Álgebra Conmutativa

Geometría Algebraica

Colección manuales uex - 00

(E.E.E.S.)

Carlos Sancho de Salas

Pedro Sancho de Salas

00

ÁLGEBRA CONMUTATIVA
GEOMETRÍA ALGEBRAICA

MANUALES UEX

00

(E.E.E.S.)
Espacio
Europeo
Educación
Superior

CARLOS SANCHO DE SALAS
PEDRO SANCHO DE SALAS

ÁLGEBRA CONMUTATIVA
GEOMETRÍA ALGEBRAICA

UNIVERSIDAD DE EXTREMADURA
2013

CARLOS SANCHO DE SALAS / PEDRO SANCHO DE SALAS

Álgebra Conmutativa. Geometría Algebraica / Carlos Sancho de Salas, Pedro Sancho de Salas. – Cáceres: Universidad de Extremadura, Servicio de Publicaciones, 2013
XXX pp.; 21x29.7 cm (Manuales UEX, ISSN 1135-870-X; 00)
ISBN XXX-XX-XXX-XXXX-X
1. Álgebra, 2. Aritmética. Teoría de los números, 3. Geometría.
I. Sancho de Salas, Pedro. II. Álgebra Conmutativa. Geometría Algebraica
III. Universidad de Extremadura, Servicio de Publicaciones, ed. IV. Manuales UEX
512, 511, 514

UNIVERSIDAD DE EXTREMADURA

UNIÓN EUROPEA
FONDO EUROPEO DE DESARROLLO REGIONAL: UNA MANERA DE HACER EUROPA

GOBIERNO DE EXTREMADURA
Consejería de Empleo, Empresa e Innovación

Edita

Universidad de Extremadura. Servicio de Publicaciones
C./ Caldereros, 2 - Planta 2ª - 10071 Cáceres (España)
Telf. 927 257 041 - Fax 927 257 046
publicac@unex.es
www.unex.es/ publicaciones

ISSN 1135-870-X
ISBN XXX-XX-XXX-XXXX-X
Depósito Legal X-XX.XXX-2013

Índice general

Introducción **9**

0. Grupos, anillos y módulos **11**
0.1. Grupos . . . 11
0.1.1. Grupos cíclicos . . . 15
0.1.2. Grupo simétrico . . . 16
0.1.3. Producto directo y semidirecto de grupos . . . 18
0.1.4. G-conjuntos. Teoremas de Sylow . . . 19
0.2. Anillos . . . 23
0.2.1. Anillos. Dominios de ideales principales . . . 25
0.2.2. Cociente por un ideal . . . 29
0.2.3. Operador de Euler. Polinomios ciclotómicos . . . 30
0.2.4. Ideales primos. Ideales maximales . . . 33
0.2.5. Espectro primo de un anillo . . . 34
0.2.6. Localización. Dominios de factorización única . . . 39
0.2.7. Localización y espectro primo. Fórmula de la fibra . . . 42
0.3. Módulos . . . 46
0.3.1. Módulos, submódulos y cocientes. Sistema de generadores . . . 46
0.3.2. Localización de módulos . . . 49
0.3.3. Anillos y módulos noetherianos . . . 52
0.3.4. Módulos y anillos de longitud finita . . . 55
0.3.5. Clasificación de los módulos sobre dominios de ideales principales . . . 59
0.4. Categorías. Funtor de homomorfismos . . . 65
0.5. Producto tensorial de módulos y álgebras . . . 69
0.5.1. Álgebra tensorial, simétrica y exterior de un módulo . . . 73
0.6. Módulos planos y proyectivos . . . 77
0.7. Ideales de Fitting. Estratos de $Spec\ A$ en los que un A-módulo M es libre . . . 81
0.8. Límites proyectivos e inductivos . . . 85
0.9. Teorema de representabilidad . . . 90
0.10. Problemas . . . 92

1. Raíces de un polinomio **101**
1.1. Extensiones de cuerpos . . . 101
1.1.1. Teorema de Kronecker. Cierre algebraico . . . 101
1.1.2. Grado de trascendencia de una extensión de cuerpos . . . 104
1.1.3. Espectro primo y soluciones de un sistema de ecuaciones algebraicas . . . 105
1.2. Teorema de las funciones simétricas . . . 105
1.3. Teorema fundamental del Álgebra . . . 107
1.4. Fórmulas de Newton y Girard . . . 107
1.5. El discriminante de un polinomio . . . 108
1.6. Teoría de la eliminación: Resultante de dos polinomios . . . 110
1.6.1. Métodos de cómputo de la resultante . . . 113
1.6.2. Aplicaciones de la resultante . . . 115

MANUALES UEX

1.6.3. Ejercicios y ejemplos . . . 117
1.7. Exceso. Polinomios de Sturm. Separación de raíces . . . 118
1.7.1. Acotación de las raíces . . . 118
1.7.2. Exceso de una función racional real . . . 118
1.7.3. Vueltas de una curva alrededor del origen. Teorema de D'Alambert . . . 119
1.7.4. Polinomios de Sturm . . . 121
1.7.5. Teorema de Budan-Fourier. Teorema de Descartes . . . 123
1.8. Problemas . . . 124

2. Teoría de Galois **129**
2.1. Introducción . . . 129
2.2. k-álgebras finitas triviales y racionales . . . 131
2.3. k-álgebras finitas separables. Trivialización. . . . 135
2.3.1. Cuerpos perfectos . . . 137
2.3.2. Subálgebra separable maximal . . . 137
2.3.3. Métrica de la traza . . . 139
2.4. Extensiones de Galois . . . 140
2.4.1. Cuerpos finitos . . . 141
2.5. Teorema de Galois categorial . . . 142
2.6. Resolubilidad de las ecuaciones polinómicas por radicales . . . 145
2.7. Resolución de ecuaciones polinómicas por radicales . . . 150
2.7.1. Grupo de Galois de las cúbicas y las cuárticas . . . 154
2.8. Extensiones por radicales cuadráticos . . . 155
2.8.1. Construcciones con regla y compás . . . 156
2.9. Apéndice: Grupos resolubles . . . 159
2.10. Problemas . . . 164

3. Variedades algebraicas **167**
3.1. Introducción . . . 167
3.2. Descomposición primaria . . . 168
3.2.1. Una descomposición primaria canónica . . . 173
3.3. Morfismos finitos . . . 175
3.4. Teoremas de ascenso y descenso de ideales . . . 177
3.5. Lema de Normalización de Noether. Teorema de los ceros de Hilbert . . . 179
3.6. Teoría de la dimensión en variedades algebraicas . . . 181
3.7. Variedades algebraicas lisas . . . 183
3.7.1. Módulo de las diferenciales de Kähler y módulo de derivaciones . . . 183
3.7.2. Variedades lisas . . . 189
3.7.3. Módulo de diferenciales de una variedad en el punto genérico . . . 191
3.8. Variedades proyectivas . . . 192
3.9. Apéndice: Cálculo tensorial diferencial valorado . . . 195
3.9.1. Derivada de Lie. Fórmula de Cartan . . . 196
3.9.2. Cálculo diferencial valorado. Identidades de Bianchi . . . 198
3.9.3. Módulos de jets y operadores diferenciales . . . 202
3.10. Problemas . . . 206

4. Álgebra local **211**
4.1. Introducción . . . 211
4.2. Teoría de la dimensión local . . . 211
4.2.1. Cono tangente y espacio tangente en un punto . . . 212
4.2.2. Función de Hilbert . . . 213
4.2.3. Teorema de Artin-Rees . . . 214
4.2.4. Dimensión en anillos locales noetherianos . . . 215
4.3. Anillos locales regulares . . . 217
4.4. Compleción . . . 220

4.4.1. Topología I-ádica. Compleción I-ádica . . . 222
4.4.2. Compleción y noetherianidad . . . 224
4.4.3. Teorema de Cohen . . . 225
4.4.4. Lema de Hensel . . . 226
4.5. Problemas . . . 227

5. Anillos de enteros y anillos de curvas 229
5.1. Introducción . . . 229
5.2. Anillos de valoración . . . 229
5.3. Anillos de Dedekind . . . 231
5.4. Desingularización . . . 234
5.4.1. Finitud del morfismo de cierre entero . . . 234
5.4.2. Cierre entero y anillos de valoración . . . 236
5.4.3. Variedad de Riemann . . . 238
5.5. Teoremas fundamentales de la Teoría de Números . . . 240
5.5.1. Valores absolutos arquimedianos . . . 240
5.5.2. Valores absolutos no arquimedianos y valoraciones . . . 242
5.5.3. Producto de valores absolutos de una función . . . 243
5.5.4. Divisores afines . . . 245
5.5.5. Divisores completos . . . 246
5.5.6. Volumen de un paralelepípedo. Discriminante . . . 248
5.5.7. Teorema de Riemann-Roch débil . . . 249
5.5.8. Finitud de la clase de ideales . . . 250
5.5.9. Unidades de un anillo de enteros . . . 252
5.5.10. Número de ideales de norma acotada . . . 254
5.5.11. La función zeta . . . 255
5.6. Explosión a lo largo de un cerrado. Desingularización . . . 258
5.7. Multiplicidad de un punto singular . . . 261
5.8. Multiplicidad de intersección . . . 263
5.9. Ramas analíticas . . . 264
5.9.1. Polígono de Newton . . . 265
5.10. Puntos cuspidales y contacto maximal . . . 265
5.10.1. Desingularización de curvas planas vía el contacto maximal . . . 266
5.11. Teoremas de Bézout y Max Noether . . . 268
5.12. Apéndice: Revestimientos . . . 271
5.12.1. Introducción . . . 271
5.12.2. Teoría de Galois de revestimientos . . . 271
5.12.3. El maravilloso automorfismo de Frobënius . . . 276
5.12.4. Revestimientos ramificados de curvas . . . 278
5.12.5. Cálculos locales . . . 279
5.13. Problemas . . . 281

6. Álgebra Conmutativa Homológica 287
6.1. Introducción . . . 287
6.2. Módulos diferenciales. Homología . . . 287
6.3. Tores y Extens . . . 293
6.4. Complejo de Koszul . . . 296
6.5. Teorema de Serre para los anillos regulares . . . 298
6.6. Anillos de Cohen-Macaulay y Gorenstein . . . 301
6.7. Criterios de platitud . . . 306
6.7.1. Criterio local de platitud y consecuencias . . . 306
6.7.2. Platitud genérica . . . 310
6.8. Morfismos lisos y formalmente lisos . . . 311
6.9. Problemas . . . 315

7. Desingularización de superficies **317**
7.1. Introducción . . . 317
7.2. Multiplicidad y platitud normal en hipersuperficies . . . 318
7.3. Contacto maximal para hipersuperficies . . . 321
7.4. Exponente idealístico . . . 324
7.5. Tangente estricto . . . 326

8. Bases de Gröbner **329**
8.1. Órdenes monomiales . . . 329
8.2. Bases de Gröbner . . . 331
8.3. Aplicaciones . . . 333
8.3.1. Teoría de la eliminación . . . 334
8.3.2. Cálculo de la función de Hilbert . . . 334
8.3.3. Cierre proyectivo de una variedad afín . . . 335
8.3.4. Deformación plana de una variedad proyectiva a una variedad proyectiva monomial 335
8.3.5. Cálculo del espacio tangente en un punto . . . 336
8.3.6. Expresión de un elemento como combinación lineal de los generadores . . . 337
8.3.7. Cálculo del núcleo y de antimágenes de un morfismo entre módulos finito generados 337
8.3.8. Cálculo de extens y tores. . . . 338

Bibliografía **339**

Índice de términos **341**

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 el catedrático Juan Bautista Sancho Guimerá y su discípulo el catedrático 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 catedrático Juan A. Navarro, en el capítulo sobre la desingularización de superficies he seguido unas notas del catedrático 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 segundo manual, los conocimientos básicos de un profesor en el área de Álgebra.

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.

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 sólo 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, $\operatorname{Spec} A_X$. 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 $A_X \to A_U := \{f/g,\, f, g \in A_X$ y g 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 $A_X \to A_Y = \{\bar{f},\ f \in A_X : \bar{f} = \bar{g}$ si y sólo si $f - g$ 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
$p_1(x_1,\ldots,x_n) = \cdots = p_r(x_1,\ldots,x_n) = 0$	$\mathbb{C}[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$
$\phi\colon X \to Y$	$\phi^* : A_Y \to A_X$, $\phi^*(f) = f \circ \phi$
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.

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 con una "significación real" de otras áreas de la Matemática. 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 Conmutativa.

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 sólo 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 sólo si lo es para $-d$ (sólo 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 sólo si $1 = f(g)^{-1} \cdot f(g') = f(g^{-1} \cdot g')$, es decir, si y sólo 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 sólo 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

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

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.

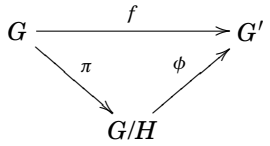
19. Teorema: *Sea $H \subseteq G$ un subgrupo y $\pi : G \to G/H$ la aplicación de paso al cociente. H es un subgrupo normal de G si y sólo si existe en G/H una (única) estructura de grupo, de modo que π sea un morfismo de grupos.*

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 $\overline{gHg'H} = \overline{gg'HH} = \overline{gg'H}$. 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 sólo 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 sólo 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, $\phi : G/\operatorname{Ker} f \to \operatorname{Im} f$, $\phi(\bar{g}) := f(g)$, es un isomorfismo de grupos.*

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

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 sólo 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. $\operatorname{Im} f$ es un subgrupo de G, que contiene a g, luego $\operatorname{Im} f = G$ y f es epiyectivo. $\operatorname{Ker} f$ es un subgrupo de $\mathbb{Z}$, luego existe $n \in \mathbb{N}$ tal que $\operatorname{Ker} f = n\mathbb{Z}$. 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 $\pi : \mathbb{Z} \to G$, $\pi(n) := g^n$, 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 sólo si el máximo común divisor de m y n es 1 ("m y n son primos entre sí").*

Demostración. Consideremos el epimorfismo natural $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(z) = \bar{z}$. 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 sólo $\pi^{-1}(\langle \bar{m} \rangle) = \mathbb{Z}$. Por tanto, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y sólo 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 sólo 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 $\tau: X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f: X \to X$, 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 $\tau \circ f \circ \tau^{-1}: Y \to Y$". 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

$$BiyX \to BiyY, \quad \sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$$

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 $BiyY = BiyX =: S_n$. 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 $r > 1$, denotaremos $(x_1,\dots,x_r) = \sigma \in BiyX$ a 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 $x \notin \{x_1,\dots,x_r\}$. 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 $BiyX$ 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 $d_1,\dots,d_s$ es la forma de σ .

34. Definición: Dado un elemento $g \in G$, diremos que el morfismo $\tau_g: G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h,h' \in G$ son conjugados si y sólo 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 $\sigma = (x_{11},\dots,x_{1d_1})\circ\cdots\circ(x_{s1},\cdots,x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

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

que tiene la misma forma. Sea $\sigma' = (x'_{11},\dots,x'_{1d_1})\circ\cdots\circ(x'_{s1},\cdots,x'_{sd_s})$. 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 $d_1,\dots,d_s$ es la forma de $\sigma \in S_n$, entonces el orden de σ es el mínimo común múltiplo de $d_1,\dots,d_s$.*

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 sólo 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 $(x_1,\dots,x_r) \in S_n$. Obviamente, $(x_1,x_2)(x_1,\dots,x_r) = (x_2,\dots,x_r)$, luego

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

□

Signo de una permutación.

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

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 $\mathrm{sign}(\sigma)$, al número entero 1 ó -1 tal que $\delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \mathrm{sign}(\sigma)\cdot\delta(x_1,\dots,x_n)$.

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

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

es un morfismo de grupos.

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

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

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,

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

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*

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

Demostración. Si $\sigma = (x_1,\dots,x_r)$ es un ciclo, 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 el morfismo sign es un morfismo de grupos, $\mathrm{sign}(\sigma) = (-1)^{r-1}$.

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

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 0.3.5), 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. Dados $h \in H$ y $h' \in H'$, se tiene que $(hh'h^{-1})h'^{-1} = h(h'h^{-1}h'^{-1}) \in H \cap H' = \{1\}$, 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 $h_1 h_1' \in HH'$ y $h_2 h_2' \in HH'$, entonces $(h_1(h_1' h_2 h_1'^{-1})) \cdot (h_1' h_2') \in HH'$. 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 $h_1 h_1' = h_2 h_2'$. 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 $(h_1 h_1') \cdot (h_2 h_2') = (h_1(h_1' h_2 h_1'^{-1})) \cdot (h_1' h_2')$, que no coincide en general con $(h_1 h_2) \cdot (h_1' h_2')$.

48. Ejercicio: Sean G y G' dos grupos y $\phi : G' \to \operatorname{Aut}_{grp}(G)$ un morfismo de grupos. Consideremos las aplicaciones $i_1 : G \to \operatorname{Biy}(G \times G')$, $i_1(g)$ está definida por $i_1(g)(g_1, g') := (gg_1, g')$ y $i_2 : G' \to \operatorname{Biy}(G \times G')$, $i_2(g')$ está definida por $i_2(g')(g, g_1') := (\phi(g')(g), g' g_1')$. Probar 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, probar que $G \cap G' = \{1\}$ y que $G' \subseteq N(G)$. Probar que $g' g g'^{-1} = \phi(g')(g)$ y que por tanto $(g_1 g_1') \cdot (g_2 g_2') = (g_1 \phi(g_1')(g_2)) \cdot (g_1' g_2')$. Se dice que $G \rtimes G'$ es el producto semidirecto de los grupos G y G'.

49. Ejercicio: Sea $G' \to \operatorname{Aut}_{gr}(G)$, $g' \mapsto \mathrm{Id}$, para todo $g' \in G'$, el morfismo trivial. Probar 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 $\operatorname{Biy}(\mathbb{R}^n)$ vía el morfismo inyectivo $G \to \operatorname{Biy}(\mathbb{R}^n)$, $e \mapsto T_e$, donde $T_e(e') := e + e'$. Consideremos G' como subgrupo de $\operatorname{Biy}(\mathbb{R}^n)$ 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 $1 \le i < n$.

52. Ejercicio: Sea $n \ge 2$, $A_n \subseteq S_n$ y $\mathbb{Z}/2\mathbb{Z} = \langle (1,2)\rangle \subseteq S_n$. Probar 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 verifican 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 $G \subset S_n = Biy\{1,\dots,n\}$ es transitivo si opera transitivamente en $\{1,\dots,n\}$.

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

57. Definición: 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 inversa de 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. Teorema: *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. Probar 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 conjunto

$$X/G := \{\bar{x}, x \in X : \bar{x'} = \bar{x} \text{ si y sólo si } x' \in G \cdot x \text{ (o equivalentemente } G \cdot x' = G \cdot x)\}$$

X/G es igual al conjunto de las órbitas de 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 define

$$X/\sim := \{\bar{x}, x \in X : \bar{x'} = \bar{x} \text{ si y sólo si } x' \sim x\}$$

Es decir, si en X identificamos cada $x \in X$ con sus equivalentes, obtenemos el "conjunto cociente por $\sim$", $X/\sim$.

