Sean $2g-4$ puntos distintos $p_1,\dots,p_{\frac{g-2}{2}}$, $p'_1,\dots,p'_{\frac{g-2}{2}}$, de modo que la recta tangente que pasa por p_i pasa por p'_i para todo i. Sea K un divisor canónico y $D=\sum_i 2p_i+2p'_i$. Tenemos que

$$2\leq \dim_k H^0(C,L_{K-2p_1-\dots-2p_{\frac{g-2}{2}}})=\dim_k H^0(C,L_{K-D})$$

Ahora bien, $K-D$ es un divisor de grado 2, luego C sería una curva hiperelíptica.

Supongamos que g es impar. Sean $2g-6$ puntos distintos $p_1,\dots,p_{\frac{g-3}{2}}$, $p'_1,\dots,p'_{\frac{g-3}{2}}$, de modo que la recta tangente que pasa por p_i pasa por p'_i para todo i. Sea K un divisor canónico y $D=\sum_{i>1} 2p_i+2p'_i$. Tenemos que

$$3\leq h^0(C,L_{K-2p_1-\dots-2p_{\frac{g-1}{2}}})=h^0(C,L_{K-D})$$

$K-D$ es un divisor de grado 4. Si $h^0(C,L_{K-D})>3$ o cualquier hiperplano que pase por $D+p$ (para cierto $p\in C$) implica que pasa por $D+p+q$ (para cierto $q\in C$) es fácil demostrar de nuevo que C es hiperelíptica. Por tanto, el morfismo natural $C\hookrightarrow \mathbb{P}(H^0(C,L_{K-D})^*)=\mathbb{P}^2$ define un isomorfismo de C con una curva plana no singular de grado 4. El morfismo de C en la curva plana dual C^*, que asigna a cada punto de C su recta tangente, viene definido por el morfismo $C\to\mathbb{P}(H^0(C,L_{K-D}))$, $p\mapsto 2p+2p'$, donde denotamos por p' el segundo punto de tangencia de la recta tangente a C en p. El automorfismo $\tau\colon C\to C$, $\tau(p):=p'$, cumple que $\tau^2=\mathrm{Id}$ e induce una proyectividad en $\mathbb{P}(H^0(C,L_{K-D}))$, que sobre la curva dual es la identidad. Por tanto, la curva dual es una recta proyectiva, luego todas las tangentes a C pasan por un punto. En conclusión, C es una strange curve, luego su género es cero y hemos llegado a contradicción.

□

3. Teorema de Torelli: *Los automorfismos de C están en correspondencia biunívoca con el conjunto de los automorfismos de J_C^{g-1}, que dejan estable a $W_{g-1}:=W^0_{g-1}$, módulo la involución $*$.*

Demostración. Todo automorfismo τ de la curva induce un automorfismo de la Jacobiana de la curva, que deja estable W_{g-1}. Además, τ es el automorfismo identidad si y sólo si el automorfismo inducido en W_{g-1} o $S^{g-1}C$ es el automorfismo identidad.

W_{g-1} es una variedad de Gorenstein, por ser una hipersuperficie de una variedad regular. W_{g-1} es una variedad normal porque es regular al localizar por los puntos codimensión 1, pues es isomorfa a $S^{g-1}C$ fuera de un cerrado de codimensión 2. Por dualidad 15.4.14, si denotamos $A' \colon S^{g-1}C \to W_{g-1}$ el morfismo natural, tenemos que el dualizante de $S^{g-1}C$ es igual a la subida del dualizante de W_{g-1}, ya que fuera de un cerrado de codimensión 2 coinciden. Igualmente, $A'_*(w_{S^{g-1}C}) = w_{W_{g-1}}$. Por tanto, las secciones globales del dualizante de W_{g-1} coincide con las de $S^{g-1}C$. Por tanto, el morfismo canónico de W_{g-1} ramifica en el dual de C.

Dado un automorfismo T de la Jacobiana que deja estable a W_{g-1}, tenemos un cuadrado conmutativo

$$\begin{array}{ccc} W_{g-1} & \xrightarrow{K} & \mathbb{P}(H^0(W_{g-1}, w_{W_{g-1}})^*) = \mathbb{P}(H^0(C, w_C)) \\ \downarrow T & & \downarrow T' \\ W_{g-1} & \xrightarrow{K} & \mathbb{P}(H^0(W_{g-1}, w_{W_{g-1}})^*) = \mathbb{P}(H^0(C, w_C)) \end{array}$$

de modo que T' deja estable la ramificación, es decir, el dual de C^*, de C.

Veamos que componiendo T con el automorfismo inducido por cierto automorfismo de C, podemos suponer que T' es el morfismo identidad. Salvo dos (a lo más), las únicas subvariedades lineales de codimensión 2 de $\mathbb{P}(H^0(C, w_C)))$ contenidas en C^* son los haces de hiperplanos que pasan por las tangentes de C, porque si todos los hiperplanos de que pasan por tres rectas (no tangentes a C) son tangentes a C entonces proyectando C convenientemente a $\mathbb{P}^3$, tendremos que cada tangente a C en cada punto $p \in C$ pertenecen a los tres planos que pasan por tres rectas fijadas y el punto p, lo cual es imposible. Por tanto, la proyectividad dual de T', T'^*, transforma rectas tangentes a C en rectas tangentes a C. Componiendo T con el automorfismo inducido por un automorfismo de la curva, podemos suponer que T'^* deja estable cada recta tangente a C. Luego deja fijo un punto en cada recta tangente. Veamos ya que T' es el morfismo identidad. Proyectando la curva a un hiperplano desde punto fijo p, T'^* induce una proyectividad sobre dicho hiperplano que, por inducción sobre la dimensión, podemos afirmar que es la identidad. En conclusión, podemos afirmar que T'^* deja estable cada recta del haz de rectas que pasa por p. Con todo ya es fácil concluir que $T'^* = \mathrm{Id}$, luego $T' = \mathrm{Id}$.