65. Definición: Sea X un G-conjunto. Diremos que $x \in X$ es invariante por G 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 sólo 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 $g \in G$. Es claro 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 psubgrupo de Sylow. G contiene un único p-subgrupo de Sylow si y sólo 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 sólo 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 sólo 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

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

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. Así pues, el sistema de ecuaciones definido por los polinomios $p_1(x_1,x_2,x_3), \ldots, p_r(x_1,x_2,x_3)$ es equivalente al sistema definido por los polinomios del ideal $(p_1(x_1,x_2,x_3), \ldots, p_r(x_1,x_2,x_3))$. 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, por razones obvias, 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 $\tau\colon \bar{k}\to\bar{k}$ 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 $\mathfrak{m}:=\{p(x_1,\dots,x_n)\in A$, 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.

0.2.1. Anillos. Dominios de ideales principales

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 $A\times A \overset{+}{\to} A$, $(a,a')\mapsto a+a'$, $A\times A\overset{\cdot}{\to}A$, $(a,a')\mapsto a\cdot a'$, 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, sólo consideraremos anillos conmutativos con unidad, es decir, verificando

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: $\mathbb{Z}$, el anillo de funciones reales continuas $C(X)$ de un espacio topológico X, los anillos de polinomios $\mathbb{C}[x_1,\dots,x_n]$.

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

$$A[[x_1,\dots,x_n]] := \{\sum_{|\alpha|=0}^{\infty} a_\alpha\cdot x^\alpha,\ a_\alpha\in A\},$$

donde dadas $s(x)=\sum_{|\alpha|=0}^{\infty}a_\alpha\cdot x^\alpha$, $t(x)=\sum_{|\alpha|=0}^{\infty}b_\alpha\cdot x^\alpha\in A[[x_1,\dots,x_n]]$, se define

$$\begin{array}{lcl} s(x)+t(x) & := & \sum_{|\alpha|=0}^{\infty}(a_\alpha+b_\alpha)\cdot x^\alpha \\ s(x)\cdot t(x) & := & \sum_{|\alpha|=0}^{\infty}(\sum_{\beta+\beta'=\alpha}a_\beta\cdot b_{\beta'})\cdot x^\alpha \end{array}$$

3. 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 $i\in I$.

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). Explícitamente $(F)=\{a\in A\colon a=\sum_{i=0}^{n}a_i f_i$ con $f_i\in F, a_i\in A$ y $n\in\mathbb{N}$ cualesquiera$\}$. Dado $a\in A$, también notaremos $(a)=aA$. 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 $I_1+I_2:=\{i_1+i_2\colon i_1\in I_1, i_2\in I_2\}$, que es el mínimo ideal de A que contiene a I_1 y I_2.

4. 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.

$\mathbb{Z}$ 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 anillo es un cuerpo si para cada $a\in A$ no nulo, existe el inverso respecto de la multiplicación, que denotaremos a^{-1}.

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

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

6. Definición: Sea A un anillo. Diremos que un ideal $I\subset A$ es principal si está generado, como A-módulo, por un sólo elemento, i.e., $I=aA$. Diremos que un anillo es un dominio de ideales principales si es un anillo íntegro cuyos ideales son principales.

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

$\mathbb{Z}$ es un dominio de ideales principales: Si $I \subseteq \mathbb{Z}$ es un ideal, en particular es un subgrupo (aditivo), luego $I = n\mathbb{Z}$.

7. Definición: Diremos que el grado de $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$, con $a_n \neq 0$ es n y denotaremos $gr\,P(x) = n$. Seguiremos la convención: $gr\,(0) = -1$.

8. Observación: Si A es un anillo íntegro, entonces el grado de polinomios es aditivo, es decir, se verifica la fórmula

$$gr\,(P(x)Q(x)) = gr\,(P(x)) + gr\,(Q(x))\ .$$

para cada par de polinomios no nulos $P(x), Q(x)$. Por tanto, si $P(x)$ es múltiplo de $Q(x)$, entonces $gr\,P(x) \geq gr\,Q(x)$.

9. 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. □

10. Definición: Se dice que un polinomio $P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in k[x]$, con $a_0 \neq 0$ es mónico si $a_0 = 1$.

11. Proposición: *$k[x]$ (y en general, todo anillo euclídeo) es un dominio de ideales principales.*

Demostración. Cada ideal no nulo de $k[x]$ está generado por el polinomio (digamos mónico) de grado más pequeño: Dado un ideal $0 \neq I \subseteq k[x]$, sea $0 \neq Q(x) \in I$ el polinomio de grado más pequeño. Dado $P(x) \in I$, por el algoritmo de división existen polinomios $C(x)$ y $R(x)$ tales que $P(x) = C(x) \cdot Q(x) + R(x)$ y $gr\,R(x) < gr\,(Q(x))$. Como $R(x) \in I$, entonces $R(x) = 0$ e $I = (Q(x))$. Si $Q(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in k[x]$, con $a_0 \neq 0$, entonces $Q'(x) = a_0^{-1} \cdot Q(x)$ es mónico e $I = (Q'(x))$. □

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

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

Si A es un dominio de ideales principales, los elementos de A, salvo productos por invertibles, se corresponden con los ideales de A. En éstos anillos es válida gran parte de la teoría elemental de la divisibilidad de números enteros. En efecto, si $a, b \in A$, 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 $aA \cap bA$. Por tanto, el máximo común divisor y el mínimo común múltiplo de dos elementos de un dominio de ideales principales A siempre existen y están bien definidos salvo factores invertibles.

12. 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*

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

13. Observación: El algoritmo de Euclides en $k[x]$ (y en $\mathbb{Z}$) nos da un algoritmo para calcular el máximo común divisor de dos polinomios: Dados dos polinomios P,Q 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. Entonces,

$$\begin{aligned} P &= C_1Q + R_2 \\ Q &= C_2R_2 + R_3 \\ R_2 &= C_3R_3 + R_4 \\ &\cdots \\ R_{r-2} &= C_{r-1}R_{r-1} + R_r \end{aligned}$$

siendo R_r el primero tal que $R_r = 0$. Entonces,

$$m.c.d(P,Q) = m.c.d.(Q,R_2) = \cdots = m.c.d.(R_{r-2},R_{r-1}) = (R_{r-1})$$

Además, el algoritmo de Euclides nos permite calcular $\lambda(x)$, $\mu(x)$ tales que $\lambda(x)\cdot P(x) + \mu(x)\cdot Q(x) = m.c.d(P,Q)$: Sabemos expresar R_2 como combinación $k[x]$-lineal de P y Q, luego sabemos expresar R_3 como combinación lineal de P y Q, y así sucesivamente sabremos expresar R_{r-1} como combinación lineal de P y Q.

14. Definición: Un elemento propio (no nulo ni invertible) de un anillo íntegro se dice que es irreducible si no descompone en producto de dos elementos propios. Se dice que dos elementos propios son primos entre sí, si carecen de divisores propios comunes.

15. Definición: Los elementos irreducibles de $\mathbb{Z}$ se denominan números primos.

16. Lema de Euclides: *Si un elemento irreducible de un dominio de ideales principales divide a un producto divide algún factor.*

Demostración. Si a es irreducible y divide a bc, entonces si a no divide a b implica que el máximo común divisor de a y b es el 1. Por tanto, existen $\alpha,\beta \in A$ tales que $\alpha a + \beta b = 1$. Luego $\alpha ac + \beta bc = c$. De esta igualdad obtenemos que a divide a c. □

17. Definición: Se dice que un anillo A es noetheriano si todo ideal es finito generado.

18. Proposición: *Un anillo A es noetheriano si y sólo si toda cadena creciente de ideales de A, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ estabiliza, es decir, para $n >> 0$, $I_n = I_m$, para todo $m \geq n$.*

Demostración. Si A es noetheriano e $I_1 \subseteq I_2 \subset \cdots \subset I_n \subseteq \cdots$ una cadena creciente de ideales de A, consideremos el ideal $J := \cup_i I_i = (a_1,\ldots,a_r)$. Para $n >> 0$, $a_1,\ldots,a_r \in I_n$, luego $I_n \subseteq J \subseteq I_n$, es decir, $J = I_n$ y $I_n = I_m$, para todo $m \geq n$.

Veamos el recíproco. Sea I un ideal, si $I \neq 0$ sea $0 \neq a_1 \in I$ y $I_1 := (a_1)$, Si $I_1 \neq I$, sea $a_2 \in I \backslash I_1$ e $I_2 := (a_1,a_2)$. Así sucesivamente vamos construyendo una cadena $0 \underset{\neq}{\subset} I_1 \underset{\neq}{\subset} I_2 \underset{\neq}{\subset} I_3 \underset{\neq}{\subset} \cdots$ que por la propiedad exigida a A ha de ser finita. Luego, para $n >> 0$, $I = I_n = (a_1,\ldots,a_n)$.

□

Evidentemente, los dominios de ideales principales son noetherianos. El teorema de la base de Hilbert afirmará que los anillos de polinomios $k[x_1,\ldots,x_n]$ son noetherianos.

19. Teorema de descomposición en factores irreducibles: *Todo elemento propio $a \in A$, de un anillo noetheriano íntegro, descompone en producto de factores irreducibles $a = p_1 \cdots p_n$. Además, si A es un dominio de ideales principales, la descomposición es única salvo orden y factores invertibles.*

Demostración. 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 $(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \ldots$ que ha de ser finita por noetherianidad y terminará cuando a_n sea irreducible.

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 $(a) \underset{\neq}{\subset} (b_1) \underset{\neq}{\subset} (b_2) \underset{\neq}{\subset} \ldots$ que ha de ser finita y terminará cuando b_n sea irreducible. En tal caso $a = a_1 \cdots a_{n-1} \cdot b_n$ es producto de irreducibles.

Veamos ahora la unicidad, cuando A es un dominio de ideales principales. Sean $a = p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones en factores irreducibles. Por el Lema de Euclides, q_1 divide algún factor p_i, luego coincide con él (salvo un factor invertible). Pongamos $p_1 = q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$ (salvo invertibles). 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). □

Sea A un dominio de ideales principales, $a, b \in A$ 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 $p_1, \ldots, p_r$ irreducibles y primos entre sí. Es fácil calcular el máximo común divisor y el mínimo común múltiplo (salvo invertibles):

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

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

21. Proposición: *Sea $P(x) \in k[x]$ un polinomio y $\alpha \in k$. Entonces, α es una raíz de $P(x)$ si y sólo 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. □

El teorema fundamental del álgebra afirma que todo polinomio de grado mayor que cero con coeficientes complejos tiene al menos una raíz compleja. Por tanto, si $P(x) \in \mathbb{C}[x]$ es irreducible entonces existe una raíz $\alpha \in \mathbb{C}$ de $P(x)$, luego $P(x) = \lambda \cdot (x - \alpha)$, para cierto $\lambda \in \mathbb{C}$. Por lo tanto, por el teorema de descomposición en factores irreducibles, dado $Q[x] \in \mathbb{C}[x]$, existen $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ distintos de modo que

$$Q(x) = \lambda \cdot (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$$

para cierto $\lambda \in \mathbb{C}$.

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

22. Lema: *Sea $P(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{Q}[x]$ un polinomio con coeficientes racionales. Supongamos que es de coeficientes enteros, multiplicando por un número entero conveniente. 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 $0 = (\frac{r}{s})^n a_0 + (\frac{r}{s})^{n-1} a_1 + \cdots + a_n$, luego $0 = r^n a_0 + r^{n-1} s a_1 + \cdots + s^n a_n$. Por tanto, $s^n a_n$ es múltiplo de r y $r^n a_0$ es múltiplo de s. Luego, a_n es múltiplo de r y a_0 es múltiplo de s. □

23. Proposición: *Si $P(x) \neq 0$ es un polinomio de grado $n \geq 0$, no puede tener más de n raíces distintas.*

Demostración. Procedamos por inducción sobre n. Si $n = 0$, entonces $P(x) = \lambda \in k$ y no tiene raíces. Si $\text{gr}P(x) \geq 0$ y α es una raíz de $P(x)$, entonces $P(x) = (x - \alpha) \cdot Q(x)$, con $\text{gr}Q(x) = \text{gr}(P(x)) - 1$. Las raíces de $P(x)$ son las de $Q(x)$ junto con α. Las raíces de $Q(x)$ son a lo más $n - 1$, por inducción. Luego, $P(x)$ tiene a lo más n raíces.

□

24. Fórmula de interpolación de Lagrange: *Dados $\alpha_0, \ldots, \alpha_n \in k$ distintos y $\lambda_0, \ldots, \lambda_n \in k$ existe un único polinomio $P(x)$ de grado menor o igual que n tal que $P(\alpha_i) = \lambda_i$, para todo i. Además,*

$$P(x) = \sum_{i=1}^{n} \lambda_i \cdot \frac{(x - \alpha_0) \cdots \widehat{(x - \alpha_i)} \cdots (x - \alpha_n)}{(\alpha_i - \alpha_0) \cdots \widehat{(\alpha_i - \alpha_i)} \cdots (\alpha_i - \alpha_n)}$$

Diremos que $P(x)$ es el polinomio de interpolación de $\alpha_0, \ldots, \alpha_n$ con valores $\lambda_0, \ldots, \lambda_n$.

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

Si $Q(x)$ fuese otro polinomio con las mismas propiedades 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 $Q(x) = P(x)$. □

25. 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 $Q(\alpha) \neq 0$.

26. Ejercicio: Probar que 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.

27. Proposición: *Sea $P(x) \in k[x]$ un polinomio. Entonces, $\alpha \in k$ es una raíz múltiple de $P(x)$ si y sólo 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 sólo si es raíz de $Q(x)$, es decir, si y sólo si α es una raíz múltiple de $P(x)$. □

0.2.2. Cociente por un ideal

28. 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. $f(1) = 1$.

29. Ejemplos: La aplicación $\mathbb{C}[x] \to \mathbb{C}$, $p(x) \mapsto p(33)$, es un morfismo de anillos. Dada una aplicación continua $\phi: X \to Y$ entre espacios topológicos, la aplicación $\tilde{\phi}: C(Y) \to C(X)$, $f \mapsto f \circ \phi$ 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. Si un morfismo de anillos es epiyectivo la imagen de un ideal es un ideal.

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

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

$$A/I := \{\bar{a},\ a \in A, \text{ de modo que } \bar{a} = \bar{a'} \iff a - a' \in I\}$$

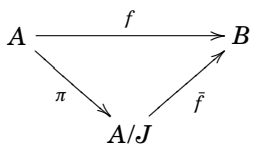
Podemos definir en A/I la operación "producto", $\bar{a} \cdot \bar{a'} := \overline{a \cdot a'}$, que dota a A/I de estructura de anillo (compruébese), y es la única estructura de anillo que podemos definir en A/I, de modo que el morfismo de paso al cociente $A \to A/I$, $a \mapsto \bar{a}$, sea un morfismo de anillos.

30. 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

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

Por tanto, un número natural $n = n_1 n_2 \ldots n_r$, escrito en base decimal, es divisible por nueve si y sólo si la suma de sus cifras, $n_1 + \cdots + n_r$ es divisible por nueve.

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 $\bar{f}: A/J \to B$ (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.

31. Teorema de isomorfía: *Sea $f: A \to B$ un morfismo de anillos. La aplicación, $\phi: A/\mathrm{Ker}\, f \to \mathrm{Im}\, f$, $\phi(\bar{a}) := f(a)$, es un isomorfismo de anillos.*

32. 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 $\mathrm{Ker}\, f = (p(x))$. Obviamente, $x^2+1 \in \mathrm{Ker}\, f$, luego $p(x)$ ha de dividir a x^2+1. Como no existe ningún polinomio de grado 1 en $\mathrm{Ker}\, f$, concluimos que $\mathrm{Ker}\, f = (x^2+1)$ y por el teorema de isomorfía $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

33. 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, sólo 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, $f(a + i_1) = (\overline{a + i_1}, \overline{a + i_1}) = (\bar{a}, \bar{b})$. □

En particular, dados dos números enteros $n, m \in \mathbb{Z}$, primos entre sí (luego $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$), se tiene que

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

La identidad de Bézout nos da el isomorfismo inverso: Por 0.2.13, 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.

0.2.3. Operador de Euler. Polinomios ciclotómicos

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

Si $p \in \mathbb{Z}$ es un número primo entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, porque todo elemento no nulo es invertible. Luego, $\mathbb{Z}/p\mathbb{Z}$ es un anillo íntegro, cuando p es un número primo.

34. Definición: Denotamos $(\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$ al grupo de los elementos invertibles de $\mathbb{Z}/n\mathbb{Z}$ con el producto.

35. Teorema: *Se verifica la igualdad:*

$$(\mathbb{Z}/n\mathbb{Z})^* = Aut_{grp}(\mathbb{Z}/n\mathbb{Z}), \bar{m} \mapsto h_{\bar{m}}$$

donde $h_{\bar{m}}(\bar{i}) := \bar{m} \cdot \bar{i}$.

Demostración. Las homotecias son morfismos de grupos con la suma. Si $\tau \in \mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ y denotamos $\bar{m} = \tau(\bar{1})$, entonces $\tau(\bar{i}) = \tau(\bar{1} + \overset{i}{\cdots} + \bar{1}) = \tau(\bar{1}) + \overset{i}{\cdots} + \tau(\bar{1}) = i \cdot \bar{m} = h_{\bar{m}}(\bar{i})$, es decir, $\tau = h_{\bar{m}}$ es una homotecia. Luego, $\mathbb{Z}/n\mathbb{Z} = \mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, $\bar{m} \mapsto h_{\bar{m}}$.

Como $h_{\bar{m} \cdot \bar{m'}} = h_{\bar{m}} \circ h_{\bar{m'}}$, los invertibles (con el producto) de $\mathbb{Z}/n\mathbb{Z}$ se identifican con los invertibles de $\mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ con la composición.

□

36. Definición: Sea $\phi: \mathbb{N} \to \mathbb{N}$ 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|.

37. Notación: 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).

38. Congruencia de Euler: *Si n, m son naturales primos entre sí, se verifica la fórmula:*

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

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

En el caso de ser $p \in \mathbb{N}$ un número primo es claro que todo número natural menor que p es primo con p, luego:

$$\boxed{\phi(p) = p - 1}$$

En particular, se verifica que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (todo elemento no nulo tiene inverso) y la congruencia de Euler dice:

39. Congruencia de Fermat: *Si p es primo y $m \not\equiv 0 \, mod \, p$, se entonces verifica la fórmula:*

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

Otra congruencia útil es la siguiente:

40. Congruencia de Wilson: *Si p es un número 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 un número no es igual a su inverso en $(\mathbb{Z}/p\mathbb{Z})^*$, entonces en este producto ambos se cancelan (dando 1) luego en el producto mencionado sólo permanecen aquellos x que verifiquen que son igual a su inverso. Si $1 = xx = x^2$ en $\mathbb{Z}/p\mathbb{Z}$, o lo que es lo mismo, si $0 = x^2 - 1 = (x-1)(x+1)$ en $\mathbb{Z}/p\mathbb{Z}$, entonces como $\mathbb{Z}/p\mathbb{Z}$ es íntegro, $x - 1$ ó $x + 1 = 0$ en $\mathbb{Z}/p\mathbb{Z}$, es decir, $x = 1, -1$ en $\mathbb{Z}/p\mathbb{Z}$. Por tanto, $(p-1)! = 1 \cdot (-1) = -1$ en $\mathbb{Z}/p\mathbb{Z}$. □

41. Teorema: *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. Es $G = \mathbb{Z}/n\mathbb{Z}$. 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, $H = \langle \bar{m'} \rangle$. □

42. Teorema: *Se verifica 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 $n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d|n} |X_d| = \sum_{d|n} \phi(d)$.

□

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

Demostración. El directo ya está probado (teorema 0.2.41).

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. □

44. Proposición: *Si n,m son números 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 $\phi(nm) = |(\mathbb{Z}/nm\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*| \cdot |(\mathbb{Z}/m\mathbb{Z})^*| = \phi(n)\phi(m)$. □

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

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

Demostración. Un número r es primo con p^n si y sólo 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, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

A partir de estas proposiciones se obtiene inmediatamente el siguiente:

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

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

47. 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 $0 < m < n$.

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

Observemos que

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

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,

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

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

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

Una raíz n-ésima de la unidad es primitiva si y sólo si no es d-ésima para ningún divisor estricto d de n y, por tanto,

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

luego 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.

49. 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,* $\Phi_{r\cdot p^n}(x) = \frac{\Phi_r(x^{p^n})}{\Phi_r(x^{p^{n-1}})}$.

10. *Si $r>2$ es impar,* $\Phi_{2r}(x) = \Phi_r(-x)$.

50. Lema: *Para cada $Q(x)\in\mathbb{Z}/p\mathbb{Z}[x]$ se verifica la identidad:*

$$Q(x)^p = Q(x^p)$$

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

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

□

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

Demostración. Sea $\Phi_n(x) = P(x)\cdot Q(x)$ con $P(x)\in\mathbb{Z}[x]$, $\operatorname{gr}P(x)>0$. Como se sabe, si ε es una raíz primitiva de la unidad, entonces las raíces primitivas n-ésimas de la unidad son exactamente las de la forma ε^m con $(m,n)=1$. Por tanto, para ver que $P(x)=\Phi_n(x)$ basta ver que si ε es raíz de $P(x)$ y p un número primo no divisor de n, entonces ε^p es también raíz de $P(x)$. Sea pues ε una raíz de $P(x)$ tal que ε^p sea raíz de $Q(x)$. Entonces, los polinomios $P(x)$ y $Q(x^p)$ que tienen en común la raíz ε, no son primos entre sí. Luego, $P(x)^p$ y $Q(x^p)$ no son primos entre sí. Entonces, en $\mathbb{Z}/p\mathbb{Z}[x]$, $\overline{P(x)^p} = \overline{P(x)}^p$ y $\overline{Q(x^p)} = \overline{Q(x)}^p$ no son primos entre sí. Luego, $\overline{P(x)}$ y $\overline{Q(x)}$ no son primos entre sí. Luego, $\overline{\Phi_n(x)} = \overline{P(x)}\cdot\overline{Q(x)}$ tiene raíces múltiples. Sin embargo, $\overline{\Phi_n(x)}$ tiene las raíces distintas, pues todas las raíces de x^n-1 son distintas ya que es primo con su derivada $\bar{n}x^{n-1}\neq 0$. Hemos llegado a contradicción. □

0.2.4. Ideales primos. Ideales maximales

52. 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 $b\in\mathfrak{p}$.

53. Proposición: *Un ideal $\mathfrak{p}\underset{\neq}{\subset}A$ es un ideal primo si y sólo 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. □

54. 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.

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

1. *p es irreducible en A.*

2. *pA es un ideal primo de A.*

3. pA es un ideal maximal de A.

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

2. $\Rightarrow$ 1. Sea pA un ideal primo. Por tanto, si $ab = p$, p ha de dividir a uno de los factores, por ejemplo a, y tendremos $pa'b = p$, luego b sería invertible y p irreducible.

1. $\Rightarrow$ 3. Sea $I = aA$ un ideal. Si $pA \subseteq I = aA$, entonces existe $b \in A$ tal que $ab = p$. Luego, a es invertible y $I = A$, o b es invertible y $I = pA$. En conclusión, pA es maximal.

□

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

Demostración. Esta es una aplicación típica del lema de Zorn (que puede evitarse en anillos noetherianos, más tarde estudiados). 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. □

57. Definición: Se dice que un ideal primo es minimal si no contiene estrictamente ningún ideal primo.

58. Ejercicio: En todo anillo $A \neq 0$ existen ideales primos minimales.

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

Demostración. Sea $\pi : A \to A/I$ el morfismo de paso al cociente. En la correspondencia biunívoca

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

$$J \longmapsto \pi(J)$$

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

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 sólo si $(a) = A$ (suponemos $A \neq 0$). Por tanto, $a \in A$ es invertible si y sólo si no está incluido en ningún ideal maximal. En particular, un anillo es un cuerpo si y sólo si los únicos ideales del anillo son el (0) y todo el anillo.

60. Proposición: *Un ideal $\mathfrak{m} \subsetneq A$ es maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo. En particular, los ideales maximales son ideales primos, por la proposición 0.2.53.*

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

0.2.5. Espectro primo de un anillo

61. 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.

62. Ejemplos: $k[x_1,\dots,x_n]$ es una k-álgebra y $\mathrm{Hom}_{k-alg}(k[x_1,\dots,x_n],B)=B^n$, $\phi\mapsto(\phi(x_1),\dots,\phi(x_n))$
El anillo de funciones continuas reales de un espacio topológico es una $\mathbb{R}$-álgebra.

63. 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 $\phi\colon A\to k$ (que ha de ser epiyectivo) tenemos el ideal primo racional $\mathrm{Ker}\,\phi$. En conclusión,

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

64. 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 las biyecciones

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

Por último, $\mathrm{Ker}\,\phi_\alpha=(x_1-\alpha_1,\dots,x_n-\alpha_n)$, porque $(x_1-\alpha_1,\dots,x_n-\alpha_n)\subseteq\mathrm{Ker}\,\phi_\alpha$.

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.

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

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

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

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 $V=\mathrm{Spec}_{rac}A$.

66. Ejemplo: Sea $X=[0,1]\subset\mathbb{R}$ 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 $C(X)/\mathfrak{m}_p\simeq\mathbb{R}$, $\bar f\mapsto f(p)$.

Veamos el recíproco: 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

$$X\xrightarrow{\ \ =\ \ }\mathrm{Spec}_{rac}\,C(X),\ p\mapsto\mathfrak{m}_p$$

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 $C=\{x\in X,$ tales que $f(x)=0,$ para toda $f\in I_C\}$. Dado un ideal $I\subset C(X)$, denotemos $(I)_0^{rac}$ el conjunto de los ideales racionales de $C(X)$ que contienen a I. Bien, a través de la igualdad anterior, se cumple que $\{x\in X,$ tales que $f(x)=0,$ para toda $f\in I\}=(I)_0^{rac}$.

Si $f\colon A\to B$ 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

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

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

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

porque 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 $(\bar{x}_1-f_1(\alpha_1,\dots,\alpha_m),\dots,\bar{x}_n-f_n(\alpha_1,\dots,\alpha_m))$.

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

68. Notación: Un ideal primo lo denotaremos por x cuando lo consideremos como elemento de $\mathrm{Spec}A$, 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 $\mathrm{Spec}A$. Diremos que una función $a\in A$ se anula en un punto $x\in\mathrm{Spec}A$ 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 $\mathrm{Spec}A$.
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.

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

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

71. 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,

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

72. Proposición: *Se verifican 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 $(I_1\cap I_2)_0\subseteq(I_1)_0\cup(I_2)_0$. □

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

74. 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, $(4)_0 = (2)_0 \subset \operatorname{Spec}\mathbb{Z}$.

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

76. 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).

77. 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.

□

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

79. 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, $\bar{Y} = (I)_0$.

□

80. 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 sólo si $\mathfrak{p}_x$ es un ideal maximal.*

81. 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, 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.

82. 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 $g \in I$.

□

83. Ejercicio: Calcular 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

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

84. 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.

□

85. Ejercicio: Sea $X = [0,1] \subset \mathbb{R}$ y $C(X)$ el anillo de las funciones reales continuas definidas en X. Probar que la aplicación

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

es biyectiva (usar el ejemplo 0.2.66 y que todo morfismo $C(X) \to C(X)$ induce un morfismo entre los espectros).

86. 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 verifica 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,

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

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

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

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.

□

87. Ejercicio: Sea Y un subespacio cerrado de un espacio topológico X. Probar 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 probar 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).

88. 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.

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

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

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

0.2.6. Localización. Dominios de factorización única

90. 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 $s \cdot s' \in S$.

91. Ejemplo: $\mathbb{Z} \setminus \{0\}$ es un sistema multiplicativo de $\mathbb{Z}$.

92. 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

$$A_S := \left\{ \frac{a}{s},\ a \in A \text{ y } s \in S \colon \frac{a}{s} = \frac{a'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones } \frac{s_1 a}{s_1 s}, \frac{s_2 a'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \right\}^{2}$$

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 $\varphi(ta, ts) = \varphi(a,s)$ 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.

93. Ejercicio: Probar que una fracción $\frac{a}{s} = 0 \in A_S$ si y sólo si existe $s' \in S$ tal que $s' \cdot a = 0$ (en A).

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

95. 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.

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

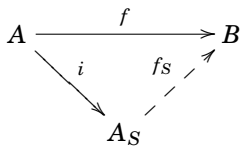
2. $\mathbb{Q}(x) := \mathbb{Q}[x]_{\mathbb{Q}[x] \setminus \{0\}}$

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

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

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

98. Propiedad universal de la localización: *Sea $i \colon A \to A_S$ el morfismo de localización. Si $f \colon A \to B$ es morfismo de anillos tal que $f(s)$ es invertible para todo $s \in S$, entonces existe un único morfismo de anillos $f_S \colon A_S \to B$ tal que $f = f_S \circ i$, es decir, tal que el diagrama siguiente es conmutativo*



(explícitamente, $f_S(\frac{a}{s}) = f_S(\frac{a}{1} \cdot \frac{1}{s}) = f_S(\frac{a}{1} \cdot (\frac{s}{1})^{-1}) = f_S(\frac{a}{1}) \cdot f_S(\frac{s}{1})^{-1} = f(a) \cdot f(s)^{-1}$).

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

100. 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 y factores invertibles. DFU significará dominio de factorización única.

101. Ejemplo: Los dominios de ideales principales son dominios de factorización única.

[2] Observemos que $\frac{a}{s} = \frac{a}{s}$, que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'}{s'} = \frac{a}{s}$, y que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{a'}{s'} = \frac{a''}{s''}$ entonces $\frac{a}{s} = \frac{a''}{s''}$.

102. Lema de Euclides: *Sea A DFU. Si $a \in A$ es irreducible y a divide a un producto entonces a divide a uno de los factores. Por tanto, si a es irreducible entonces $A/(a)$ es un anillo íntegro.*

Demostración. Sea $b \cdot c = a \cdot d$. Si consideramos las descomposición en factores irreducibles de b, c y d, y recordamos que A es DFU, tenemos que a aparece (salvo multiplicación por un invertible) en la descomposición en producto de factores irreducibles de b o c. Luego, a divide a b o c. Dicho de otro modo, si $\bar{b} \cdot \bar{c} = \bar{0} \in A/(a)$ entonces o $\bar{b} = \bar{0}$, o bien $\bar{c} = 0$. □

103. Definición: Un polinomio $P(x) \in A[x]$ se dice *primitivo* cuando sus coeficientes no admiten un divisor común no invertible, es decir, si $P(x) = a \cdot Q(x)$ con $a \in A$, entonces a es invertible.

104. 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 verifica:*

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 $\overline{P(x)}, \overline{C(x)}, \overline{D(x)} \in (A/(p))[x] \subseteq k(p)[x]$ las clases de $P(x), C(x)$ y $D(x)$ módulo p (siendo $k(p)$ el cuerpo de fracciones de $A/(p)$). Por 2., es $\overline{P(x)} = \overline{a}_0x^n$ y, por tanto, $\overline{C(x)} = \overline{c}_{n-i}x^i$ 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.

□

105. 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 $u \in A$. □

106. Teorema: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio no constante primitivo, $P(x) \in A[x]$, es irreducible en $A[x]$ si y sólo 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 0.2.105, $\frac{a}{b} = u \in A$, luego $P(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

107. Teorema (Gauss): *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 0.2.105, $\frac{b}{c} = u \in A$ es un invertible de A.
- Cada $Q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por el teorema 0.2.106.

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 teorema 0.2.106. 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 del teorema anterior, se obtiene el siguiente teorema.

108. 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.*

109. Descomposición de un polinomio con coeficientes racionales en factores irreducibles. Sea $P(x) \in \mathbb{Q}[x]$ no constante. $P(x) = \frac{r}{s} \cdot Q(x)$, con $r, s \in \mathbb{Z}$ y $Q(x) \in \mathbb{Z}[x]$, primitivo. Por el lema de Gauss, para descomponer $P(x)$ en factores irreducibles basta descomponer $Q(x)$ en factores irreducibles en $\mathbb{Z}[x]$. Basta saber calcular los polinomios $Q_r(x) \in \mathbb{Z}[x]$, con $r = \operatorname{gr} Q_r(x) \leq (\operatorname{gr} Q(x))/2$ que dividen a $Q(x)$. Todo polinomio de grado r, $R(x)$ coincide con el polinomio de interpolación de $0, 1, \ldots, r$ con valores $R(0), \ldots, R(r)$. Si $Q(x) = Q_r(x) \cdot Q_s(x)$, entonces $Q_r(i)$ divide a $Q(i)$ (observemos que sólo hay un número finito de enteros que dividen al entero $Q(i)$). Sea $Y = \{(\lambda_0, \ldots, \lambda_r) \in \mathbb{Z}^{r+1} \colon \ \lambda_i \text{ divide a } Q(i), \text{ para todo } i\}$, y para cada $y = (\lambda_0, \ldots, \lambda_r) \in Y$ sea $Q_y(x)$ el polinomio de interpolación de $0, 1, \ldots, r$ con valores $\lambda_0, \ldots, \lambda_r$. Entonces, $Q_r(x)$ coincide con $Q_y(x)$ para algún $y \in Y$ ($Q_y(x)$ debe dividir a $Q(x)$).

0.2.7. 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 $j \colon A \to B$, 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 $(j(I)) = j(I) \cdot B = I \cdot B$.

110. Teorema: *Consideremos el morfismo $j \colon A \to A_S$, $a \mapsto \frac{a}{1}$, de localización por S. La aplicación inducida $j^* \colon \operatorname{Spec} A_S \to \operatorname{Spec} A$ 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. Consideremos el morfismo de localización $j\colon A \to A_S$.

Las asignaciones

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

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

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

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 $j^*((\frac{a}{s})_0) = j^*((\frac{a}{1})_0) = (a)_0 \cap \operatorname{Im} j^*$.

□

111. 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 $\operatorname{Spec} A$.

112. 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, $\operatorname{Spec} A_f$ 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 $\operatorname{Spec} A_f$ se corresponde con los ideales primos $\mathfrak{p}_x$ de A que no contienen a f, es decir, U_f. □

113. 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. Probar 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 $h = \frac{f}{s}$).

114. 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. $\operatorname{Spec} A_x$ 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 $\mathfrak{p}_x$. □

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

"Podemos decir que el anillo de funciones que consideramos en $U_f = \operatorname{Spec} A_f$ 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 $\operatorname{Spec} A$, 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".

116. 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.

117. 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 sólo 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 0.2.112, $\operatorname{Spec} A_f = \emptyset$. 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 $\operatorname{Spec} A = \operatorname{Spec}(A/\operatorname{rad} A)$.

118. 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 $\bar{a} = 0$.

119. Proposición: $\operatorname{Spec} A$ *es irreducible si y sólo 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. □

120. 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 $B_{j(A \setminus \mathfrak{p}_x)} = B_x$.

121. Fórmula de la fibra: *Sea* $j : A \to B$ *un morfismo de anillos y* $j^* : \operatorname{Spec} B \to \operatorname{Spec} A$ *el morfismo inducido. 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 $\operatorname{Spec} C = \emptyset$.

122. Ejemplo: Calculemos $\operatorname{Spec}\mathbb{C}[x,y]$. 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,

$$i^{*-1}(\alpha) = \operatorname{Spec}\mathbb{C}[y] = \{(y-\beta), (0) \text{ con } \beta \in \mathbb{C}\}$$

que se corresponden con los ideales primos de $\mathbb{C}[x,y]$, $(x-\alpha, y-\beta), (x-\alpha)$.

Sólo 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).

123. 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 $q_i(x,y) = 0$.

124. Proposición: *Sea $f : A \hookrightarrow B$ un morfismo inyectivo de anillos. Entonces, la imagen del morfismo $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es densa.*

Demostración. Sea $x \in \operatorname{Spec} A$ el punto genérico de una componente irreducible de $\operatorname{Spec} A$ (es decir, $\mathfrak{p}_x$ es un ideal primo minimal de A). Por la fórmula de la fibra $f^{*-1}(x) = \operatorname{Spec} B_x \neq \emptyset$, porque $B_x \neq 0$, ya que $1 \neq 0$ en B_x. En conclusión, $x \in \operatorname{Im} f^*$ y $\overline{\operatorname{Im} f^*} = \operatorname{Spec} A$. □

0.3. 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 $\pi: E \to X$, 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.

0.3.1. Módulos, submódulos y cocientes. Sistema de generadores

1. Definición: Sea A un anillo y M un conjunto. Diremos que una operación $M \times M \xrightarrow{+} M$, $(m, m') \mapsto m + m'$ y una aplicación $A \times M \dashrightarrow M, (a, m) \mapsto a \cdot m$ 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 $m \in M$.

Es decir, dada una aplicación $A \times M \dashrightarrow M$, $(a, m) \mapsto a \cdot m$, cada elemento $a \in A$ define 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.

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 $\bigoplus_{i\in I} M_i$ 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. 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.

4. Notación: Alguna vez, escribiremos am en vez de $a\cdot m$ por sencillez de escritura.

5. 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.

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.

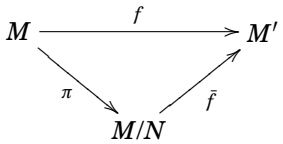
El conjunto de los elementos de un módulo M, que por un morfismo de A-módulos $f: M \to M'$ van al cero, se denomina núcleo de f y se denota por $\mathrm{Ker} f$. Se cumple que $\mathrm{Ker} f$ es un submódulo de M y que f es inyectiva si y sólo si $\mathrm{Ker} f = 0$. El conjunto de los elementos de 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, donde

$$M/N = \{\bar{m},\ m \in M,\ \text{de modo que } \bar{m} = \bar{m'} \iff m - m' \in N\}$$

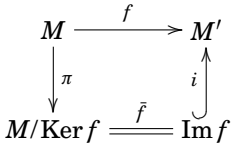
El producto $a\cdot\bar{m} := \overline{a\cdot m}$ dota a M/N de estructura de A-módulo (compruébese) y es la única estructura de A-módulo que podemos definir en M/N, de modo que el morfismo de paso al cociente $M \to M/N$, $m \mapsto \bar{m}$, sea un morfismo de módulos.

6. 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.

7. 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 conjuntos 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 sólo si $\{m_i\}_{i\in I}$ es un sistema generador de M, ϕ es inyectivo si y sólo si $\{m_i\}_{i\in I}$ son linealmente independientes. Por tanto, ϕ es isomorfismo si y sólo 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 sólo 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

$$A^{(J)}\xrightarrow{s} A^{(I)}\xrightarrow{\pi} M$$

M es isomorfo a $\mathrm{Coker}\,s := A^{(I)}/\mathrm{Im}\,s = A^{(I)}/\mathrm{Ker}\,\pi$, 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 sólo si es un A/I-submódulo, y que $\bar{m}_1,\dots,\bar{m}_r\in M/IM$ es un sistema A-generador de M/IM si y sólo si es un sistema A/I-generador de M/IM. En el caso de que $I=\mathfrak{m}$ sea un ideal maximal, tendremos que $\bar{m}_1,\dots,\bar{m}_r\in M/\mathfrak{m}M$ es un sistema A-generador de $M/\mathfrak{m}M$ si y sólo si es un sistema generador del $A/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}M$.