T sobre W_{g-1} es la identidad o $*$: En efecto, T ha de dejar estable las fibras $K^{-1}(H_q) = W_q \cup W_q^*$. Por continuidad y conexión $T(W_q) = W_q$ para todo q o $T(W_q) = W_q^*$ para todo q. Componiendo con $*$ si es necesario, podemos suponer que $T(W_q) = W_q$ y $T(W_q^*) = W_q^*$ para todo q. Ahora bien, $W_q^* = q + S^{g-2}C$ y sobre un abierto denso de puntos $p = p_1 + \ldots + p_{g-1} \in S^{g-1}C - G^1_{g-1} = W_{g-1} - W^1_{g-1}$, tenemos que $p = \cap_{i=1}^{g-1}(p_i + S^{g-2}C)$, luego T es la identidad en ese abierto, luego en W_{g-1}.

En conclusión podemos suponer que T es la identidad sobre W_{g-1}. Dado $p_0 \in C$, podemos considerar J_C^{g-1} como una variedad abeliana de origen el haz de línea asociado a $(g-1)p_0$, que pertenece a W_{g-1}. Por la teoría de variedades abelianas todo automorfismo de una variedad abeliana que deje fijo el origen es un automorfismo de grupos, luego T lo es. Nos falta probar que W_{g-1} "genera" J_C^{g-1}. Denotaré a un divisor y su haz de línea asociado igual. El morfismo suma $W_{g-1} \times W_{g-1} \to J_C^{g-1}, (D, D') \mapsto D + D' - (g-1)p_0$ es obviamente epiyectivo.

□

Capítulo 20

Degeneración de Hodge y Teorema de Anulación

20.1. Introducción

Sea $\mathscr{X}$ una variedad compleja de dimensión n, denotemos $\Omega^p_{\mathscr{X}}$ el haz de p-formas holomorfas sobre $\mathscr{X}$ y $\mathrm{d}\colon \Omega^p_{\mathscr{X}} \to \Omega^{p+1}_{\mathscr{X}}$ la diferencial exterior. El lema de Poincaré holomorfo afirma que la sucesión de haces

$$0 \to \mathbb{C} \hookrightarrow \mathscr{O}_{\mathscr{X}} \xrightarrow{\mathrm{d}} \Omega^1_{\mathscr{X}} \xrightarrow{\mathrm{d}} \Omega^2_{\mathscr{X}} \xrightarrow{\mathrm{d}} \cdots \xrightarrow{\mathrm{d}} \Omega^n_{\mathscr{X}} \to 0$$

es exacta. En otras palabras, el complejo de De Rham $\Omega^{\cdot}_{\mathscr{X}}$ es una resolución del haz constante $\mathbb{C}$. Por tanto, por el teorema de De Rham

$$H^i(\mathscr{X},\mathbb{C}) = \mathbb{H}^i(\mathscr{X},\Omega^{\cdot}_{\mathscr{X}})$$

donde el segundo miembro es el i-ésimo grupo de hipercohomología de $\mathscr{X}$ con valores en $\Omega^{\cdot}_{\mathscr{X}}$. Por otra parte, se tiene la sucesión espectral convergente de hipercohomología

$$E_1^{p,q} = H^p(\mathscr{X},\Omega^q_{\mathscr{X}}) \Rightarrow \mathbb{H}^{p+q}(\mathscr{X},\Omega^{\cdot}_{\mathscr{X}}) \tag{1}$$

denominada *sucesión espectral de Hodge a De Rham*. Si suponemos además $\mathscr{X}$ *compacta*, entonces por el teorema de finitud de Cartan-Serre los términos de la sucesión espectral son espacios vectoriales de dimensión finita. Si denotamos

$$b_i = \dim \mathbb{H}^i(\mathscr{X},\Omega^{\cdot}_{\mathscr{X}}) = \dim H^i(\mathscr{X},\mathbb{C})$$

(i-ésimo número de Betti de $\mathscr{X}$) y

$$h^{pq} = \dim H^p(\mathscr{X}, \Omega^q_{\mathscr{X}})$$

(número de Hodge), se tiene entonces

$$b_i \leq \sum_{p+q=i} h^{pq}$$

y se da la igualdad (para todo i) si y sólo si la sucesión espectral degenera en E_1. Supongamos además $\mathscr{X}$ *kähleriana*. Entonces el teorema de descomposición de Hodge afirma que

$$H^i(\mathscr{X}, \mathbb{C}) \simeq \bigoplus_{p+q=i} H^p(\mathscr{X}, \Omega^q_{\mathscr{X}})$$

(*descomposición de Hodge*) lo que equivale a decir que la sucesión espectral degenera en E_1. Estos resultados se aplican notablemente al caso en que $\mathscr{X}$ es la variedad analítica compleja asociada a un esquema liso y proyectivo X sobre $\mathbb{C}$. En este caso, la degeneración de Hodge se puede formular en términos puramente algebraicos. El complejo de De Rham $\Omega^{\cdot}_{\mathscr{X}}$ es el complejo de haces analíticos asociado al complejo de De Rham algebraico $\Omega^{\cdot}_X$ de X sobre $\mathbb{C}$. El morfismo canónico de espacios anillados $\mathscr{X} \to X$ induce homomorfismos

$$\begin{aligned} H^p(X, \Omega^q_X) &\to H^p(\mathscr{X}, \Omega^q_{\mathscr{X}}) \\ \mathbb{H}^i(X, \Omega^{\cdot}_X) &\to \mathbb{H}^i(\mathscr{X}, \Omega^{\cdot}_{\mathscr{X}}) \end{aligned} \tag{2}$$