8. 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 $m_1,\dots,m_n \in M$ es un sistema generador de M, si sus clases $\bar{m}_1,\dots,\bar{m}_n$ en $M/\mathfrak{m}M$ son un sistema generador.

Demostración. $\Rightarrow$) Sea $n_1,\dots,n_r$ 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 $\langle n_2,\dots,n_r\rangle = M$, lo que es contradictorio salvo que $r = 0$, es decir, $M = 0$.

$\Leftarrow$) Es obvio.

Veamos la consecuencia. Si $\langle \bar{m}_1,\dots,\bar{m}_n\rangle = M/\mathfrak{m}M$ entonces $M = \langle m_1,\dots,m_n\rangle + \mathfrak{m}M$. Haciendo cociente por $\langle m_1,\dots,m_n\rangle$ y denotando $\bar{M} = M/\langle m_1,\dots,m_n\rangle$, tenemos $\bar{M} = 0 + \mathfrak{m}\bar{M}$. Por tanto, $\bar{M} = 0$, es decir, $M = \langle m_1,\dots,m_n\rangle$. □

0.3.2. Localización de módulos

Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$M_S = \left\{ \frac{m}{s},\ m \in M \text{ y } s \in S\colon \frac{m}{s} = \frac{m'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones } \frac{s_1 m}{s_1 s}, \frac{s_2 m'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \right\}^{3}$$

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 y diremos que es la localización de M por S. 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. Dado un morfismo $f\colon M \to N$ de A-módulos, induce de modo natural la aplicación (bien definida)

$$f_S\colon M_S \to N_S,\ \frac{m}{s} \underset{\text{def}}{\mapsto} \frac{f(m)}{s}$$

que es morfismo de A_S-módulos. Es inmediato comprobar que la localización de morfismos es compatible con composiciones y combinaciones A-lineales:

$$(f \circ g)_S = f_S \circ g_S$$
$$(af + bg)_S = af_S + bg_S$$

9. Proposición: *Dado un morfismo $f\colon M \to N$ de A-módulos y S un sistema multiplicativo de A, se cumple que*

$$(\operatorname{Ker} f)_S = \operatorname{Ker} f_S \ \ y \ \ (\operatorname{Im} f)_S = \operatorname{Im} f_S$$

[3] Observemos que $\frac{m}{s} = \frac{m}{s}$, que si $\frac{m}{s} = \frac{m'}{s'}$ entonces $\frac{m'}{s'} = \frac{m}{s}$, y que si $\frac{m}{s} = \frac{m'}{s'}$ y $\frac{m'}{s'} = \frac{m''}{s''}$ entonces $\frac{m}{s} = \frac{m''}{s''}$.

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 $m \in \operatorname{Ker} f$ y $s \in S$). 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.

10. 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 sólo si i es inyectiva.
2. $M \xrightarrow{\pi} M'' \to 0$ es una sucesión exacta si y sólo si π es un epimorfismo.
3. $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ es exacta si y sólo 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 sólo si $0 \to \operatorname{Im} f_{n-1} \to M_n \to \operatorname{Im} f_n \to 0$ son exactas, para todo n,

11. 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 $\operatorname{Ker} g = \operatorname{Im} f$. Por tanto, $\operatorname{Ker} g_S = (\operatorname{Ker} g)_S = (\operatorname{Im} f)_S = \operatorname{Im} f_S$ (explícitamente, $\frac{m}{s} \mapsto \frac{m}{s}$) y $M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$ es exacta. □

12. Ejercicio: Probar 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 sólo 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 este capítulo 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.

13. Definición: Sea M un A-módulo, llamaremos anulador de M al ideal

$$\mathrm{Anul}(M) := \{a \in A : am = 0, \text{ para todo } m \in M\}$$

Dicho de otro modo, el anulador de M es el núcleo del morfismo de estructura $A \to \mathrm{End}(M)$, $a \mapsto a\cdot$. Se dice que M es un A-módulo fiel si $\mathrm{Anul}(M) = 0$, es decir, si el morfismo $A \to \mathrm{End}(M)$ es inyectivo. Todo A-módulo M es de modo natural un $A/\mathrm{Anul}(M)$-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

$$\mathrm{Anul}(m) = \{a \in A : am = 0\}$$

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 $A/\mathrm{Anul}(m) \simeq \langle m\rangle$.

Igual que hacíamos para los anillos, dada $f \in A$ denotaremos M_f a la localización de M por el sistema multiplicativo $S = \{1, f, f^2, \dots\}$. Dado un ideal primo $\mathfrak{p}_x \subset A$ denotaremos por M_x a la localización de M por el sistema multiplicativo $S = A \setminus \mathfrak{p}_x$.

14. Definición: Llamaremos soporte de un A-módulo M, al subespacio de $\mathrm{Spec}A$ formado por los puntos x donde $M_x \neq 0$ y lo denotaremos por $\mathrm{Sop}(M)$, i.e.,

$$\mathrm{Sop}(M) = \{x \in \mathrm{Spec}A : M_x \neq 0\}$$

15. Teorema: *El soporte de un A-módulo finito generado coincide con los ceros de su ideal anulador, i.e.,*

$$\mathrm{Sop}\, M = (\mathrm{Anul}\, M)_0$$

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 $x \in \mathrm{Spec}A$.

Demostración. Empecemos probando que si $M = \langle m_1, \dots, m_r\rangle$ es un A-módulo finito generado, entonces $M_S = 0$ si y sólo 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 $x \in \mathrm{Spec}A$, tendremos que $M_x \neq 0$ si y sólo si $\mathrm{Anul}(M) \cap (A \setminus \mathfrak{p}_x) = \emptyset$, es decir, $\mathrm{Anul}(M) \subseteq \mathfrak{p}_x$. Luego $\mathrm{Sop}(M) = (\mathrm{Anul}\, M)_0$.

Por último, veamos la consecuencia. Probemos sólo la suficiencia. Si $M_x = 0$ para todo punto cerrado $x \in \mathrm{Spec}A$, entonces para todo submódulo $\langle m\rangle \subseteq M$ se cumple que $\langle m\rangle_x = 0$. Por tanto, el $(\mathrm{Anul}\langle m\rangle)_0$, no contiene ningún punto cerrado de $\mathrm{Spec}A$, es decir, $\mathrm{Anul}\langle m\rangle$ no está contenido en ningún ideal maximal. En conclusión, $\mathrm{Anul}(\langle m\rangle) = A$, luego $m = 1 \cdot m = 0$ y $M = 0$.

□

16. Proposición: *1. Una inclusión $N \subseteq M$ de módulos es una igualdad si y sólo si $N_x = M_x$, para todo punto cerrado $x \in \mathrm{Spec}A$.*

2. Dos submódulos N, N' de un módulo M son iguales si y sólo si $N_x = N'_x$, para todo punto cerrado $x \in \mathrm{Spec}A$.

Demostración. 1. $N = M \iff M/N = 0 \iff (M/N)_x = 0$, para todo punto cerrado $x \in \mathrm{Spec}A \iff M_x/N_x = 0$ para todo punto cerrado $x \in \mathrm{Spec}A \iff M_x = N_x$, para todo punto cerrado $x \in \mathrm{Spec}A$.

2. Veamos sólo que si $N_x = N'_x$, para todo punto cerrado $x \in \mathrm{Spec}A$, entonces $N = N'$. Tendremos que $N_x = N_x + N'_x = (N + N')_x$, para todo punto cerrado $x \in \mathrm{Spec}A$. Luego por el punto 1. $N = N + N'$, es decir, $N' \subseteq N$. Del mismo modo obtenemos la inclusión inversa y concluimos la igualdad.

□

17. 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 0.3.11. 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 sólo si lo es localmente, para todo punto cerrado del espectro del anillo.

Si U es un abierto de $\operatorname{Spec} A$, 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 0.2.88.

18. Proposición: *Si* $\operatorname{Spec} A$ *es la unión disjunta de dos abiertos* U_1, U_2 *entonces* $A = A_{U_1} \times A_{U_2}$.

Demostración. Veamos que $\operatorname{Spec} A_{U_1} = U_1$ (igualmente $\operatorname{Spec} A_{U_2} = U_2$). $U_1 \subseteq \operatorname{Spec} A_{U_1}$, 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 $\operatorname{Spec} A_{U_1} \subseteq U_1$ y $\operatorname{Spec} A_{U_1} = U_1$.

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, $\operatorname{Spec}(A_{U_2})_x = \emptyset$, porque $U_2 \cap \{y \in \operatorname{Spec} A : \mathfrak{p}_y \subseteq \mathfrak{p}_x, i.e., x \in \bar{y}\} = \emptyset$, 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.

□

19. Definición: Llamamos radical de Jacobson de un anillo al ideal que es la intersección de todos los ideales primos maximales del anillo.

20. 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. □

0.3.3. 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.

21. Definición: Un A-módulo M se dice que es un A-módulo noetheriano si todo submódulo suyo (propio o no) es finito generado.

22. 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 $M_r = M_{r+1} = \cdots$.

23. Proposición: *Las dos definiciones anteriores son equivalentes.*

Demostración. **def**$^1 \Rightarrow$ **def**^{2}: Dada una cadena ascendente de submódulos de M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$, sea $M' = \overset{\infty}{\underset{i=1}{\cup}} M_i \subseteq M$. 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 $M_r = M_{r+1} = \cdots$.

def$^2 \Rightarrow$ **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 $\langle m_1, \ldots, m_r \rangle = M'$.

□

24. Ejemplo: Los k-espacios vectoriales de dimensión finita son k-módulos noetherianos.

25. Proposición: *Todo submódulo de un módulo noetheriano es noetheriano.*

26. Proposición: *Todo cociente de un módulo noetheriano es noetheriano.*

Demostración. Sea M noetheriano y $\pi : M \to M/N$ 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, $\bar{M} = \langle \pi(m_1), \ldots, \pi(m_r) \rangle$. □

27. 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 $M' = \langle m_1, \ldots, m_r, n_1, \ldots, n_s \rangle$.

□

28. Ejercicio: Probar que M y M' son noetherianos si y sólo si $M \oplus M'$ es noetheriano.

29. 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.

30. 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.

31. 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 0.3.28. 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.

32. Ejercicio: Probar que si A es noetheriano A_S es noetheriano

33. Ejercicio: Demostrar que $\mathbb{Q}[x, x_1, \dots, x_n, \dots]/((x-n)x_n)_{\{n\in\mathbb{N}\}}$ es localmente noetheriano pero no es noetheriano.

34. Definición: Se dice que un espacio topológico es noetheriano si toda cadena descendente de cerrados estabiliza.

35. 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 sólo 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.

□

36. Proposición: *Si A es un anillo noetheriano, entonces* $\operatorname{Spec} A$ *es un espacio topológico noetheriano. En particular,* $\operatorname{Spec} A$ *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, $C_m = C_{m+1} = \cdots$.

□

37. Corolario: *Sea A un anillo noetheriano e $I \subsetneq A$ un ideal radical. Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ 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.

□

38. 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 $p(x) \in I$. Es fácil ver que J es un ideal de A. Observemos para ello, que 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 $\operatorname{gr} p_i = m$.

Dado $p(x) = a_0x^n + \cdots + a_n \in I$. Supongamos que $n \geq m$. Escribamos $a_0 = \lambda_1 b_1 + \cdots + \lambda_r b_r$, con $\lambda_i \in A$ para todo i. 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 $I = (p_1, \ldots, p_r, q_1, \ldots, q_s)$.

□

39. Definición: Dado un morfismo de anillos $f : A \to B$ se dice que B es una A-álgebra.

40. 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.

41. Ejemplo: $A[x_1, \ldots, x_n]$ es una A-álgebra de modo natural: tenemos el morfismo de anillos $A \to A[x_1, \ldots, x_n]$, $a \mapsto a$.

42. 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.

43. 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.

□

0.3.4. 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.

44. 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 $M \simeq A/\mathrm{Anul}\langle m \rangle$. Ahora bien, los submódulos de $A/\mathrm{Anul}\langle m \rangle$ se corresponden con los ideales de A que contienen a $\mathrm{Anul}\langle m \rangle$. Por tanto, M es simple si y sólo si $\mathrm{Anul}\langle m \rangle$ es un ideal maximal, es decir, M es simple si y sólo si $M \simeq A/\mathfrak{m}$, donde $\mathfrak{m}$ es un ideal maximal de A.

45. Definición: Diremos que una cadena finita de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ 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 $M_{i-1} \subsetneq N \subsetneq M_i$. 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".

46. 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.

47. Proposición: *Todas las series de composición de un módulo tienen la misma longitud.*

Demostración. Si $l(M) = \infty$ la proposición es obvia. Supongamos que $l(M) = n < \infty$.

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 $M_i \cap N/M_{i-1} \cap N \hookrightarrow M_i/M_{i-1}$, luego $M_i \cap N/M_{i-1} \cap N = M_i/M_{i-1}$ pues M_i/M_{i-1} es simple. 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).

48. 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 sólo 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

$$l(M_0) - l(M_1) + \cdots + (-1)^n l(M_n) = 0$$

49. Ejercicio: Sea $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n$ una cadena de A-submódulos de M. Probar que $l(M/M_n) = \sum_{i=1}^{n} l(M_{i-1}/M_i)$.

50. Ejercicio: Sea $\mathscr{O}$ una k-álgebra local de ideal maximal $\mathfrak{m}$. Probar que si M es un $\mathscr{O}$-módulo de longitud finita entonces $\dim_k M = l(M) \cdot \dim_k \mathscr{O}/\mathfrak{m}$.

51. 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 sólo si $M_i/M_{i-1} = \langle \bar{m}_i \rangle$ son de longitud finita. 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 $(I)_0 = \operatorname{Spec}(A/I) = \{x_1, \ldots, x_r\}$. 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 $l_{A_i}(\mathfrak{m}_i^r/\mathfrak{m}_i^{r-1}) = \dim_{A_i/\mathfrak{m}_i}(\mathfrak{m}_i^r/\mathfrak{m}_i^{r-1}) < \infty$.

□

52. 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.

53. Corolario: *Un anillo es de longitud finita si y sólo si es noetheriano de dimensión de Krull nula.*

Demostración. Es consecuencia inmediata de 0.3.51. □

54. Corolario: *Sea A un anillo de longitud finita. Entonces, A es producto directo de un finito de anillos locales de longitud finita. Explícitamente,* $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$*, 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 0.3.18. □

55. Corolario: *Sea A un anillo de longitud finita. A es producto directo de cuerpos si y sólo 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. □

56. Corolario: *Sea A un anillo de longitud finita. A es íntegro si y sólo si es un cuerpo.*

Demostración. Es consecuencia inmediata del corolario anterior.

□

57. 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 0.2.124, f^* es de imagen densa. Como $\operatorname{Spec} A$ es igual a un número finito de puntos cerrados, entonces f^* es epiyectiva.

□

58. Definición: Diremos que una k-álgebra A, es una k-álgebra finita, si A es un k-espacio vectorial de dimensión finita.

59. 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.

60. 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 sólo 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.*

61. Definición: 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

$$\text{Nº punt. de } X \text{ cont. mult. y grad.} = \dim_k A = \sum_i \dim_k A_{x_i} = \sum_i l_A(A_{x_i}) \cdot \dim_k A/\mathfrak{m}_{x_i} = \sum_{x_i \in X} m_{x_i}(X) \cdot \operatorname{gr}_k(x_i)$$

62. Ejercicio: Sea $A = \mathbb{R}[x]/((x^2+1)^2(x-1)(x-2)^3)$. Calcular el espectro primo de A, el número de puntos de $\operatorname{Spec} A$, multiplicidades y grados.

0.3.5. Clasificación de los 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 sólo una diferencia en la terminología usada. Así, por ejemplo, un grupo abeliano es finito generado si y sólo 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.

63. 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

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ E & \xrightarrow{T'} & E \end{array}$$

64. Proposición: *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y sólo 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. □

65. Proposición: *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y sólo 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 $\tau\colon E_T \to E_{T'}$ 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 $\tau(p(x) \cdot e) = p(x) \cdot \tau(e)$.

Para el recíproco se razona de modo similar. □

Sigamos con la teoría general.

66. 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.

67. 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.

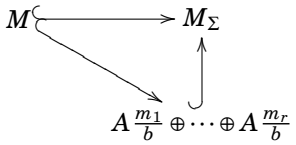
Se dice que un módulo M es libre de torsión si $T(M) = 0$, se dice que es de torsión si $T(M) = M$.

68. Ejemplo: Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})$.

$$\begin{aligned} T(\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})) &= \{(n, \bar{m}) \in \mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z}) \mid \text{Existe } r \in \mathbb{Z}\setminus\{0\}, \text{ tal que } r(n, \bar{m}) \\ &= (rn, \bar{r}m) = 0\} = \{(0, \bar{m}) \mid \bar{m} \in \mathbb{Z}/4\mathbb{Z}\} \simeq \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

69. 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 $M = \langle m_1, \dots, m_n \rangle$ y el morfismo de localización $M \hookrightarrow M_\Sigma$ es inyectivo. Evidentemente $\frac{m_1}{1}, \dots, \frac{m_n}{1}$ es un sistema generador del Σ-espacio vectorial M_Σ. Reordenado, podemos suponer que $\frac{m_1}{1}, \dots, \frac{m_r}{1}$ 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



□

70. 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).

71. 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 0.3.69. 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 0.3.70 $M = (L' \cap M) \oplus \pi(M)$. En conclusión, M es libre. □

72. 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. En efecto, 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. El epimorfismo de paso al cociente $M \to M/T(M)$ tiene sección, porque $M/T(M)$ es libre, luego $M \simeq T(M) \oplus (M/T(M))$. 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.

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 $M = \langle m_1, \dots, m_n \rangle$, y $a_i \in A\setminus\{0\}$ cumplen que $a_i m_i = 0$, entonces $0 \neq a_1 \cdots a_n \in \operatorname{Anul}(M)$.

73. Lema: *Sea A un dominio de ideales principales y M un A-módulo anulado por pq, siendo p y q primos entre sí. Entonces M descompone en suma directa de un módulo anulado por p y otro submódulo anulado por q, en concreto*

$$M = \operatorname{Ker} p \oplus \operatorname{Ker} q$$

donde definimos $p\colon M \to M$, $m \mapsto pm$ $q\colon M \to M$, $m \mapsto qm$.

Demostración. De acuerdo con la identidad de Bézout existen $\lambda, \mu \in A$ tales que

$$\lambda p + \mu q = 1$$

Por tanto, cada $m \in M$ cumple $\lambda pm + \mu qm = m$, donde $\lambda pm \in \operatorname{Ker} q$ y $\mu qm \in \operatorname{Ker} p$. Por consiguiente $M = \operatorname{Ker} p + \operatorname{Ker} q$.

Sólo nos falta probar que $\operatorname{Ker} p \cap \operatorname{Ker} q = 0$. Si $m \in \operatorname{Ker} p \cap \operatorname{Ker} q$ entonces $m = \lambda pm + \mu qm = 0 + 0 = 0$.

□

74. Segundo teorema de descomposición: *Sea A un dominio de ideales principales. Sea M un A-módulo de ideal anulador aA y $a = p_1^{n_1} \cdots p_s^{n_s}$ la descomposición de a en factores irreducibles. Entonces M descompone de modo único en suma directa de submódulos M_i de anuladores respectivos $p_i^{n_i}A$, explícitamente*

$$M = \operatorname{Ker} p_1^{n_1} \oplus \cdots \oplus \operatorname{Ker} p_s^{n_s}$$

Demostración. Por el lema anterior,

$$M = \operatorname{Ker} p_1^{n_1} \oplus \operatorname{Ker}(p_2^{n_2} \cdots p_s^{n_s}) = \operatorname{Ker} p_1^{n_1} \oplus \cdots \oplus \operatorname{Ker} p_s^{n_s}$$

Como el ideal anulador de una suma directa es el mínimo común múltiplo de los anuladores de los sumandos, tendremos que si $p_i^{n_i'}A$ son los anuladores de los $\operatorname{Ker} p_i^{n_i}$, entonces el anulador de M es $p_1^{n_1'} \cdots p_s^{n_s'}A$. Por tanto, $p_i^{n_i} = p_i^{n_i'}$ y tenemos que efectivamente el ideal anulador de $\operatorname{Ker} p_i^{n_i}$ es $p_i^{n_i}$. Obviamente, si $M = M_1 \oplus \cdots \oplus M_s$, con M_i de anulador $p_i^{n_i}$, entonces $M_i \subseteq \operatorname{Ker} p_i^{n_i}$ y por tanto $M_i = \operatorname{Ker} p_i^{n_i}$.

□

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 $M \xrightarrow{a\cdot=\bar{a}\cdot} M$ 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 M es un A-módulo finito generado de torsión, entonces

$$M_x = (\operatorname{Ker} p_1^{n_1} \oplus \cdots \oplus \operatorname{Ker} p_s^{n_s})_x = \begin{cases} 0 & \text{si } \mathfrak{m}_x \neq (p_i), \text{ para todo } i \\ \operatorname{Ker} p_i^{n_i} & \text{si } \mathfrak{m}_x = (p_i) \end{cases}$$

Luego si $\{x_1, \ldots, x_r\}$ son los puntos cerrados del soporte de M, $M = M_{x_1} \oplus \cdots \oplus M_{x_r}$.

75. Proposición: *Dos módulos finito generados sobre un dominio de ideales principales son isomorfos si y sólo 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.

□

76. 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.

77. Proposición: *Sea A un anillo noetheriano. Un A-módulo M es de presentación finita si y sólo si M es finito generado.*

Demostración. Supongamos que $M = \langle m_1, \ldots, m_n \rangle$ es un A-módulo finito generado. Consideremos el epimorfismo $\pi\colon A^n \to M$, $\pi((a_i)) := \sum_i a_i m_i$. $\operatorname{Ker} \pi = \langle n_1, \ldots, n_m \rangle$ es finito generado porque es un submódulo del módulo noetheriano A^n, luego M es de presentación finita. □

78. 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.

79. 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 $\{e_1, \ldots, e_m\}$, $\{e'_1, \ldots, e'_n\}$ en A^m y A^n, de modo que $\phi(e_i) = \lambda_i e'_i$, para $1 \leq i \leq m$.*

Demostración. Sea (a_{ij}) la matriz asociada a ϕ, en las bases estándar $\{u_1, \ldots, u_m\}$, $\{u'_1, \ldots, u'_n\}$ de A^m y A^n. Si en vez de $\{u_1, \ldots, u_m\}$, consideramos la base que se obtiene permutando dos vectores de $\{u_1, \ldots, u_m\}$, 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 $\{u'_1, \ldots, u'_n\}$, la matriz de ϕ se obtiene permutando las correspondientes filas de (a_{ij}). Si en vez de $\{u_1, \ldots, u_m\}$, consideramos la base $\{u_1, \ldots, \overset{i}{u_i - a_j u_j}, \ldots, u_m\}$, 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 $\{u'_1, \ldots, u'_m\}$, consideramos la base $\{u'_1, \ldots, \overset{i}{u'_i - a_j u'_j}, \ldots, u'_n\}$, 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}. 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.

□

80. 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 $A/(p^i)$.

81. 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,

$$M = \mathrm{Coker}\,\phi = [Ae_1 \oplus \cdots \oplus Ae_n]/[(\lambda_1)e_1 \oplus \dots (\lambda_m)e_m \oplus 0 \oplus \cdots \oplus 0] = A/(\lambda_1) \oplus \cdots \oplus A/(\lambda_m) \oplus A \oplus \cdots \oplus A$$

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 $\mathrm{Ker}\,p^i = (\bar{p}^{r-i})$, para $i \leq r$, y $\mathrm{Ker}\,p^i = (\bar{1})$, para $i \geq r$. Por tanto, $\mathrm{Ker}\,p^i/(\mathrm{Ker}\,p^{i-1} + p \cdot \mathrm{Ker}\,p^{i+1}) = 0$ si $i \neq r$ y $\mathrm{Ker}\,p^r/(\mathrm{Ker}\,p^{r-1} + p \cdot \mathrm{Ker}\,p^{r+1}) = \langle \bar{1} \rangle$ (que es un A/pA espacio vectorial de dimensión 1).

Ahora en general, $m_i = \dim_{A/pA} \mathrm{Ker}\,p^i/(\mathrm{Ker}\,p^{i-1} + p \cdot \mathrm{Ker}\,p^{i+1})$. □

82. Teorema de clasificación : *Sea A un dominio de ideales principales y M un A-módulo finito generado. Existe un isomorfismo de A-módulos*

$$M \simeq (A \oplus \overset{r}{\dots} \oplus A) \oplus (\bigoplus_{i,j} A/p_i^{n_{i,j}}A)$$

donde los $p_{i,j} \in A$ son irreducibles y r, $n_{i,j}$ y p_i están unívocamente determinados por M.

Demostración. Es un consecuencia directa de los tres teoremas de descomposición. □

83. Definición : A las potencias $p_i^{n_{i,j}}$ del teorema de clasificación se les denomina divisores elementales de M.

84. Corolario : *Dos módulos finito generados son isomorfos si y sólo si tienen el mismo rango y los mismos divisores elementales.*

85. Ejercicio : Probar que en el caso de que $r = 0$ entonces $\mathrm{Anul}(M) = m.c.m.\{p_i^{n_{i,j}}\}_{i,j} A$.

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 $\{e'_1,\dots,e'_m\}$ y $\{e_1,\dots,e_n\}$ 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:

86. 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 $i>n$ seguiremos la convención $F_i(M)=(1)$ y si $m<i\leq n$ 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: Consideremos otra base $\{\bar e_1,\dots,\bar e_m\}$ 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 $\{e'_1,\dots,e'_m\}$ 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 $A_x^m \xrightarrow{\psi_x} A_x^n \to M_x\to 0$ es exacta. La matriz asociada a ψ, es la misma que la asociada a ψ_x, por tanto $(F_i(M))_x=F_i(M_x)$.

87. 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 $\phi_i=0$.

88. 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 sólo 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 sólo si lo son localmente. Por tanto, el teorema es local y podemos suponer que A es local de ideal maximal $\mathfrak{m}=(p)$.

Por los teoremas de descomposición sabemos que

$$M\simeq A^s\oplus A/(p^{n_1})\oplus\cdots\oplus A/(p^{n_r})$$

con $n_1\geq\cdots\geq n_r>0$. Por tanto, tenemos la presentación libre

$$A\oplus\overset{r}{\dots}\oplus A \xrightarrow{(p^{n_1}\cdot,\dots,p^{n_r}\cdot)\oplus 0} A\oplus\overset{r}{\dots}\oplus A\oplus A^s\to M\to 0$$

Ahora ya, es una sencilla comprobación que $\phi_i=0$ para $i\leq s$, $\phi_i=p^{n_i}$, para $i>s$. □

89. Observaciones:

1. Por el cálculo efectuado en la demostración del teorema anterior, que 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 0.7.7).

90. Teorema de clasificación de endomorfismos: *Dos endomorfismos de un k-espacio vectorial de dimensión finita E son equivalentes si y sólo 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: Obviamente $\mathrm{Im}(x*-T) \subseteq \mathrm{Ker}\,\pi$. Veamos que $\mathrm{Ker}\,\pi \subseteq \mathrm{Im}(x*-T)$: Dado $\sum_i e_i x^i \in \mathrm{Ker}\,\pi$, es fácil probar que módulo $\mathrm{Im}(x*-T)$ es equivalente a $\sum_i T^i(e_i)$, que es nulo por hipótesis, luego $\sum_i e_i x^i \in \mathrm{Im}(x*-T)$.

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 $x\cdot \mathrm{Id} - (a_{ij})$.

91. 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.

92. 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 $xId-(a_{ij})$.

0.4. 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, cuyos elementos 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 verifique 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 verifica $F(f \circ g) = F(g) \circ F(f)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Un morfismo $f\colon M \to M'$ induce, para cada objeto $N \in \mathscr{C}$, 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 morfismo $f\colon M \to M'$ induce, para cada objeto $N \in \mathscr{C}$, 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 $\theta\colon F \to F'$, es dar para cada objeto M de $\mathscr{C}$ 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 los morfismos de F en F'.

4. Definición: Se dice que dos categorías $\mathscr{C}$ y $\mathscr{C}'$ son equivalentes (resp. anti-equivalentes) 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 categorial 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 $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{conj}$ un funtor covariante. 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 sólo 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

$$\begin{array}{ccc} \mathrm{Hom}_{\mathscr{C}}(M,M) & \xrightarrow{\theta_M} & F(M) \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle F(f)} \\ \mathrm{Hom}_{\mathscr{C}}(M,N) & \xrightarrow{\theta_N} & F(N) \end{array} \qquad \begin{array}{ccc} \mathrm{Id}_M & \xmapsto{\theta_M} & g \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle F(f)} \\ f & \xmapsto{\theta_N} & F(f)(g) \end{array}$$

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 $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{conj}$ un funtor contravariante. 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 sólo 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 $\operatorname{Spec} A$. En conclusión, los objetos de $\mathscr{C}_{Var}$, son $\operatorname{Spec} A$, y los morfismos $\operatorname{Spec} B \to \operatorname{Spec} A$ son los morfismos de k-álgebras $A \to B$.

Dado $X = \operatorname{Spec} A$, denotaremos por $X^{\cdot}$ el funtor sobre $\mathscr{C}_{Var}$ en la categoría de conjuntos, definido para cada $Y = \operatorname{Spec} B \in \mathscr{C}_{Var}$, por

$$X^{\cdot}(Y) := \operatorname{Hom}_{\mathscr{C}_{Var}}(Y, X) = \operatorname{Hom}_{k-alg}(A, B)$$

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 $\operatorname{Spec} A = X$: $X^{\cdot}(\operatorname{Spec} k) = \operatorname{Hom}_{k-alg}(A, k) = \{\text{puntos } k\text{-racionales de } \operatorname{Spec} A\}$. Supongamos que

$$X = \operatorname{Spec} A, \quad A = k[x_1, \ldots, x_n]/(p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n))$$

Entonces

$$X^{\cdot}(\operatorname{Spec} B) = \operatorname{Hom}_{\mathscr{C}_{Var}}(\operatorname{Spec} B, X) = \operatorname{Hom}_{k-\text{álg.}}(A, B)$$
$$= \left\{ \begin{array}{l} \text{Soluciones con valores en } B \text{ del sistema} \\ \text{de ecuaciones } p_1(x_1, \ldots, x_n) = \cdots = p_r(x_1, \ldots, x_n) = 0 \end{array} \right.$$

Así pues, $X^{\cdot}$ (con valores en $\operatorname{Spec} B$) son las soluciones del sistema algebraico anterior (con valores en B) que es la interpretación geométrica que queríamos dar a $\operatorname{Spec} A = X$.

Con la noción de funtor de puntos podemos hablar de $\operatorname{Spec} A$ en términos de su "conjunto de puntos", y los morfismos quedan reducidos a aplicaciones (funtoriales) entre conjuntos.

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 $A, B \in \mathscr{C}$, $\operatorname{Hom}_{\mathscr{C}}(A, B)$ es un grupo abeliano y para todo $f \in \operatorname{Hom}_{\mathscr{C}}(B, C)$, $i \in \operatorname{Hom}_{\mathscr{C}}(Z, A)$ y $g, h \in \operatorname{Hom}_{\mathscr{C}}(A, B)$ 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 $\pi_1 \colon A \times B \to A$, $\pi_2 \colon A \times B \to B$ de modo que

$$\operatorname{Hom}_{\mathscr{C}}(C, A \times B) \to \operatorname{Hom}_{\mathscr{C}}(C, A) \times \operatorname{Hom}_{\mathscr{C}}(C, B),\ f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$$

   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 $F \colon \mathscr{C} \rightsquigarrow \mathscr{C}'$ entre categorías aditivas, se dice que es aditivo si la aplicación $\operatorname{Hom}_{\mathscr{C}}(A, B) \to \operatorname{Hom}_{\mathscr{C}'}(F(A), F(B))$, $f \mapsto F(f)$ es un morfismo de grupos.

Una categoría abeliana es una categoría aditiva que cumple

1. Todo morfismo tiene núcleo y conúcleo. Es decir, dado $f \colon A \to B$ existen objetos, $\operatorname{Ker} f$ y $\operatorname{Coker} f$, y morfismos $\operatorname{Ker} f \to A$, $B \to \operatorname{Coker} f$, de modo que las sucesiones de grupos $0 \to \operatorname{Hom}_{\mathscr{C}}(C, \operatorname{Ker} f) \to \operatorname{Hom}_{\mathscr{C}}(C, A) \to \operatorname{Hom}_{\mathscr{C}}(C, B)$, $0 \to \operatorname{Hom}_{\mathscr{C}}(\operatorname{Coker} f, C) \to \operatorname{Hom}_{\mathscr{C}}(B, C) \to \operatorname{Hom}_{\mathscr{C}}(A, C)$ son exactas, para todo C.

2. Todo morfismo inyectivo $f \colon A \to B$ es el núcleo de $B \to \operatorname{Coker} f$ ($f \colon A \to B$ se dice que es inyectivo si $\operatorname{Hom}_{\mathscr{C}}(C, A) \to \operatorname{Hom}_{C}(C, B)$ es una aplicación inyectiva para todo C).

3. Todo morfismo epiyectivo $f \colon A \to B$ es el conúcleo de $\operatorname{Ker} f \to A$ ($f \colon A \to B$ se dice epiyectivo si $\operatorname{Hom}_{\mathscr{C}}(B, C) \to \operatorname{Hom}_{C}(A, C)$ es una aplicación inyectiva para todo C).

En las categorías abelianas como en la categoría de módulos se habla de sucesiones exactas (véase 0.3.10).

11. Definición: Diremos que un funtor covariante $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$ 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 $\mathscr{C} \overset{G}{\rightsquigarrow} \mathscr{C}'$ 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.

0.5. 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 $\beta: M \times N \to P$ es A-bilineal si

$$\begin{array}{l} \beta(m+m',n) = \beta(m,n) + \beta(m',n) \\ \beta(m,n+n') = \beta(m,n) + \beta(m,n') \\ \beta(am,n) = a\beta(m,n) \\ \beta(m,an) = a\beta(m,n) \end{array}$$

El conjunto de las aplicaciones A-bilineales de $M \times N$ en P se denota $\mathrm{Bil}_A(M,N;P)$.

Con mayor generalidad puede el lector definir aplicación A-multilineal de $M_1 \times \overset{n}{\cdots} \times M_n$ en P. El conjunto de las aplicaciones A-multilineales de $M_1 \times \overset{n}{\cdots} \times M_n$ en P se denota $\mathrm{Multl}_A(M_1,\overset{n}{\ldots},M_n;P)$.

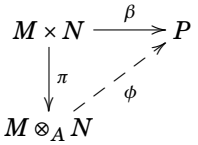
La condición de que una aplicación $\beta\colon M \times N \to P$ sea A-bilineal implica que la aplicación $\beta_m : N \to P$, $\beta_m(n) = \beta(m,n)$, es un morfismo de A-módulos para cada elemento $m \in M$. Tenemos así, un morfismo natural $\mathrm{Bil}_A(M,N;P) \to \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, $\beta \mapsto \tilde{\beta}$, 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: *La aplicación $\beta\colon M \times N \to P$ es una aplicación bilineal si y sólo 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 0.5.3,

$$\mathrm{Hom}_A(M \otimes_A N,P) = \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P)),\ f \mapsto \tilde{f},\ \textit{donde}\ \tilde{f}(m)(n) := f(m \otimes n)$$

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.

□

Así pues, este teorema nos dice que definir un morfismo de A-módulos $\phi\colon M \otimes N \to P$, es asignar a cada $m \otimes n \in M \otimes_A N$ un elemento $\phi(m \otimes n)$ 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 $M_1,\ldots,M_n$ de A-módulos, obteniéndose un A-módulo $M_1 \otimes_A \cdots \otimes_A M_n$ con la propiedad universal

$$\mathrm{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_n,P) = \mathrm{Multl}_A(M_1,\overset{n}{\ldots},M_n;P)$$

Para definir un morfismo de A-módulos $f : M_1 \otimes_A \cdots \otimes_A M_n \to P$, bastará definir las imágenes $f(m_1 \otimes \cdots \otimes m_n)$ de modo que

$$f(m_1 \otimes \cdots \otimes a_i m_i + n_i \otimes \cdots) = a_i f(m_1 \otimes \cdots \otimes m_i \otimes \cdots) + f(m_1 \otimes \cdots \otimes n_i \otimes \cdots)$$

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. $(\oplus_i M_i) \otimes_A N = \oplus_i (M_i \otimes N)$, $(m_i) \otimes n \mapsto (m_i \otimes n)$.

Demostración. Dejamos al lector que defina los morfismos inversos. Veamos, sólo, que el morfismo de 1. está bien definido: Para cada p el morfismo $M \otimes_A N \times p \to M \otimes_A (N \otimes_A P)$, $(m \otimes n) \times p \mapsto m \otimes (n \otimes p)$ está bien definido. Luego tenemos un morfismo $(M \otimes_A N) \times P \to M \otimes_A (N \otimes_A P)$, 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 0.4.6, $(M \otimes_A N) \otimes_A P = M \otimes_A (N \otimes_A P)$.

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. Basta comprobar que 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 0.4.9

$$\mathrm{Hom}_A(M^\bullet, \mathrm{Hom}_A(N,P)) = \mathrm{Bil}_A(M^\bullet, N; P) = \mathrm{Hom}_A(M^\bullet \otimes_A N, P)$$

es una sucesión exacta para todo A-módulo P. De nuevo 0.4.9 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: El producto es el morfismo $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$, $(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'$ inducido por el correspondiente morfismo $B \otimes_A C \otimes B \otimes_A C \to B \otimes_A C$. 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,

$$\mathrm{Spec}_{rac}(A \otimes_k B) = \mathrm{Hom}_{k-alg}(A \otimes_k B, k) = \mathrm{Hom}_{k-alg}(A,k) \times \mathrm{Hom}_{k-alg}(B,k) = \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B$$

□

Este hecho justificará la definición $\mathrm{Spec} A \times \mathrm{Spec} A' := \mathrm{Spec}(A \otimes_{\mathbb{C}} A')$ (advertencia: $\mathrm{Spec} A \times \mathrm{Spec} A'$ no denota producto cartesiano de los conjuntos $\mathrm{Spec} A$ y $\mathrm{Spec} A'$) 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 $i : A \to A \otimes_k B$, $i(a) = a \otimes 1$ es

$$\begin{array}{rccc} i^* : \mathrm{Spec}_{rac}(A \otimes_k B) = \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B & \to & \mathrm{Spec}_{rac} A \\ (\alpha, \beta) & \mapsto & \alpha \end{array}$$

En efecto, vía las aplicaciones $\mathrm{Hom}_{k-alg}(A,k) \times \mathrm{Hom}_{k-alg}(B,k) = \mathrm{Hom}_{k-alg}(A \otimes_k B, k) \xrightarrow{i^*} \mathrm{Hom}_{k-alg}(A,k)$, (ϕ_1, ϕ_2) se aplica en $(\phi_1 \otimes \phi_2)_{|1 \otimes A} = \phi_1$.