Además se tiene una sucesión espectral de Hodge a De Rham algebraica

$$E_1^{p,q} = H^p(X, \Omega^q_X) \Rightarrow \mathbb{H}^{p+q}(X, \Omega^{\cdot}_X) \tag{3}$$

y un morfismo de (3) a (1) que induce los morfismos de (2) entre los términos iniciales y finales de las sucesiones espectrales. Por el teorema de comparación de Serre (GAGA), los morfismos de (2) son isomorfismos. Por tanto, la degeneración en E_1 de (1) equivale a la de (3); en otras palabras, si denotamos

$$h^{pq}(X) = \dim H^p(X, \Omega^q_X), \qquad b_i(X) = \dim \mathbb{H}^i(X, \Omega^{\cdot}_X)$$

el teorema de degeneración de Hodge para $\mathscr{X}$ se puede expresar por las relaciones puramente algebraicas

$$b_i(X) = \sum_{p+q=i} h^{pq}(X)$$

Más generalmente, si X es un esquema propio y liso sobre un cuerpo k, se puede considerar el complejo de De Rham $\Omega^{\cdot}_{X/k}$ de X sobre k, y se tiene una sucesión espectral de Hodge a De Rham

$$E_1^{p,q} = H^p(X, \Omega^q_{X/k}) \Rightarrow \mathbb{H}^{p+q}(X, \Omega^{\cdot}_{X/k}) \tag{4}$$

de k-espacios vectoriales de dimensión finita. Si k es de característica cero, el teorema de degeneración de Hodge implica la degeneración de (4) en E_1 (de modo estándar se reduce al caso $k = \mathbb{C}$, y por el lema de Chow y la resolución de singularidades se reduce al caso proyectivo). El objetivo de esta lección es ver una demostración puramente algebraica de la degeneración de (4) para k de característica nula. Veremos que la degeneración de (4) se prueba por reducción al caso en que k es de característica positiva (¡donde el teorema de degeneración es falso!), con ciertas hipótesis suplementarias (mayoración de la dimensión, relevabilidad). El núcleo central de la lección es la estructura del complejo de De Rham de un esquema liso sobre un cuerpo de característica positiva: isomorfismo de Cartier, teoremas de degeneración y de anulación. A partir de ella, se verá cómo la técnica estándar de pasar de la característica p a la característica nula permite probar los teoremas de degeneración de Hodge y de anulación de Kodaira-Akizuki-Nakano a partir de sus análogos en característica p.

20.2. Frobenius e isomorfismo de Cartier

Sea X un esquema sobre un cuerpo perfecto k de característica $p > 0$. El *endomorfismo de Frobenius* de X es el endomorfismo de X

$$F : X \to X$$

que es la identidad sobre el espacio topológico subyacente y la elevación a p sobre $\mathcal{O}_X$. Si $X = \operatorname{Spec} A$ es afín, F se corresponde con el morfismo de anillos $A \to A$, $a \mapsto a^p$.

Si f es una sección local de $\mathcal{O}_X$, entonces $\mathrm{d}f^p = pf^{p-1}\mathrm{d}f = 0$. Por tanto, la diferencial del complejo $F_*\Omega^{\cdot}_{X/k}$ (véase el problema **??** del capítulo 2) es $\mathcal{O}_X$-lineal y los haces de cohomología $\mathscr{H}^i F_*\Omega^{\cdot}_{X/k}$ son $\mathcal{O}_X$-módulos. En particular !localizan!. Esta es la diferencia esencial con la característica nula. El producto exterior dota al $\mathcal{O}_X$-módulo graduado $\bigoplus_{i\geq 0} \mathscr{H}^i F_*\Omega^{\cdot}_{X/k}$ de estructura de álgebra graduada y anticonmutativa.

1. Lema: $H^1(\Omega^{\cdot}_{k[t]/k}) = k[t^p] \cdot t^{p-1}\mathrm{d}t$.

2. Teorema (Isomorfismo de Cartier): *Existe un único morfismo de $\mathcal{O}_X$-álgebras graduadas*

$$\gamma\colon \bigoplus_i \Omega^i_{X/k} \to \bigoplus_i \mathscr{H}^i F_*\Omega^{\cdot}_{X/k}$$

tal que:

(i) para $i=0$, es el morfismo de Frobenius $F^*\colon \mathscr{O}_X \to F_*\mathscr{O}_X$.

(ii) para $i=1$, transforma $\mathrm{d}f$ en la clase de $f^{p-1}\mathrm{d}f$.

Si además X es liso sobre k, entonces γ es isomorfismo.

Demostración. En grado 1, el morfismo $\Omega^1_{X/k} \to \mathscr{H}^1 F_*\Omega^{\cdot}_{X/k}$ se corresponde con la derivación $f \mapsto f^{p-1}\mathrm{d}f$ (la suma va a la suma módulo una diferencial exacta[1]). Como γ debe ser morfismo de álgebras, (i) y (ii) lo determinan. Veamos que γ es isomorfismo cuando X es liso. Por cambio de cuerpo base podemos suponer que k es algebraicamente cerrado. Como la cuestión es local, podemos suponer que X es afín y existe un morfismo inyectivo $k[x_1,\dots,x_n] \hookrightarrow \mathscr{O}_X$ de modo que $\Omega_{X/k} = \Omega_{\mathbb{A}^n/k} \otimes_{\mathscr{O}_{\mathbb{A}^n}} \mathscr{O}_X$. Luego, el morfismo $k[x_1,\dots,x_n] \hookrightarrow \mathscr{O}_X$ es isomorfismo por compleciones y es plano. Por tanto basta probar el isomorfismo de Cartier para $\mathbb{A}^n_k$, y por Künneth, basta probarlo para $\mathbb{A}^1_k$. □

20.3. Teoremas de degeneración y de anulación

Vamos a ver ahora que el isomorfismo de Cartier es el morfismo inducido en cohomología por un morfismo entre complejos, si suponemos que $X \xrightarrow{F} X$ levanta a $W_2(k) =$ anillo de vectores de Witt de longitud 2. En esta sección X es un esquema liso sobre un cuerpo perfecto k de característica $p>0$.