El morfismo inducido en los espectros racionales por $f : A \otimes_k A \to A$, $f(a \otimes a') = aa'$ es

$$\begin{array}{rcl} \mathrm{Spec}_{rac} A & \to & \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} A = \mathrm{Spec}_{rac}(A \otimes_k A) \\ \alpha & \mapsto & (\alpha, \alpha) \end{array}$$

En efecto, vía las aplicaciones $\mathrm{Hom}_{k-alg}(A,k) \xrightarrow{f^*} \mathrm{Hom}_{k-alg}(A \otimes_k A, k) = \mathrm{Hom}_{k-alg}(A,k) \times \mathrm{Hom}_{k-alg}(A,k)$, ϕ se aplica en $((\phi \circ f)_{|A \otimes 1}, (\phi \circ f)_{|A \otimes 1}) = (\phi, \phi)$.

13. Proposición: *Sean B y C A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc} \mathrm{Hom}_A(B,C) & = & \mathrm{Hom}_C(B_C, C) \\ \phi & \longmapsto & \phi' : \phi'(b \otimes c) = \phi(b) \cdot c \\ \phi'_{|B} & \longmapsto & \phi' \end{array}$$

0.5.1. Álgebra tensorial, simétrica y exterior de un módulo

Dado un A-módulo M, diremos que $T^nM := M \otimes_A \overset{n}{\dots} \otimes_A M$ es el producto tensorial n-ésimo de M. Seguiremos las convenciones $T^0M = A$ y $T^1M = M$.

Si M es un A-módulo libre de base $\{e_i\}_{i\in I}$, entonces T^nM es un A-módulo libre de base $\{e_{i_1} \otimes \cdots \otimes e_{i_n}\}_{i_1,\dots,i_n\in I}$.

Podemos pensar los elementos de T^nM como ciertas aplicaciones multilineales. Con precisión, sea $M^* = \mathrm{Hom}_A(M,A)$, tenemos el morfismo natural

$$\phi\colon T^nM \to \mathrm{Multl}_A(M^*,\overset{n}{\dots},M^*,A),\ \ \phi(m_1 \otimes \overset{n}{\dots} \otimes m_n)(w_1,\dots,w_n) := w_1(m_1)\cdots w_n(m_n)$$

Si M es un A-módulo libre finito generado entonces $T^nM = \mathrm{Multl}_A(M^*,\overset{n}{\dots},M^*;A)$.

14. Notación: 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.

16. Definición: Se dice que un álgebra graduada $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ es conmutativa si $r_i \cdot r_j = r_j \cdot r_i$, para todo $r_i \in R_i$, $r_j \in R_j$.

Los anillos de polinomios, $k[x_1,\dots,x_n]$, 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. Se cumple un isomorfismo natural*

$$\mathrm{Hom}_{A-grd}(T^{\cdot}M,R) = \mathrm{Hom}_A(M,R_1)$$

Demostración. Dado un morfismo $\phi\colon T^{\cdot}M \to R$, 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.

□

20. Proposición: *Se cumple*

1. $(T^{\cdot}_AM) \otimes_A B = T^{\cdot}_B(M \otimes_A B)$.
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 $T^{\cdot}M$-submódulo de $T^{\cdot}M$ generado por $N \subset T^{\cdot}M$, es decir, un sistema generador de $\langle N\rangle$ como A-módulo es* $\{m_1 \otimes \dots \otimes \overset{i}{n} \otimes \dots \otimes m_r \mid n \in N, m_k \in M, i,r \in \mathbb{N}\}$.

Demostración. 1. Se deduce de las igualdades

$$\begin{aligned}\mathrm{Hom}_{B-grd}(T^{\cdot}_B(M \otimes_A B),R) &= \mathrm{Hom}_B(M \otimes_A B,R_1) = \mathrm{Hom}_A(M,R_1)\\ &= \mathrm{Hom}_{A-grd}(T^{\cdot}_AM,R) = \mathrm{Hom}_{B-grd}(T^{\cdot}_AM \otimes_A B,R)\end{aligned}$$

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^nM el submódulo

$$M'_n = \langle m_1\otimes\cdots\otimes \overset{i}{m}_i\otimes\cdots\otimes \overset{j}{m}_j\otimes\cdots\otimes m_n - m_1\otimes\cdots\otimes \overset{i}{m}_j\otimes\cdots\otimes \overset{j}{m}_i\otimes\cdots\otimes m_n \mid m_k\in M\,\forall i,j,k\rangle$$

21. Definición: Diremos que $S^nM = T^nM/M'_n$ es el producto tensorial simétrico n-ésimo del A-módulo M. Diremos que $S^{\cdot}M = \overset{\infty}{\underset{i=0}{\oplus}} S^iM$ es el álgebra simétrica de M. Denotaremos $S^{\cdot}M = S^{\cdot}_AM$ cuando queramos precisar quién es el anillo.

Se dice que una aplicación multilineal $\beta\colon M\times \overset{n}{\ldots}\times M \to M'$ es una aplicación multilineal simétrica de orden n de M en M' si

$$\beta(m_1,\ldots,m_n) = \beta(m_{\sigma(1)},\ldots,m_{\sigma(n)})$$

para todo $\sigma\in S_n$. Denotemos $\mathrm{Sim}_A(M,\overset{n}{\ldots},M;M')$ 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* $\mathrm{Hom}_A(S^nM,M') = \mathrm{Sim}_A(M,\overset{n}{\ldots},M;M')$.

Es claro que $M'_n\cdot T^rM \subseteq M'_{n+s}$. 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 $m_1\otimes\overset{n}{\ldots}\otimes m_n$ 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 $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ 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 $S^{\cdot}A^n \simeq A[x_1,\ldots,x_n]$. Si E es un A-módulo libre de base $\{e_1,\ldots,e_n\}$, entonces S^rE es un A-módulo libre de base $\{e_{i_1}\cdots e_{i_r}\}_{i_1\le\cdots\le i_r}$.*

Demostración. $\mathrm{Hom}_{A-grd}(S^{\cdot}A^n,R) = \mathrm{Hom}_A(A^n,R_1) = (R_1)^n = \mathrm{Hom}_{A-grd}(A[x_1,\ldots,x_n],M)$ para toda A-álgebra graduada conmutativa, luego $S^{\cdot}A^n \simeq A[x_1,\ldots,x_n]$. Por tanto, S^rA^n es isomorfo al A-módulo formado por los polinomios homogéneos de grado r de $A[x_1,\ldots,x_n]$, que es un A-módulo libre de base $\{x_{i_1}\cdots x_{i_r}\}_{i_1\le\cdots\le i_r}$. Obviamente, $\{e_{i_1}\cdots e_{i_r}\}_{i_1\le\cdots\le i_r}$ 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 $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ y $R' = \underset{n\in\mathbb{Z}}{\oplus} R'_n$ son A-álgebras graduadas, entonces la A-álgebra $R\otimes_AR'$ es graduada con la graduación

$$(R\otimes_AR')_n = \underset{i+j=n}{\oplus} R_i\otimes_AR'_j$$

El producto tensorial $R\otimes_AR'$ 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* $S^n(M\oplus M')=\underset{i+j=n}{\oplus} S^iM\otimes_A S^jM'$.
2. $(S^{\cdot}_AM)\otimes_A B=S^{\cdot}_B(M\otimes_A B)$.
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* $S^{\cdot}M$*-submódulo de* $S^{\cdot}M$ *generado por* $N\subset S^{\cdot}M$, *es decir,* $\langle N\rangle=N\cdot S^{\cdot}M$.

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 0.5.20. □

La composición del morfismo $S^nM\to T^nM$, $m_1\cdots m_n\mapsto\sum_{\sigma\in S_n}m_{\sigma(1)}\otimes\cdots\otimes m_{\sigma(n)}$ con el epimorfismo natural $T^nM\to S^nM$ es una homotecia de factor $n!$. Podemos pensar los elementos de S^nM como ciertas aplicaciones multilineales simétricas. Con precisión, sea $M^*=\mathrm{Hom}_A(M,A)$, tenemos el morfismo natural

$$\phi\colon S^nM\to\mathrm{Sim}_A(M^*,\overset{n}{\ldots},M^*,A),\quad \phi(m_1\cdots m_n)(w_1,\ldots,w_n):=\sum_{\sigma\in S_n}w_{\sigma(1)}(m_1)\cdots w_{\sigma(n)}(m_n).$$

Si $n!$ es invertible en A y M es un A-módulo libre finito generado entonces $S^nM=\mathrm{Sim}_A(M^*,\overset{n}{\ldots};M^*;A)$.

Ahora, nuestro objetivo es definir el álgebra exterior de un módulo.

Consideremos en T^nM el submódulo

$$M''_n=\langle m_1\otimes\overset{n}{\ldots}\otimes m_n\in T^nM\mid m_i=m_j\text{ para dos índices }i\neq j\rangle$$

26. Definición: Diremos que $\Lambda^nM=T^nM/M''_n$ es el álgebra exterior n-ésima del A-módulo M. Diremos que $\Lambda^{\cdot}M=\overset{\infty}{\underset{i=0}{\oplus}}\Lambda^iM$ es el álgebra exterior de M. Denotaremos $\Lambda^{\cdot}M=\Lambda^{\cdot}_AM$ cuando queramos precisar quién es el anillo.

Se dice que una aplicación multilineal $w_n\colon M\times\overset{n}{\ldots}\times M\to M'$ 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 del álgebra exterior n-ésima de un A-módulo: *De la definición es inmediato que* $\mathrm{Hom}_A(\Lambda^nM,M')=\mathrm{Hem}_A(M,\overset{n}{\ldots},M;M')$.

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 $M''_n\cdot T^rM\subseteq M''_{n+s}$. 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 Λ^nM 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 $w_n\in\Lambda^nM$ y $w_r\in\Lambda^rM$, 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 $R = \oplus_{n\in\mathbb{Z}} R_n$ un álgebra graduada tal que $r_1 \cdot r_1 = 0$ para todo $r_1 \in R_1$. 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* $\Lambda^n(M \oplus M') = \oplus_{i+j=n} \Lambda^i M \otimes_A \Lambda^j M'$.
2. $(\Lambda^{\cdot}_A M) \otimes_A B = \Lambda^{\cdot}_B (M \otimes_A B)$.
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 $\Lambda^{\cdot} M$-submódulo de $\Lambda^{\cdot} M$ generado por $N \subset \Lambda^{\cdot} M$, es decir, $\langle N \rangle = N \wedge \Lambda^{\cdot} M$.*

Demostración. Se demuestra igual que la proposición 0.5.25. □

31. Proposición: *Sea E un A-módulo libre de base $\{e_1, \ldots, e_n\}$. Entonces, $\Lambda^r E$ 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 $\Lambda^r E = 0$, para $r > n$.*

Demostración. Si $n = 1$, es claro que $\Lambda^{\cdot} E = \Lambda^{\cdot} A e_1 = A \oplus A \cdot e_1$. Por inducción sobre el rango de E, se cumple que

$$\begin{aligned}\Lambda^{\cdot} E = \Lambda^{\cdot}(Ae_1 \oplus \overset{r}{\cdots} Ae_n) &= \Lambda^{\cdot}(Ae_1) \otimes \Lambda^{\cdot}(Ae_2 \oplus \overset{r}{\cdots} Ae_n) = \Lambda^{\cdot}(Ae_1) \otimes \overset{r}{\cdots} \otimes \Lambda^{\cdot} Ae_n \\ &= (A \oplus Ae_1) \otimes \overset{r}{\cdots} \otimes (A \oplus Ae_n)\end{aligned}$$

Luego, $\Lambda^r E = \oplus_{i_1 < \cdots < i_r} A \cdot e_{i_1} \wedge \overset{r}{\cdots} \wedge e_{i_r}$, para $r \le n$ y $\Lambda^r E = 0$, para $r > n$. □

La composición del morfismo $\Lambda^n M \to T^n M$, $m_1 \wedge \cdots \wedge m_n \mapsto \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \cdot m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)}$ con el epimorfismo natural $T^n M \to \Lambda^n M$, es una homotecia de factor $n!$. Podemos pensar los elementos de $\Lambda^n M$ como ciertas aplicaciones multilineales hemisimétricas. Con precisión, sea $M^* = \mathrm{Hom}_A(M, A)$, tenemos el morfismo natural

$$\phi \colon \Lambda^n M \to \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*, A), \quad \phi(m_1 \wedge \overset{n}{\cdots} \wedge m_n)(w_1, \ldots, w_n) := \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \cdot w_{\sigma(1)}(m_1) \cdots w_{\sigma(n)}(m_n).$$

Si M es un A-módulo libre finito generado entonces $\Lambda^n M = \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*; A)$.

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 verifica que $\Lambda^n(T) \circ \Lambda^n(T') = \Lambda^n(T \circ T')$: $(\Lambda^n(T) \circ \Lambda^n(T'))(e_1 \wedge \cdots \wedge e_n) = \Lambda^n(T)(T'(e_1) \wedge \cdots \wedge T'(e_n)) = (T \circ T')(e_1) \wedge \cdots \wedge (T \circ T')(e_n) = \Lambda^n(T \circ T')(e_1 \wedge \cdots \wedge e_n)$.

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 $\{e_1,\dots,e_n\}$. Dada $\sigma\in S_n$, sea $\sigma: E\to E$ 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 $v_1,\cdots,v_n\in E$, con $v_i=\sum_j\lambda_{ij}e_j$, tendremos que

$$\begin{aligned}v_1\wedge\cdots\wedge v_n&=(\textstyle\sum_i\lambda_{1i}e_i)\wedge\cdots\wedge(\sum_i\lambda_{ni}e_i)=\sum_{i_1\neq\cdots\neq i_n}\lambda_{1i_1}\cdots\lambda_{ni_n}e_{i_1}\wedge\cdots\wedge e_{i_n}\\&=\sum_{\sigma\in S_n}\lambda_{1\sigma(1)}\cdots\lambda_{n\sigma(n)}\cdot e_{\sigma(1)}\wedge\cdots\wedge e_{\sigma(n)}=(\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\lambda_{1\sigma(1)}\cdots\lambda_{n\sigma(n)})\cdot e_1\wedge\cdots\wedge e_n\end{aligned}$$

Sea $\{e_1,\dots,e_n\}$ 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

$$\begin{aligned}&\det(a_{ij})e_1\wedge\cdots\wedge e_n=(\sum_j a_{1j}e_j)\wedge\cdots\wedge(\sum_j a_{nj}e_j)=\sum_k a_{1k}e_k\wedge(\sum_j a_{2j}e_j)\wedge\cdots\wedge(\sum_j a_{nj}e_j)\\&=a_{11}e_1\wedge(\sum_{j\neq1}a_{2j}e_j)\wedge\cdots\wedge(\sum_{j\neq1}a_{nj}e_j)+\cdots+a_{1n}e_n\wedge(\sum_{j\neq n}a_{2j}e_j)\wedge\cdots\wedge(\sum_{j\neq n}a_{nj}e_j)\\&=a_{11}A_1^1\cdot e_1\wedge\cdots\wedge e_n+\cdots+a_{1n}A_1^n\cdot e_n\wedge e_1\wedge\cdots\wedge e_{n-1}\\&=(\sum_j(-1)^j a_{1j}A_1^j)\cdot e_1\wedge\cdots\wedge e_n\end{aligned}$$

y hemos concluido. □

Sea $T: E\to E$ 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

$$b_{ij}=(-1)^{i+j}\frac{A_j^i}{\det(a_{ij})}$$

0.6. 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 0.5.8, 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 sólo 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 $m_1, \dots, m_r$ un sistema de generadores de M, obtenido por el lema de Nakayama (es decir, de modo que $\bar{m}_1, \dots, \bar{m}_r$ 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 $I = (a_1, \dots, a_r)$. 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 $\bar{m}_1, \dots, \bar{m}_r$ 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, $m_1, \dots, m_r$ es una base de M y M es libre. □

6. Teorema: *Un módulo finito generado es plano si y sólo 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 0.6.4. □

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 $m_1, \dots, m_n$ 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 sólo si lo es al tensarla por el módulo M.

11. 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 $x \in \operatorname{Spec} A$.*

Demostración. $1 \Rightarrow 2)$ Si M es fielmente plano, es plano. Además, la sucesión $0 \to N \to 0$ es exacta si y sólo 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

$$N \otimes_A M \xrightarrow{f\otimes 1} N' \otimes_A M \xrightarrow{f'\otimes 1} N'' \otimes_A M \qquad (**)$$

Igual que veíamos con la localización en la proposición 0.3.9, si M es plano entonces $\operatorname{Im} f \otimes_A M = \operatorname{Im}(f \otimes 1)$ y $\operatorname{Ker} f' \otimes_A M = \operatorname{Ker}(f' \otimes 1)$. Por tanto,

$$[(\operatorname{Ker} f' + \operatorname{Im} f)/\operatorname{Im} f] \otimes_A M = (\operatorname{Ker}(f' \otimes 1) + \operatorname{Im}(f \otimes 1))/\operatorname{Im}(f \otimes 1)$$

Así pues, tendremos que $(\operatorname{Ker} f' + \operatorname{Im} f)/\operatorname{Im} f = 0$ si y sólo si $(\operatorname{Ker}(f' \otimes 1) + \operatorname{Im}(f \otimes 1))/(\operatorname{Im} f \otimes 1) = 0$. Igualmente, $(\operatorname{Ker} f' + \operatorname{Im} f)/\operatorname{Ker} f' = 0$ si y sólo si $(\operatorname{Ker}(f' \otimes 1) + \operatorname{Im}(f \otimes 1))/\operatorname{Ker}(f' \otimes 1) = 0$. En conclusión, $(*)$ es exacta si y sólo 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 $\langle n \rangle \simeq A/\operatorname{Anul}(n)$. Sea $\mathfrak{m}_x \subset A$ un ideal maximal que contenga a $\operatorname{Anul}(n)$. El epimorfismo $A/\operatorname{Anul}(n) \to A/\mathfrak{m}_x$ induce el epimorfismo $A/\operatorname{Anul}(n) \otimes_A M \to A/\mathfrak{m}_x \otimes_A M$, 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. □

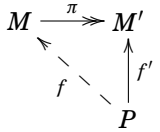
12. Definición: Diremos que un morfismo de anillos $f : A \to B$ es plano si B es un A-módulo plano. Diremos que un morfismo de anillos $f : A \to B$ es fielmente plano si B es un A-módulo fielmente plano.

13. Proposición: *Un morfismo $f : A \to B$ de anillos es fielmente plano si y sólo si es plano y el morfismo inducido en los espectros es epiyectivo.*

Demostración. La fielplatitud es una propiedad local, por el punto 2 de 0.6.11.

Por la fórmula de la fibra, el morfismo $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo si y sólo si $B_x/\mathfrak{p}_x B_x \neq 0$ para todo $x \in \operatorname{Spec} A$. Así pues, por la proposición 0.6.11, $f : A \to B$ es plano y el morfismo inducido en los espectros es epiyectivo si y sólo si f es fielmente plano. □

14. 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 0.4.8, 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.

15. Proposición: *Un A-módulo es proyectivo si y sólo 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, $\pi\colon A^{(I)} \to P$. Si consideramos el morfismo $\mathrm{Id}\colon P \to P$ sabemos que levanta a un morfismo $s\colon P \to A^{(I)}$, tal que $\pi \circ s = \mathrm{Id}$, por ser P proyectivo. Por el ejercicio 0.3.70, $A^{(I)} = \mathrm{Ker}\,\pi \oplus P$.

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 $\mathrm{Hom}_A(M \oplus M', -) = \mathrm{Hom}_A(M,-) \times \mathrm{Hom}_A(M',-)$ es fácil probar que una suma directa de módulos es un módulo proyectivo si y sólo si lo es cada sumando. En conclusión, M es proyectivo. □

16. 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. □

17. Proposición: *Los módulos proyectivos finito generados son módulos de presentación finita.*

Demostración. Sea P un A-módulo proyectivo finito generado y $\pi\colon A^n \to P$ un epimorfismo. Entonces, $A^n = P \oplus \mathrm{Ker}\,\pi$ y $\mathrm{Ker}\,\pi \simeq A^n/P$. Luego, $\mathrm{Ker}\,\pi$ es un A-módulo finito generado y P es de presentación finita. □

18. 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. □

19. 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*

$$\mathrm{Hom}_A(M,N)_S = \mathrm{Hom}_{A_S}(M_S, N_S)$$

Demostración. Si un A-módulo $L \simeq A^r$ es libre entonces $\mathrm{Hom}_A(L,N)_S = (N^r)_S = (N_S)^r = \mathrm{Hom}_{A_S}(L_S, N_S)$.

Por hipótesis tenemos una sucesión exacta $A^m \xrightarrow{\phi} A^n \to M \to 0$. Tomando $\mathrm{Hom}_A(-,N)$ obtenemos la sucesión exacta

$$0 \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(A^n,N) \xrightarrow{\phi^*} \mathrm{Hom}_A(A^m,N)$$

Localizando por S tenemos la sucesión exacta

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(M,N)_S & \longrightarrow & \mathrm{Hom}_A(A^n,N)_S & \longrightarrow & \mathrm{Hom}_A(A^m,N)_S \\ & & \| & & \| & & \| \\ 0 & \longrightarrow & \mathrm{Ker}\,\phi_S^* & \longrightarrow & \mathrm{Hom}_{A_S}(A_S^n, N_S) & \xrightarrow{\phi_S^*} & \mathrm{Hom}_{A_S}(A_S^m, N_S) \end{array}$$

Ahora bien, tomando $\mathrm{Hom}_{A_S}(-,N_S)$ en la sucesión exacta $A_S^m \to A_S^n \to M_S \to 0$, concluimos que $\mathrm{Ker}\,\phi_S^* = \mathrm{Hom}_{A_S}(M_S,N_S)$ y terminamos.

□

20. Teorema: *Un módulo P de presentación finita es proyectivo si y sólo si es localmente proyectivo (es decir, para todo $x \in \mathrm{Spec}\,A$, 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 sólo si para toda sucesión exacta $N^\bullet$ de A-módulos entonces la sucesión $\mathrm{Hom}_A(P,N^\bullet)$ es exacta. Con estas convenciones tenemos: P es proyectivo $\iff$ para toda sucesión exacta $N^\bullet$ de A-módulos $\mathrm{Hom}_A(P,N^\bullet)$ es exacta $\iff$ para toda sucesión exacta $N^\bullet$ de A-módulos $\mathrm{Hom}_A(P,N^\bullet)_x = \mathrm{Hom}_{A_x}(P_x, N_x^\bullet)$ es exacta para todo punto cerrado $x \in \mathrm{Spec}\,A$ $\iff$ 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 $(N'^\bullet)_x = N'^\bullet$). □

21. Teorema : *Las condiciones de ser plano, localmente libre y proyectivo son equivalentes para los módulos de presentación finita.*

Demostración. Si M es plano, por 0.6.6, 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 0.6.16, es plano. □

22. Proposición: *Un módulo M finito generado es proyectivo si y sólo si existe un recubrimiento finito $\{U_{a_i}\}$ por abiertos básicos de* Spec$A$*, de modo que M_{a_i} es un A_{a_i}-módulo libre.*

Demostración. Sea M proyectivo. Dado $x \in \mathrm{Spec}\, A$ existe un isomorfismo

$$A_x \oplus \cdots \oplus A_x \simeq M_x$$

Por tanto, existe un entorno $U_a = \mathrm{Spec}\, A_a$ 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. $(\mathrm{Coker}\,\pi_a)_x = 0$, por tanto existe un entorno $U_{a'} \subset U_a$ de x, de modo que $(\mathrm{Coker}\,\pi_a)_{a'} = 0$. Es decir, podemos suponer que π_a es epiyectivo. Como M_a es un A_a-módulo proyectivo, π_a tiene sección, luego $\mathrm{Ker}\,\pi_a$ es un cociente de $A_a \oplus \cdots \oplus A_a$ y es finito generado. $(\mathrm{Ker}\,\pi_a)_x = 0$, por tanto existe un entorno $U_{a'} \subset U_a$ de x, de modo que $(\mathrm{Ker}\,\pi_a)_{a'} = 0$. Es decir, podemos suponer que π_a es un isomorfismo. Así podremos construir para cada punto $x \in \mathrm{Spec}\, A$ un entorno básico donde M es libre. Como Spec$A$ es compacto, podremos construir el recubrimiento finito buscado.

Si existe un recubrimiento finito $\{U_{a_i}\}$ por abiertos básicos de Spec$A$, de modo que M_{a_i} es un A_{a_i}-módulo libre, obviamente M es localmente libre. Sólo 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 $(\mathrm{Ker}\,\pi)_{a_i}$ es finito generado. Si escribimos $(\mathrm{Ker}\,\pi)_{a_i} = \langle \frac{m_{i1}}{1}, \ldots, \frac{m_{in_i}}{1} \rangle$, con $m_{i_j} \in \mathrm{Ker}\,\pi$, entonces $\mathrm{Ker}\,\pi$ está generado por $\{m_{i_j}\}_{i_j}$, porque así es localmente. En conclusión, $\mathrm{Ker}\,\pi$ es finito generado y M es de presentación finita. □

0.7. Ideales de Fitting. Estratos de $Spec\ A$ 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 $\pi' : A^m \to M$ es un epimorfismo entonces* $\mathrm{Ker}\,\pi'$ *es un A-módulo finito generado.*

Demostración. Sabemos que tenemos un epimorfismo $\pi : A^n \to M$, tal que $\mathrm{Ker}\,\pi$ es un A-módulo finito generado. Sea $f : A^n \to A^m$ un morfismo de A-módulos, tal que $\pi' \circ f = \pi$. Obviamente, $f(\mathrm{Ker}\,\pi) \subseteq \mathrm{Ker}\,\pi'$. Tenemos el diagrama de fila superior exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathrm{Ker}\,\pi'/f(\mathrm{Ker}\,\pi)) & \longrightarrow & (A^m/f(\mathrm{Ker}\,\pi)) & \xrightarrow{\bar{\pi}'} & M & \longrightarrow & 0 \\ & & & & \uparrow \bar{f} & \nearrow \bar{\pi} & & & \\ & & & & A^n/\mathrm{Ker}\,\pi & & & & \end{array}$$

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 $\{m_1,\dots,m_r\}$ un sistema generador mínimo de M (que equivale a decir que $\{\bar{m}_1,\dots,\bar{m}_r\}$ 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 $\{n_1,\dots,n_s\}$ 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 sólo 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 sólo si su determinante es invertible. Como A es local, $a \in A$ es invertible si y sólo si $\bar{a} \in A/\mathfrak{m}$ es invertible. Por tanto, la matriz (a_{ij}) es invertible si y sólo 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 sólo 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 $n-i \le 0$ 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 sólo 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 sólo si $F_i(M)\cdot(A/\mathfrak{p}_x) = 0$, que equivale a $F_i(M)\cdot k(x) = 0$. Por la proposición 0.7.6, $F_i(M)\cdot k(x) = F_i^{k(x)}(M_x/\mathfrak{p}_x M_x)$, $k(x)$ es un cuerpo, y $F_i^{k(x)}(M_x/\mathfrak{p}_x M_x) = 0$ si y sólo 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 $M = A^n/\langle v_1,\dots,v_m\rangle$, 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

$$M/IM = (A^n/\langle v_1,\dots,v_m\rangle)/I(A^n/\langle v_1,\dots,v_m\rangle) = A^n/(\langle v_1,\dots,v_m\rangle + I\cdot A^n)$$

Si $I = \langle i_1,\dots,i_r\rangle$, $F_i(M/IM)$ es el ideal generado por los menores de orden $n-i$, de la matriz formada por los vectores $\{v_i\}$ y los vectores $\{(0,\dots,\overset{j}{i_k},\dots,0)\}_{j,k}$. 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 $I \subset \mathrm{Anul}(M)$ 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, $\mathrm{Anul}(M) \cdot F_{i+1}(M) \subseteq F_i(M)$.

□

14. Proposición: *Se cumple que* $F_0(M) \subseteq \mathrm{Anul}(M)$.

Demostración. Tenemos que $M = A^n/\langle v_1, \ldots, v_m \rangle$. 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 $v_1, \ldots, v_n$. Sea Ad_{kl} el menor complementario del coeficiente kl de la matriz (a_{ij}), afectado del signo $(-1)^{i+j}$. Se cumple que

$$(0, \ldots, \overset{k}{\det(a_{ij})}, \ldots, 0) = \sum_l Ad_{kl} v_l$$

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 sólo 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

$$A^s \xrightarrow{\varphi} A^{i+1} \to M \to 0$$

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 $x \notin (F_{i+1}(M))_0$ se cumple que $(F_{i+1}(M))_x = A_x$. 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

$$\boxed{\mathrm{Spec} A = U_0 \coprod \ldots \coprod U_n}$$

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 $f^*: \mathrm{Spec} B \to \mathrm{Spec} A$ 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 sólo 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 $\mathrm{Im} f^* \subseteq U_{i+1}$.*

Demostración. Por la proposición anterior, $f^*M = M \otimes_A B$ es localmente libre de rango $i+1$ si y sólo 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 $\mathrm{Im} f^* \cap (F_{i+1}(M))_0 = \emptyset$.

□

18. Ejercicio: Probar que si $M \to M'$ es epiyectivo, entonces $F_i(M) \subseteq F_i(M')$.

19. Ejercicio: Probar 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. Demostrar que $F_0(\Lambda^n M) = F_{n-1}(M)$.

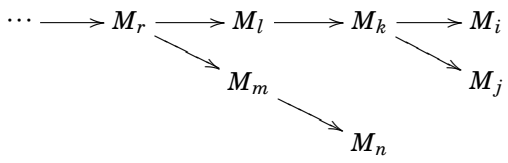
0.8. Límites proyectivos e inductivos

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"



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

$$\mathrm{Hom}_{\mathscr{C}}(N, \varprojlim_i M_i) = \{(f_i) \in \prod_i \mathrm{Hom}_{\mathscr{C}}(N, M_i) \mid f_j = f_{ij}f_i \text{ para todo } i \leq j\}$$

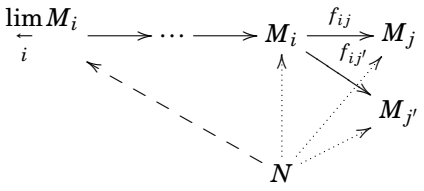
para todo objeto N de la categoría $\mathscr{C}$.

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 $\phi_i: \varprojlim_i M_i \to M_i$, 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 $\phi_i: M \to M_i$, verificando 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 $\phi_i: \varprojlim_i M_i \to M_i$, $\phi_i((m_j)) = m_i$.

Demostración. Denotemos $M = \{(m_i) \in \prod_i M_i \mid f_{ij}(m_i) = m_j \text{ para todo } i \leq j\}$. Dado $\{(f_i) \in \prod_i \mathrm{Hom}(N, M_i) \mid f_j = f_{ij} f_i \text{ para todo } i \leq j\}$, entonces la aplicación $f : N \to M$, $f(n) := (f_i(n))$ está bien definida y cumple que $f_i = \phi_i f$.

Recíprocamente, dado $f : N \to M$, las aplicaciones $f_i = \phi_i f$ cumplen que $f_j = f_{ij} f_i$ para todo $i \leq j\}$.

Estas asignaciones son inversas entre sí, luego hemos concluido. □

4. Teorema: *En la categoría de A-módulos los límites proyectivos existen, explícitamente*

$$\varprojlim_i M_i = \{(m_i) \in \prod_i M_i \mid f_{ij}(m_i) = m_j \textit{ para todo } i \leq j\}$$

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, de morfismos $k[x]/(x^{n+1}) \to k[x](x^n)$ los morfismos naturales de paso al cociente. Probar 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 $f_{ij}: M_i \to M_j$, 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

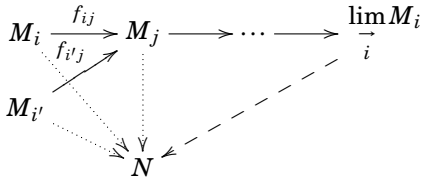
$$\mathrm{Hom}_{\mathscr{C}}(\varinjlim_i M_i, N) = \{(f_i) \in \bigoplus_i \mathrm{Hom}_{\mathscr{C}}(M_i, N) \mid f_i = f_j f_{ij} \text{ para todo } i \leq j\}$$

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 $\phi_i: M_i \to \varinjlim_i M_i$, 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*

$$\varinjlim_i M_i = \{\coprod_i M_i / \sim : m_i \sim m_j \text{ si existe un índice } k \text{ de modo que } f_{ik}(m_i) = f_{jk}(m_j)\}$$

y $\phi_j: M_j \to \varinjlim_i M_i$, $\phi_j(m_j) = \bar{m}_j$.

Demostración. 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 cumple que $f_i = f\phi_i$.

Recíprocamente, dado $f: M \to N$, las aplicaciones $f_i = f\phi_i$ cumplen que $f_i = f_j f_{ij}$ para todo $i \leq j\}$.

Estas asignaciones son inversas entre sí, luego hemos concluido. □

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 $N \in \mathscr{C}$, 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 induce 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 $\overline{g_i(m_i)} = 0$. Por tanto, existe un k, de modo que $0 = f''_{ik}(g_i(m_i)) = g_k(f_{ik}(m_i))$. Luego, $f_{ik}(m_i) = f_k(m'_k)$, para cierto $m'_k \in M'_k$. Por tanto, $\bar{m}_i = \overline{f_k(m'_k)} = f(\overline{m'}_k)$.
3. Obviamente g es epiyectiva: Dado $\overline{m''}_j \in \varinjlim_i M''_i$, 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,*

$$(\varinjlim_i M_i) \otimes_A N = \varinjlim_i (M_i \otimes_A N)$$

Demostración.

$$\begin{aligned}\mathrm{Hom}_A((\varinjlim_i M_i)\otimes_A N,R) &= \mathrm{Hom}_A(\varinjlim_i M_i,\mathrm{Hom}_A(N,R)) = \varprojlim_i \mathrm{Hom}_A(M_i,\mathrm{Hom}_A(N,R))\\ &= \varprojlim_i \mathrm{Hom}_A(M_i\otimes_A N,R) = \mathrm{Hom}_A(\varinjlim_i (M_i\otimes_A N),R)\end{aligned}$$

□

El límite inductivo de módulos planos es plano. En particular, el límite inductivo de módulos libres es plano. Queremos probar que, debilitando la noción de sistema inductivo de objetos, se cumple que todo módulo plano es límite inductivo de libres.

19. 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

$$\mathrm{Hom}_A(N,M) = N^*\otimes_A M$$

□

20. 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*

$$\begin{array}{ccc} N & \xrightarrow{\varphi} & L \\ & \searrow^{i} & \downarrow{\scriptstyle \phi} \\ & & M \end{array}$$

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 $\phi: L\to M$, $\phi((a_j)) = \sum_{j=1}^{r} a_j m_j$.

□

21. Corolario: *Sean L'' y L' dos A-módulos libres finito generados y M un A-módulo plano. Sean $\phi'': L''\to M$ y $\phi': L'\to M$ dos morfismos de A-módulos. Si f_1, f_2 son dos morfismos de A-módulos de L'' en L', tales que $\phi'' = \phi'\circ f_i$, entonces existe un módulo libre L y morfismos $f: L'\to L$ y $\phi: L\to M$ de modo que $f\circ f_1 = f\circ f_2$ y $\phi' = \phi\circ f$.*

Demostración. Considérese en el teorema anterior $N = L'/\mathrm{Im}(f_1 - f_2)$. □

Ahora ya, es fácil probar el teorema de Lazard.

22. Teorema de Govorov-Lazard: *Un A-módulo es plano si y sólo si es límite inductivo[4] de módulos libres.*

[4]En los sistemas inductivos $\{M_i\}$ que aquí consideramos, podrán existir dos o más morfismos $f_{ijk}: M_i\to M_j$, si bien imponemos que para cada par k,k' existe un h de modo que $f_{jhr}\circ f_{ijk} = f_{jhr}\circ f_{ijk'}$, para algún r. Con esta definición las propiedades demostradas y construcciones realizadas (0.8.13,0.8.14, 0.8.17 y 0.8.18) siguen cumpliéndose.

23. Corolario: *Un A-módulo M es plano si y sólo 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 0.8.20 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 0.8.19. □

0.9. Teorema de representabilidad

Hemos probado que un objeto 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.

1. Definición: Sea I un conjunto ordenado, $\{M_i, f_{ij}\}_{i\in I}$ un sistema de módulos y $F\colon \mathscr{C}_{Mod} \rightsquigarrow \mathscr{C}_{Mod}$ un funtor contravariante. Los morfismos naturales $M_j \to \varinjlim_i M_i$ inducen morfismos $F(\varinjlim_{i\in I} M_i) \to F(M_j)$ y por tanto un morfismo $F(\varinjlim_{i\in I} M_i) \to \varprojlim_{i\in I} F(M_i)$. Diremos que el funtor F transforma límites inductivos en límites proyectivos si el morfismo anterior $F(\varinjlim_{i\in I} M_i) \to \varprojlim_{i\in I} F(M_i)$ es isomorfismo, para todo sistema inductivo de módulos.

La propiedad universal del límite inductivo nos dice que el funtor $\mathrm{Hom}_A(-,N)$ transforma límites inductivos en proyectivos.

Análogamente, si F es un funtor covariante, se tiene un morfismo natural $F(\varprojlim_{i\in I} M_i) \to \varprojlim_{i\in I} F(M_i)$, y se dice que F transforma límites proyectivos en límites proyectivos si dicho morfismo es isomorfismo, para todo sistema de módulos. La propiedad universal del límite proyectivo nos dice que el funtor $\mathrm{Hom}_A(N,-)$ transforma límites proyectivos en proyectivos.