Como k es un cuerpo de característica p, es una extensión de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Existe un (único) anillo W, plano sobre $\mathbb{Z}/p^2\mathbb{Z}$, tal que $W/pW = k$. Este anillo se denomina anillo de vectores de Witt de longitud 2 sobre k y se denota $W_2(k)$. Se construye como el conjunto de parejas $(a_1,a_2) \in k\times k$ con la siguiente suma y producto

$$(a_1,a_2)+(b_1,b_2) = (a_1+b_1, S_2(a,b))$$
$$(a_1,a_2)\cdot(b_1,b_2) = (a_1b_1, P_2(a,b))$$

con $S_2(a,b) = a_2+b_2+p^{-1}(a_1^p+b_1^p-(a_1+b_1)^p)$ y $P_2(a,b) = b_1^p a_2 + b_2 a_1^p$. De ahora en adelante denotaremos $W = W_2(k)$. Todo automorfismo τ de k levanta a un automorfismo τ_W de W, sin más que operar por τ en ambas componentes de $W = k\times k$. Además, la especialización de τ_W a $k = W/pW$ es el automorfismo τ. En particular, el automorfismo de Frobenius de k induce un automorfismo de W que también denominaremos automorfismo de Frobenius de W y denotaremos F_W.

[1] $(x+y)^p = x^p+y^p+p\cdot h(x,y)$, luego $p\cdot(x+y)^{p-1}d(x+y) = p\cdot(x^{p-1}dx+y^{p-1}dy+dh(x,y))$ y por tanto $(x+y)^{p-1}d(x+y) = x^{p-1}dx+y^{p-1}dy+dh(x,y)$ en $\Omega_{\mathbb{Z}[x,y]/\mathbb{Z}}$

1. Definición: Diremos que un k-esquema liso X *levanta* a W, si existe un esquema Z liso sobre W tal que $\mathcal{O}_Z/p\mathcal{O}_Z \simeq \mathcal{O}_X$. Se dice entonces que Z es un levantamiento de X a W, y se tiene un diagrama cartesiano

$$\begin{array}{ccc} X & \longrightarrow & Z \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & \operatorname{Spec} W \end{array}$$

Análogamente, diremos que $X \xrightarrow{F} X$ levanta a W si existe un levantamiento Z de X a W y un endomorfismo $G\colon Z \to Z$, compatible con el automorfismo de Frobenius de W, y que coincide con F al especializar a X.

Denotaremos $(\Omega^{\cdot}_{X/k}, \mathrm{d}_0)$ al complejo cuyo objeto i-ésimo es $\Omega^i_{X/k}$ y cuya diferencial es **nula**. También escribiremos $(\Omega^{\cdot}_{X/k}, \mathrm{d}_0) = \bigoplus_i \Omega^i_{X/k}[-i]$.

2. Teorema (Deligne-Illusie): *Si $X \xrightarrow{F} X$ admite un levantamiento a W, $G\colon Z \to Z$, entonces hay un morfismo de complejos*

$$\varphi_G : (\Omega^{\cdot}_{X/k}, \mathrm{d}_0) \to F_* \Omega^{\cdot}_{X/k}$$

que induce en cohomología el isomorfismo de Cartier.

Demostración. Definamos $\varphi^1_G : \Omega^1_{X/k} \to F_* \Omega^1_{X/k}$. El endomorfismo G induce un morfismo en las diferenciales

$$G^* : \Omega^1_{Z/W} \to G_* \Omega^1_{Z/W}$$

que coincide con F^* al hacer módulo p. Pero F^* es nulo en las diferenciales, luego G^* valora en $pG_*\Omega^1_{Z/W} \simeq F_*\Omega^1_{X/k}$ [2] y se anula sobre $p\,\Omega^1_{Z/W}$, luego induce un morfismo $\varphi^1_G : \Omega^1_{X/k} \to F_*\Omega^1_{X/k}$. Calculemos φ^1_G localmente.

Si $\overline{f}$ es una sección local de $\mathcal{O}_X$ y f una sección local de $\mathcal{O}_Z$ que la represente, entonces $G^*(f) = f^p + pb$, para alguna sección local b de $\mathcal{O}_X$, pues G levanta a F. Por tanto, $G^*(\mathrm{d}f) = p(f^{p-1}\,\mathrm{d}f + \mathrm{d}b) = p(\overline{f}^{p-1}\,\mathrm{d}\overline{f} + \mathrm{d}b)$, luego

$$\varphi^1_G(\mathrm{d}\overline{f}) = \overline{f}^{p-1}\,\mathrm{d}\overline{f} + \mathrm{d}b$$

y por tanto φ^1_G coincide con γ^1 al pasar a cohomología. Definiendo $\varphi^i_G = \Lambda^i \varphi^1_G$, se concluye la demostración. □

[2] La sucesión exacta $0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p\cdot} \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ implica, por cambio de base plano $\mathbb{Z}/p^2\mathbb{Z} \to \mathcal{O}_Z$, que $p\mathcal{O}_Z \simeq \mathcal{O}_X$ y en general, para todo $\mathcal{O}_Z$-módulo plano M, $pM \simeq M/pM$.

3. Observación: Si $G_1, G_2 : Z \to Z$ son dos levantamientos de F, entonces existe un morfismo $h_{12} : \Omega^1_{X/k} \to F_* \mathcal{O}_X$ tal que

$$\varphi^1_{G_2} - \varphi^1_{G_1} = \mathrm{d} \circ h_{12}$$

En efecto, $(G_2^* - G_1^*)(f) = p \cdot b$, para alguna sección b de $\mathcal{O}_X$. Teniendo en cuenta que $p\mathcal{O}_Z \simeq \mathcal{O}_X$, puede entenderse $(G_2^* - G_1^*)(f)$ como una sección de $F_* \mathcal{O}_X$. Se comprueba fácilmente que $f \mapsto (G_2^* - G_1^*)(f)$ es una derivación de $\mathcal{O}_Z$ en $F_* \mathcal{O}_X$.

Ahora vamos a ver como repetir el teorema anterior pero sin suponer que $X \xrightarrow{F} X$ levanta a W, sino solamente que X levanta a W. Lo que haremos es levantar localmente el endomorfismo de Frobenius, gracias a la lisitud del levantamiento de X, y sustituir el complejo $F_* \Omega^{\cdot}_{X/k}$ por su resolución Cech. Si $\mathfrak{U} = \{U_i\}$ es un recubrimiento afín de X y $M^{\cdot}$ es un complejo inferiormente acotado de $\mathcal{O}_X$-módulos coherentes, denotaremos $\mathrm{Cech}(\mathfrak{U}, M^{\cdot})$ al complejo simple asociado al bicomplejo $\mathrm{Cech}^p(\mathfrak{U}, M^q)$. Se tiene un cuasi-isomorfismo $M^{\cdot} \to \mathrm{Cech}(\mathfrak{U}, M^{\cdot})$.

4. Teorema (Deligne-Illusie): *Sea k un cuerpo de característica $p > 0$ y X un esquema liso sobre k. Si X levanta a W, entonces existe un recubrimiento afín $\mathfrak{U} = \{U_i\}$ de X y un morfismo de complejos*

$$\varphi_Z : \bigoplus_{i<p} \Omega^i_{X/k}[-i] \longrightarrow \mathrm{Cech}(\mathfrak{U}, F_* \Omega^{\cdot}_{X/k}) \xleftarrow{cuasi} F_* \Omega^{\cdot}_{X/k}$$

que induce en cohomología el isomorfismo de Cartier (para $i < p$).

Demostración. Sea $Z \xrightarrow{\pi} W$ un levantamiento de X. Construyamos un morfismo

$$\varphi^1_Z : \Omega^1_{X/k}[-1] \to \mathrm{Cech}(\mathfrak{U}, F_* \Omega^{\cdot}_{X/k})$$

Denotemos por $i : X \hookrightarrow Z$ la inmersión cerrada y F_W el automorfismo de Frobenius de W (20.3) . Se tiene un diagrama conmutativo

$$\begin{array}{ccc} X & \xrightarrow{i \circ F} & Z \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \pi} \\ Z & \xrightarrow{F_W \circ \pi} & W \end{array}$$

Por ser $Z \xrightarrow{\pi} W$ liso, existe localmente un morfismo $Z \to Z$ que añadido al diagrama conmutativo anterior hace los triángulos conmutativos. Es decir, el endomorfismo de Frobenius $F : X \to X$ levanta, localmente en Z, a un endomorfismo de Z. Por tanto, existe un recubrimiento $\mathfrak{U} = \{U_i\}$ de X (y también de Z, pues tiene el mismo espacio subyacente) y endomorfismos $G_i : Z_i \to Z_i$ que levantan a $F_{|U_i}$ (donde hemos denotado

Z_i a U_i pensado como abierto de Z). Por la observación anterior, para cada pareja i,j existe $h_{ij}\colon \Omega^1_{U_i\cap U_j} \to F_*\mathscr{O}_{U_i\cap U_j}$ tal que $\varphi^1_{G_j} - \varphi^1_{G_i} = \mathrm{d}\circ h_{ij}$. Es fácil comprobar que $h_{ij}+h_{jk}=h_{ik}$. Definimos entonces

$$\begin{aligned}\Omega^1_{X/k} &\longrightarrow \mathrm{Cech}^1(\mathfrak{U},F_*\Omega^{\cdot}_{X/k}) = \mathrm{Cech}^0(\mathfrak{U},F_*\Omega^1_{X/k}) \oplus \mathrm{Cech}^1(\mathfrak{U},F_*\mathscr{O}_X)\\ \omega &\longmapsto \quad (\varphi^1_{G_i}(\omega_{|U_i}), h_{ij}(\omega_{|U_i\cap U_j}))\end{aligned}$$

luego tenemos un morfismo de complejos $\Omega^1_{X/k}[-1] \to \mathrm{Cech}(\mathfrak{U},F_*\Omega^{\cdot}_{X/k})$. Ahora, para $i<p$ el morfismo de hemisimetrización $\Omega^i_{X/k} \to \Omega^{\otimes i}_{X/k}$ está bien definido, luego tenemos un morfismo

$$\Omega^i_{X/k}[-i] \to \Omega^{\otimes i}_{X/k}[-i] \to \mathrm{Cech}(\mathfrak{U},F_*\Omega^{\cdot}_{X/k})^{\otimes i}$$

Ahora, para todo abierto afín U y para cualesquiera módulos coherentes $\mathscr{M}$ y $\mathscr{N}$ se verifica $\Gamma(U,\mathscr{M})\otimes\Gamma(U,\mathscr{N}) = \Gamma(U,\mathscr{M}\otimes\mathscr{N})$, lo cual induce una igualdad de complejos

$$\mathrm{Cech}(\mathfrak{U},F_*\Omega^{\cdot}_{X/k})^{\otimes i} = \mathrm{Cech}(\mathfrak{U},(F_*\Omega^{\cdot}_{X/k})^{\otimes i})$$

Finalmente, el producto exterior define un morfismo de complejos

$$\begin{aligned}(F_*\Omega^{\cdot}_{X/k})^{\otimes i} &\xrightarrow{\wedge} F_*\Omega^{\cdot}_{X/k}\\ \theta_1\otimes\cdots\otimes\theta_i &\to \theta_1\wedge\cdots\wedge\theta_i\end{aligned}$$

y por tanto un morfismo de complejos $\mathrm{Cech}(\mathfrak{U},(F_*\Omega^{\cdot}_{X/k})^{\otimes i}) \xrightarrow{\wedge} \mathrm{Cech}(\mathfrak{U},F_*\Omega^{\cdot}_{X/k})$. Juntando todo se obtiene un morfismo $\Omega^i_{X/k}[-i] \to \mathrm{Cech}(\mathfrak{U},F_*\Omega^{\cdot}_{X/k})$, y se comprueba que coincide en cohomología con el isomorfismo de Cartier. □

5. Corolario: *En las hipótesis del teorema, se verifica*

$$\mathbb{H}^i(X,\Omega^{\cdot}_{X/k}) = \bigoplus_{p+q=i} H^p(X,\Omega^q_{X/k})$$

para todo $i<p$.

Demostración.

$$\bigoplus_{p+q=i} H^p(X,\Omega^q_{X/k}) = \mathbb{H}^i(X,\bigoplus_k \Omega^k_{X/k}[-k]) \overset{i<p}{=\!=} \mathbb{H}^i(X,F_*\Omega^{\cdot}_{X/k}) = \mathbb{H}^i(X,\Omega^{\cdot}_{X/k})$$

□

6. Corolario (Teorema de anulación, Raynaud): *Sea X un esquema liso y proyectivo sobre un cuerpo perfecto de característica p, y $\mathscr{L}$ un haz de línea amplio sobre X. Si X es de dimensión $n<p$ y levanta a W, entonces*

a) $H^j(X,\Omega^i_{X/k}\otimes\mathscr{L})=0$, *para* $i+j>n$.

b) $H^j(X,\Omega^i_{X/k}\otimes\mathscr{L}^{-1})=0$, *para* $i+j<n$.

Demostración. Por dualidad a) y b) son equivalentes. Probemos b). Por el teorema de Serre, existe $k>>0$ tal que $H^j(X,\Omega^i_{X/k}\otimes\mathscr{L}^{p^k})=0$ para todo $j>0$ y todo i; por dualidad, $H^j(X,\Omega^i_{X/k}\otimes\mathscr{L}^{-p^k})=0$ para todo $j<n$ y todo i, en particular para todo $i+j<n$. Por recurrencia, basta probar el siguiente enunciado: si M es un haz de línea en X tal que $H^j(X,\Omega^i_{X/k}\otimes M^p)=0$ para todo $i+j<n$, entonces $H^j(X,\Omega^i_{X/k}\otimes M)=0$ para todo $i+j<n$. Ahora bien, $M^p=F^*M$, luego $(F_*\Omega^i_{X/k})\otimes M=F_*(\Omega^i_{X/k}\otimes M^p)$.

$$\bigoplus_{i+j=r}H^i(X,\Omega^j_{X/k}\otimes\mathscr{M})=\mathbb{H}^r(X,\bigoplus_k\Omega^k_{X/k}[-k]\otimes\mathscr{M})\overset{r\leq p}{=\!=}\mathbb{H}^r(X,F_*\Omega^{\cdot}_{X/k}\otimes\mathscr{M})$$
$$=\mathbb{H}^r(X,F_*(\Omega^{\cdot}_{X/k}\otimes\mathscr{M}^p))=\mathbb{H}^r(X,\Omega^{\cdot}_{X/k}\otimes\mathscr{M}^p)\overset{r\leq n}{=}H^r[\Gamma(X,\Omega^{\cdot}_{X/k}\otimes\mathscr{M}^p)]=H^r(0)=0$$

□

20.3.1. De la característica p a la característica 0

Veamos ahora cómo se pueden obtener la degeneración de Hodge y los teoremas de anulación de Kodaira-Akizuki-Nakano en característica cero a partir de los resultados probados en característica p, mediante la técnica estándar expuesta en E.G.A. IV, 8.

Obviamente, todo anillo es límite inductivo de sus $\mathbb{Z}$-subálgebras de tipo finito. Sea $A=k[x_1,\ldots,x_n]/I$, con $I=(p_1,\ldots,p_r)$. Sea $\mathbb{Z}_\alpha$ una $\mathbb{Z}$-subálgebra de k de tipo finito que contenga los coeficientes de los polinomios p_i. Si definimos $A_\alpha=\mathbb{Z}_\alpha[x_1,\ldots,x_n]/I_\alpha$, con $I_\alpha=(p_1,\ldots,p_r)$, tenemos que $A=A_\alpha\otimes_{\mathbb{Z}_\alpha}k$. Como k es plano sobre $\mathbb{Z}_\alpha$, tenemos que A_α se inyecta en A. Localizando $\mathbb{Z}_\alpha$ por una función conveniente podemos suponer, por 7.7.12, que A_α es una $\mathbb{Z}_\alpha$-álgebra plana.

Supongamos ahora que A es una k-álgebra lisa, es decir, $\Omega_{A/k}$ es un A-módulo localmente libre y se verifica la sucesión exacta (denotando $B=k[x_1,\ldots,x_n]$)

$$0\to I/I^2\to\Omega_{B/k}\otimes_B A\to\Omega_{A/k}\to 0$$

La condición necesaria y suficiente para que un A-módulo M sea localmente libre de rango r, es que los ideales de Fitting $F^A_{r-1}(M)=0$ y $F^A_r(M)=A$. Como los ideales de Fitting cambian de base, es fácil probar que, ampliando $\mathbb{Z}_\alpha$ por un número finito de elementos de k, podemos suponer que I_α/I_α^2 y $\Omega_{A_\alpha/\mathbb{Z}_\alpha}$ son A_α-módulos localmente libres cuya suma de rangos es n, porque así lo verifica I/I^2 y $\Omega_{A/k}$. Por tanto, $\Omega_{A_\alpha/\mathbb{Z}_\alpha}$ es un A_α-módulo localmente libre y se verifica la sucesión exacta (denotando $B_\alpha=\mathbb{Z}_\alpha[x_1,\ldots,x_n]$)

$$0\to I_\alpha/I_\alpha^2\to\Omega_{B_\alpha/\mathbb{Z}_\alpha}\otimes_{B_\alpha}A_\alpha\to\Omega_{A_\alpha/\mathbb{Z}_\alpha}\to 0$$

En conclusión, podemos suponer que A_α es una $\mathbb{Z}_\alpha$-álgebra lisa.

Si $X \to \operatorname{Spec} k$ es una variedad algebraica lisa, considerando un recubrimiento de X por abiertos afines, es fácil probar que existe una $\mathbb{Z}$-subálgebra $\mathbb{Z}_\alpha \hookrightarrow k$ de tipo finito y un morfismo liso de tipo finito $X_\alpha \to \operatorname{Spec}\mathbb{Z}_\alpha$, de modo que $X = X_\alpha \times_{\mathbb{Z}_\alpha} k$.

Si $X \to \operatorname{Spec} k$ es proyectivo, podemos suponer que $X_\alpha \to \operatorname{Spec}\mathbb{Z}_\alpha$ es proyectivo. Usando el lema de Chow, el lector puede probar que si $X \to \operatorname{Spec} k$ es propio, entonces puede suponerse que $X_\alpha \to \operatorname{Spec}\mathbb{Z}_\alpha$ es propio.

7. Teorema (Degeneración de Hodge): *Sea K un cuerpo de característica cero y X un K-esquema propio y liso. Entonces la sucesión espectral de Hodge a De Rham*

$$E_1^{pq} = H^p(X, \Omega^q_{X/K}) \Rightarrow \mathbb{H}^{p+q}(X, \Omega^\cdot_{X/K})$$

degenera en E_1.

Demostración. Sea $h^{pq} = \dim_K H^p(X, \Omega^q_{X/K})$, $b_i = \dim_K \mathbb{H}^i(X, \Omega^\cdot_{X/K})$. En las sucesiones espectrales las dimensiones de los sucesivos términos de la sucesión van disminuyendo estrictamente, pues de un término al siguiente se pasa tomando homología, si no es así es que la diferencial considerada es nula. Hay que probar que $b_i = \sum_{p+q=i} h^{pq}$.

Existe una $\mathbb{Z}$-subálgebra $\mathbb{Z}_\alpha \hookrightarrow k$ de tipo finito y un morfismo $X_\alpha \to \operatorname{Spec}\mathbb{Z}_\alpha$ propio y liso, tal que $X = X_\alpha \underset{S_\alpha}{\times} \operatorname{Spec} K$, siendo $S_\alpha = \operatorname{Spec}\mathbb{Z}_\alpha$. Sustituyendo $\mathbb{Z}_\alpha$ por $\mathbb{Z}_\alpha[1/t]$, con $t \in \mathbb{Z}_\alpha$, podemos suponer que S_α es liso sobre $\mathbb{Z}$ (pues el conjunto de puntos lisos es un abierto no vacío). Denotemos $S = S_\alpha$, $\mathscr{X} = X_\alpha$ y $f : \mathscr{X} \to S$ el morfismo estructural. Reemplazando $\mathbb{Z}_\alpha$ por $\mathbb{Z}_\alpha[1/t]$ podemos suponer que los haces $R^p f_* \Omega^q_{\mathscr{X}/S}$, $\mathbb{R}^i f_* \Omega^\cdot_{\mathscr{X}/S}$ son localmente libres (y de rangos h^{pq}, b_i respectivamente, por el teorema de cambio de base). Sea n un entero mayor que la dimensión de las fibras de $\mathscr{X}$ sobre S y sea $s \in S$ un punto cerrado cuyo cuerpo residual k es de característica $p > n$ (que existe por ser S de tipo finito sobre $\mathbb{Z}$). Como $S \to \operatorname{Spec}\mathbb{Z}$ es liso, el morfismo $\operatorname{Spec} k \to S$ levanta a $g : \operatorname{Spec} W \to S$. Sea Y la fibra de s en $\mathscr{X}$ e Y_1 la fibra de g. Se tienen diagramas cartesianos

$$\begin{array}{ccccccc}
Y & \longrightarrow & Y_1 & \longrightarrow & \mathscr{X} & \longleftarrow & X \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
s & \longrightarrow & \operatorname{Spec} W & \xrightarrow{g} & S & \longleftarrow & \operatorname{Spec} K
\end{array}$$

y por construcción Y es propio y liso sobre k, de dimensión menor que p y levanta a W, luego

$$\sum_{p+q=i} h^{pq} = \sum_{p+q=i} \dim_k H^p(Y, \Omega^q_{Y/k}) = \dim_k \mathbb{H}^i(Y, \Omega^\cdot_{Y/k}) = b_i$$

donde la primera y última igualdad son por el teorema de Grauert. □

8. Teorema (de anulación de Kodaira-Akizuki-Nakano): *Sea K un cuerpo de característica cero, X un K-esquema proyectivo y liso de dimensión n y L un haz de línea amplio en X. Entonces*

a) $H^j(X, \Omega^i_{X/K} \otimes L) = 0$, *para* $i + j > n$.

b) $H^j(X, \Omega^i_{X/K} \otimes L^{-1}) = 0$, *para* $i + j < n$.

Demostración. Como antes, existe un subanillo $\mathbb{Z}_\alpha \subset K$ de tipo finito y liso sobre $\mathbb{Z}$ y un morfismo proyectivo y liso $f\colon \mathscr{X} \to S = \operatorname{Spec} \mathbb{Z}_\alpha$, de dimensión relativa n, tal que $\mathscr{X} \underset{S}{\otimes} \operatorname{Spec} K = X$, y un haz de línea amplio $\mathscr{L}$ en $\mathscr{X}$ que cambiado de base a X da L. Reemplazando $\mathbb{Z}_\alpha$ por $\mathbb{Z}_\alpha[1/t]$, se puede suponer que los haces $R^p f_*(\Omega^q_{\mathscr{X}/S} \otimes M)$ (con $M = \mathscr{L}, \mathscr{L}^{-1}$) son libres de tipo finito y de rango $\dim_K H^p(X, \Omega^q_{X/K} \otimes M_X)$ (con $M_X = L, L^{-1}$). Elegimos $g\colon \operatorname{Spec} W \to S$ como en la demostración anterior y seguimos sus mismas notaciones. El haz $\mathscr{L}_s$ = imagen inversa de $\mathscr{L}$ sobre $Y = \mathscr{X}_s$ es amplio, luego $\dim_K H^p(Y, \Omega^q_{Y/K} \otimes \mathscr{L}_s) = 0$ para $p + q > n$ y $\dim_K H^p(Y, \Omega^q_{Y/K} \otimes \mathscr{L}_s^{-1}) = 0$ para $p + q < n$. Se concluye. □

Bibliografía

[1] ARTIN, E.: *Teoría de Galois*, Colección de Matemáticas Nuevo Límite, Vicens-Vives, España, 1970, traducción y prólogo de R. Rodríguez Vidal.

[2] ATIYAH, M.F. AND MACDONALD, I.G.: *Introduction to commutative algebra*, Reading Mass., Addison-Wesley Publishing Company, Massachusetts, 1969.

[3] BERTIN, J.; DEMAILLY, J.P.; ILLUSIE, L:; PETERS, C.: *Introduction à la Théorie de Hodge*, Panoramas et Synthèses, **3**, Soc. Math. de France, 1996.

[4] BOURBAKI, N.: *Algèbre*, Elements de Mathematique, Masson, Paris, 1981.

[5] CARTAN, H., EILENBERG, S.: *Homological Algebra*, Princeton Univ. Press, 1956.

[6] CIOCAN-FONTANINE, I.; KAPRANOV, M: *Derived Hilbert schemes.* J. Amer. Math. Soc. 15 (2002), 787-815.

[7] DELIGNE, P.; ILLUSIE, L.: *Relèvements modulo p^2 et décomposition du complex de De Rham*, Inv. Math., **89** (1987), 247-270.

[8] FULTON, W.: *Algebraic Curves*, W.A. Benjamin, New York, 1969.

[9] GAAL, L.: *Classical Galois Theory*, Chelsea Publishing Company, NY, 1973.

[10] GODEMENT, R. *Topologie Algébrique et Théorie des Faiseaux*, Hermenn, Paris, 1958.

[11] GROTHENDIECK, A.: *Fondements de la géométrie algébrique (Extraits du Séminaire Bourbaki*. Springer-Verlag (1957-1962)

[12] GROTHENDIECK, A.; DIEUDONNÉ, J. A.: *Eléments de géométrie algébrique I*. Springer-Verlag (1971)

[13] GROTHENDIECK A.;, DIEUDONNÉ J.: *Eléments de géométrie algébrique IV*, Pub. Math. IHES, Springer-Verlag (1971).

[14] HARTSHORNE, R.:*Algebraic Geometry*, GTM, Vol **52**, Springer-Verlag, New York 1977.

[15] HIRONAKA, H. *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Annals of Math. 29 1975.

[16] KOSTRIKIN, A.I.:*Introducción al algebra*, McGraw-Hill/Interamericana de España, Madrid, 1992.

[17] LANG, S.:*Álgebra*, Aguilar S.A. de ediciones, Madrid, 1971.

[18] MATSUMURA, H.:*Commutative ring theory*. Cambridge University Press (1980)

[19] MILNE, J.S.:*Field and Galois theory*, 2002.

[20] MUMFORD, D.:*Lecture on curves on an algebraic surface*. Annals of Mathematics Studies 59. Princeton University Press (1966).

[21] MUMFORD, D.:*Algebraic Geometry I*, Springer Verlag, 1976.

[22] NAGATA, M.:*Local Rings*, Interscience Tracts, 13, Interscience, 1962

[23] NAVARRO GONZÁLEZ, J.A.:*Teoría de Galois*, Sección de Matemáticas, vol. 5, Universidad de Extremadura, 1984.

[24] NAVARRO GONZÁLEZ, J.A.:*Álgebra conmutativa básica*, Manuales de Unex, vol. 19, Universidad de Extremadura, 1996.

[25] NORTHCOTT, D.G.:*Lessons on rings, modules and multiplicités*, Cambridge University Press, 1968.

[26] PASTOR, R.:*Lecciones de Álgebra*, Nuevas Gráficas, Madrid, 1960.

[27] ROTMAN, J.:*An introduction to homological Algebra*, New York Academic Press, 1979.

[28] SANCHO, F.; SANCHO, P.J.: *Álgebra Conmutativa y Geometría Algebraica II* 2012.

[29] SERRE, J.P.: *Algèbre locale multiplicités*, Lecture Notes in Mathematics, 11, Springer Verlag, 1965.

[30] SHAFAREVICH, I.R.: *Basic Algebraic Geometry*, Grundleheren 213, Springer-Verlag, Heidelberg, 1974.

[31] SPANIER, E.H. *Algebraic Topology*, McGraw-Hill, New York, 1966.

[32] STEWART, I.: *Galois Theory*, Chapman and Hall mathematics series, London 1973.

[33] VAN DER WAERDEN, B.L.:*Algebra*, vol 1,2, Frederik Ungar Publi. Co. New York, 1970.

[34] VIEHWEG, E.: *Quasi-projective Moduli for Polarized Manifolds*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol **30**, Springer-Verlag, Berlin 1995.

[35] ZARISKI, O., SAMUEL, P.: *Commutative Algebra*, vol I,II, Van Nostrand 1958.

Índice alfabético