2. Teorema de representabilidad: *Sea $F\colon \mathscr{C}_{Mod} \rightsquigarrow \mathscr{C}_{Mod}$ un funtor contravariante (resp. covariante). La condición necesaria y suficiente para que F sea representable es que sea exacto por la izquierda y transforme límites inductivos (resp. proyectivos) en límites proyectivos.*[5]

Demostración. La necesidad de la condición ya la conocemos. Veamos la suficiencia. La idea de la demostración es muy simple: se construye el representante del funtor como el límite inductivo de sus submódulos. Ahora bien, hay que decir quiénes son los submódulos en términos del funtor.

Llamaremos pareja, (N,ξ_N), al par formado por un módulo N y un elemento $\xi_N \in F(N)$. Diremos que la pareja (N,ξ_N) es un *submódulo*, cuando el morfismo de funtores $h_{\xi_N}\colon \mathrm{Hom}_A(-,N) \to F$ es inyectivo (es decir, dado M y dos morfismos $f_1, f_2\colon M \to N$, si $f_1 \neq f_2$ entonces $F(f_1)(\xi_N) \neq F(f_2)(\xi_N)$).

Un morfismo de parejas $f\colon (M,\xi_M) \to (N,\xi_N)$ es un morfismo de módulos $f\colon M \to N$ tal que $F(f)(\xi_N) = \xi_M$ y entonces diremos que (M,ξ_M) domina a (N,ξ_N).

3. Lema: *Toda pareja es dominada por algún submódulo.*

[5] En otros textos al conjunto de índices de un límite inductivo no se le impone que sea filtrante, por esto, nosotros debemos añadir una condición más a la representabilidad: que F transforme sumas directas en productos directos.

Demostración. Sea (N,ξ_N) una pareja. Consideremos las parejas (N_i,ξ_{N_i}), $f_i\colon (N,\xi_N)\to(N_i,\xi_{N_i})$ que dominan a (N,ξ_N), y tales que f_i es epiyectiva. Diremos que $(N_i,\xi_{N_i})\le(N_j,\xi_{N_j})$ si existe un morfismo de parejas $\phi_{ij}\colon (N_i,\xi_{N_i})\to(N_j,\xi_{N_j})$ tal que $f_j\circ\phi_{ij}=f_i$. Obsérvese que el morfismo ϕ_{ij}, si existe, es único. Con este orden, las parejas (N_i,ξ_{N_i}) forman un conjunto ordenado. Veamos que es filtrante creciente:

Dadas (N_i,ξ_{N_i}) y (N_j,ξ_{N_j}), la pareja $(N_i\oplus N_j,\xi_{N_i\oplus N_j})$ domina a ambas, siendo $\xi_{N_i\oplus N_j}$ el elemento de $F(N_i\oplus N_j)$ que se corresponde con (ξ_{N_i},ξ_{N_j}) vía la igualdad $F(N_i\oplus N_j)=F(N_i)\times F(N_j)$. Sea K el conúcleo del morfismo $N\overset{(f_i,-f_j)}{\longrightarrow}N_i\oplus N_j$. Se tiene la sucesión exacta

$$N\overset{(f_i,-f_j)}{\longrightarrow}N_i\oplus N_j\overset{\pi}{\longrightarrow}K\to 0$$

y por tanto (F es un functor exacto por la izquierda) una sucesión exacta:

$$0\to F(K)\overset{F(\pi)}{\longrightarrow}F(N_i)\times F(N_j)\overset{F(f_i,-f_j)}{\longrightarrow}F(N)$$

Como $F(f_i)(\xi_{N_i})-F(f_j)(\xi_{N_j})=\xi_N-\xi_N=0$, existe $\xi_K\in F(K)$ tal que $F(\pi)(\xi_K)=(\xi_{N_i},\xi_{N_j})$, luego (K,ξ_K) domina a $(N_i\oplus N_j,\xi_{N_i\oplus N_j})$ y por tanto domina a (N_i,ξ_{N_i}), y finalmente a (N,ξ_N). Además, es inmediato comprobar que el morfismo composición $\phi_{N_i,K}\colon N_i\to N_i\oplus N_j\to K$ es epiyectivo y $\phi_{N_i,K}\circ f_i=\phi_{N_j,K}\circ f_j$. Se concluye fácilmente que (K,ξ_K) es una pareja del sistema y que $(K,\xi_K)\ge(N_i,\xi_{N_i})$, $(K,\xi_K)\ge(N_i,\xi_{N_i})$. Luego las parejas (N_i,ξ_{N_i}) forman un conjunto filtrante creciente.

Sea $L=\varinjlim_i N_i$ y ξ_L el elemento de $F(L)$ que se corresponde con (ξ_{N_i}) vía la igualdad $F(L)=\varprojlim_i F(N_i)$. La composición de los morfismos $N\to N_i\to L$ es epiyectivo, pues el límite inductivo de epiyecciones es una epiyección, y no depende de i. Por tanto, (L,ξ_L) domina a (N,ξ_N). Veamos que es un submódulo: hay que ver que el morfismo

$$\mathrm{Hom}_A(M,L)\to F(M),\qquad f\mapsto F(f)(\xi_L)$$

es inyectivo. Supongamos que $F(f)(\xi_L)=0$. Sea K el conúcleo de f. Se tiene la sucesión exacta

$$M\overset{f}{\longrightarrow}L\overset{\pi}{\longrightarrow}K\to 0$$

luego

$$0\to F(K)\overset{F(\pi)}{\longrightarrow}F(L)\overset{F(f)}{\longrightarrow}F(M)$$

Como $F(f)(\xi_L)=0$ existe $\xi_K\in F(K)$ tal que $F(\pi)(\xi_K)=\xi_L$. Por tanto la pareja (K,ξ_K) domina a (L,ξ_L) luego a (N,ξ_N). Además el morfismo $N\to K$ es epiyectivo, luego es una de las parejas del sistema. Como domina a todas las demás (pues domina a (L,ξ_L)) debe coincidir con el límite inductivo, es decir, $K=L$ y f es el morfismo nulo. Por tanto (L,ξ_L) es un submódulo. □

Obsérvese ahora que un morfismo entre submódulos, si existe, es único. Por tanto, los submódulos forman un conjunto ordenado con la dominación.

Consideremos entonces el sistema de los submódulos $\{(R_i,\xi_{R_i})\}$. Sea $R=\varinjlim_i R_i$ y ξ_R el elemento de $F(R)$ que se corresponde con (ξ_{R_i}) vía la igualdad $F(R)=\varprojlim_i F(R_i)$. Veamos que (R,ξ_R) representa el functor. Hay que ver que para todo M el morfismo

$$\mathrm{Hom}_A(M,R)\longrightarrow F(M),\qquad f\to F(f)(\xi_R)$$

es isomorfismo. Es epiyectivo: dado $\xi_M\in F(M)$, sea (R_i,ξ_{R_i}) un submódulo que domine a (M,ξ_M). Entonces (R,ξ_R) domina a (R_i,ξ_{R_i}) luego a (M,ξ_M), es decir, existe un morfismo $f\colon M\to R$ tal que $F(f)(\xi_R)=\xi_M$, que es lo que queríamos probar.

Es inyectivo, es decir, (R,ξ_R) es un submódulo. En efecto, sea (R_i,ξ_{R_i}) un submódulo que le domine. Entonces este es un elemento del sistema inductivo que domina a todos los demás (pues domina a (R,ξ_R)), luego coincide con el límite inductivo, luego este es un submódulo. □

El teorema de representabilidad puede ser enunciado con mayor generalidad en cualquier categoría, y la demostración sigue los mismos pasos.

4. Teorema: *Sea $\mathscr{C}$ una categoría con sumas directas, límites inductivos, conúcleos, con una familia de generadores, y tal que los conúcleos de cualquier objeto forman un conjunto. Si F es un funtor contravariante sobre $\mathscr{C}$ con valores en la categoría de conjuntos, la condición necesaria y suficiente para que F sea representable es que sea exacto por la izquierda y transforme límites inductivos en límites proyectivos*

(Un conjunto de objetos $\{U_i\}$ se dice que es una familia de generadores cuando para cada par de subobjetos distintos A y A' de un objeto B existe un morfismo $U_i \hookrightarrow B$ que factoriza a través de A, pero no de A'.)

0.10. 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 H y K son dos subgrupos normales y $H \cap K = 1$, entonces los elementos de H conmutan con los de K.

5. Si G es un grupo de orden un número primo, entonces G es cíclico.

6. 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.

7. Todo grupo finito de orden par contiene algún elemento $g \neq 1$ tal que $g^2 = 1$.

8. 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.

9. Sea X un G-conjunto, $x \in X$ y $x' = g \cdot x$. Probar que $I_{x'} = g \cdot I_x \cdot g^{-1}$.

10. Los morfismos de G-conjuntos transforman órbitas en órbitas, y todo endomorfismo de una órbita es un automorfismo.

11. 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.

12. Sea X un G-conjunto, $H \subseteq G$ un subgrupo y consideremos G/H como G-conjunto de modo natural: $g \cdot \bar{g'} := \overline{gg'}$. Probar que la aplicación,

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

es biyectiva.

13. Si H es un subgrupo de un grupo G, el grupo de automorfismos del G-conjunto G/H es isomorfo al grupo $N(H)/H$.

14. 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.

15. Todo subgrupo de índice 2 es normal. (*Indicación:* Si $g \notin H$, entonces gH es el complementario de H.)

16. 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.)

17. El grupo A_4 no tiene ningún subgrupo de orden 6 (aunque su orden es múltiplo de 6).

18. 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.

19. 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).

20. Todo subgrupo normal de orden p de un p-grupo G está contenido en el centro de G.

21. Todo subgrupo normal H de un p-grupo G tiene intersección no trivial con el centro de G; es decir, $Z(G) \cap H \neq 1$.

22. Si G es un p-grupo no abeliano de orden p^3, entonces todo subgrupo normal de G contiene al centro.

23. Si H es un subgrupo propio de un p-grupo, entonces $H \neq N(H)$.

24. Determinar los subgrupos de Sylow de los grupos simétricos S_3, S_4 y S_5.

25. Determinar todos los subgrupos normales de S_3, S_4 y A_4.

26. 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.

27. Todo grupo de orden 100 tiene algún subgrupo normal de orden 25.

28. 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 $H \lhd H'$.

29. 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.

30. 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 $g^n = s^2 = 1$, $sgs = g^{-1}$. Calcular el centro y el grupo de automorfismos del grupo D_n.

31. Si p es un número primo, todo grupo no abeliano de orden $2p$ es isomorfo al grupo D_p.

32. 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.

33. Clasificar, salvo isomorfismos, los grupos de orden ≤ 10.

34. 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 $G \to S_d$.)

35. 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 $\tau : S_6 \to S_6$ tal que $\tau(P) = \{\sigma \in S_6 : \sigma(6) = 6\}$, y éste es un automorfismo externo del grupo S_6.

36. Demostrar que $\mathbb{C}[x,y]/(x) \simeq \mathbb{C}[y]$. Probar que $\mathbb{C}[x,y,z]/(y - x^2, y^3 + z^3) \simeq \mathbb{C}[x,z]/(x^6 + z^3)$.

37. Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. Los elementos de S son invertibles en A si y sólo si el morfismo de localización $A \to A_S$ es un isomorfismo.

38. Sea $f : A \to B$ un morfismo de anillos y $S \subset A$ un sistema multiplicativo. Si $f(S)$ son elementos invertibles de B entonces existe un único morfismo $f_S : A_S \to B$ tal que f sea la composición de los morfismos $A \to A_S \xrightarrow{f_S} B$.

39. Probar que $(A_S)_{S'} = A_{S\cdot S'}$, donde $S\cdot S' \underset{\text{def}}{=} \{s\cdot s' \mid s\in S, s'\in S'\}$.

40. Probar que $k[x,y]/(xy-1) \simeq k[x]_{1,x,x^2,\ldots}$.

41. Probar que $\mathbb{C}[x]_{\mathbb{R}[x]-0} \simeq \mathbb{C}(x)$.

42. Probar que el morfismo de localización $i\colon A \to A_S$ es un isomorfismo si y sólo si $i^*\colon \operatorname{Spec} A_S \to \operatorname{Spec} A$ es un homeomorfismo. Pruébese que si $\operatorname{Spec} A_S = \operatorname{Spec} A_{S'}$ (en $\operatorname{Spec} A$) entonces $A_S = A_{S'}$.

43. Calcular $\operatorname{Spec}\mathbb{Z}/6\mathbb{Z}$, $\operatorname{Spec}(\mathbb{C}[x,y]/(y^2-x^3))_x$.

44. Calcular $\operatorname{Spec}\mathbb{Z}[x]$, $\operatorname{Spec}\mathbb{Z}[\sqrt{5}]$.

45. Calcular $\operatorname{Spec}\mathbb{R}[x,y]$.

46. Si $\operatorname{Spec} A$ es la unión disjunta de dos abiertos U_1, U_2 probar que $U_1 = \operatorname{Spec} A_{U_1}$.

47. Sean $I, I' \subseteq A$ dos ideales. Probar que $(I)_0 = (I')_0$ si y sólo si $r(I) = r(I')$, donde denotamos $r(I) = \{a\in A\colon a^n \in I \text{ para cierto } n\in\mathbb{N}\}$.

48. Probar que los elementos de los ideales primos minimales de un anillo son divisores de cero (Pista: localícese en los ideales primos minimales).

49. Probar que si $f\colon A \hookrightarrow B$ es un morfismo de anillos inyectivo, entonces $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación continua densa.

50. Probar que la intersección de dos rectas paralelas $(ax+by+c)_0$, $(ax+by+c')_0$ $(c\neq c')$ es vacía.

51. Dado $i\colon \mathbb{C}[x] \to \mathbb{C}[x,y]/(y^2-x^2+x^3)$, calcular el morfismo $i^*\colon \operatorname{Spec}\mathbb{C}[x,y]/(y^2-x^2+x^3) \to \operatorname{Spec}\mathbb{C}[x]$, calcular las fibras de i^*.

52. Calcular 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 $x=1$.

53. Sea $I\subseteq A$ un ideal y M un A-módulo probar que $IM := \{m\in M\colon m = \sum a_i m_i, \text{ con } a_i\in I \text{ y } m_i\in M\}$ es un A-módulo.

    Si M' es otro A-módulo probar que $I(M\oplus M') = IM\oplus IM'$. Si M y M' son submódulos de un módulo probar que $I(M+M') = IM + IM'$.

54. Sean $N\subseteq M$ y $N'\subseteq M'$ submódulos. Probar que $N\oplus N'$ es un submódulo de modo natural de $M\oplus M'$, de modo que $(M\oplus M')/(N\oplus N') = M/N \oplus M'/N'$.

55. Si N, N' son submódulos de un módulo M probar que

$$(N+N')/N' = N/(N\cap N')$$

    Si denotamos por $\bar{N} = \{\bar{n}\in M/N'\colon n\in N\}$, probar que

$$(M/N')/\bar{N} = M/(N+N')$$

56. Sea $f\colon M\to M'$ un morfismo de A-módulos. Sean N_1, N_2 dos submódulos de M probar que $f(N_1+N_2) = f(N_1)+f(N_2)$ (denotamos por $f(N) = \{f(n)\in M', \text{ con } n\in N\}$). Sea I un ideal, probar que $f(I\cdot N_1) = I\cdot f(N_1)$.

57. Sea $f\colon M\to M'$ un morfismo de A-módulos y $m' = f(m)$. Probar que $f^{-1}(m') = m + \operatorname{Ker} f := \{m+n \text{ con } n\in \operatorname{Ker} f\}$. Sea N un submódulo de M, probar que $f^{-1}(f(N)) = N + \operatorname{Ker} f$.

58. Probar la igualdad $\operatorname{Hom}_A(A/I, M) = \{m\in M\colon Im = 0\}$. Probar que $\operatorname{Hom}_A(A^n, M) = M\oplus \overset{n}{\ldots} \oplus M$.

59. Calcular 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 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z},\mathbb{Z})$.

60. Probar que si un endomorfismo $f: M \to M$, cumple que $f^2 = f$ entonces $M = \operatorname{Ker} f \oplus \operatorname{Ker}(f - \mathrm{Id})$.

61. Probar que el anulador del A-módulo A/I es I.

62. Probar que si M es un A-módulo libre entonces $\operatorname{Anul}(M) = 0$.

63. Sea el $\mathbb{Z}$-módulo $M = \bigoplus_{0 \neq n \in \mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. Probar que $\operatorname{Anul} M = (0)$. ¿Existe algún $m \in M$ de modo que $\operatorname{Anul}(\langle m \rangle) = 0$?

64. Probar que si $M \simeq M_1 \oplus \cdots \oplus M_n$ entonces $\operatorname{Anul}(M) = \bigcap_i \operatorname{Anul}(M_i)$. Calcular el ideal anulador del $\mathbb{Z}$-módulo $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$.

65. Sea $0 \to M_1 \to M_2 \to M_3 \to 0$ una sucesión exacta de A-módulos. Demostrar que $\operatorname{Anul}(M_2) \supseteq \operatorname{Anul}(M_1) \cdot \operatorname{Anul}(M_3)$.

66. ¿Es $\mathbb{Z}/4\mathbb{Z}$ un $\mathbb{Z}$-módulo libre? ¿Es un $\mathbb{Z}/4\mathbb{Z}$-módulo libre? Definir un sistema generador de $\mathbb{Z}/4\mathbb{Z}$ como $\mathbb{Z}$-módulo.

67. Sea $M = \{\frac{a}{2^n}, a \in \mathbb{Z}, n \in \mathbb{N}\} \subset \mathbb{Q}$. Probar que M es un $\mathbb{Z}$-submódulo de $\mathbb{Q}$ y que no es finito generado.

68. Probar que todo cociente de un módulo finito generado es finito generado. Probar que la suma de dos submódulos finito generados es finito generado.

69. Sea $C(\mathbb{R})$ el anillo de todas las funciones reales continuas de variable real. Demostrar 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.

70. Probar que todo $\mathbb{Z}$-submódulo finito generado de $\mathbb{Q}$ no nulo, es libre generado por un elemento. Probar que $\mathbb{Q} \neq \mathbb{Z}$.

71. Hallar una base (si existe) de $\mathbb{Z}[x]$ como $\mathbb{Z}$-módulo.

72. Probar que todo epimorfismo de un módulo en un libre tiene sección.

73. Sea $i: N \hookrightarrow M$ un morfismo inyectivo de A-módulos. Si $r: M \to N$ es un retracto de i, es decir, $r \circ i = \mathrm{Id}$, probar que $M \simeq N \oplus \operatorname{Ker} r$ (defínase $N \oplus \operatorname{Ker} r \to M$, $(n, n') \mapsto i(n) + n'$).

    Sea $\pi: M \to M'$ un epimorfismo de módulos, de modo que exista una sección s de π, es decir, $\pi \circ s = \mathrm{Id}$. Probar que $M \simeq \operatorname{Ker} \pi \oplus M$.

74. 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 $\pi(m', m'') = m''$.

    Probar que si $r: M \to M'$ es un retracto de f, i.e., $r \circ f = \mathrm{Id}$ entonces la sucesión exacta rompe. Probar que si $s: M'' \to M$ es una sección de g, i.e., $g \circ s = \mathrm{Id}$, entonces la sucesión exacta rompe.

75. Probar que $(\operatorname{Anul}_A(M))_S = \operatorname{Anul}_{A_S}(M_S)$, si M es un A-módulo finito generado.

76. 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. Demostrar que $B_S = B_{f(S)}$.

77. Sea $I \subseteq A$ un ideal y $\mathfrak{p}_x \subset A$ un ideal primo. Probar que $I_x = A_x$ si y sólo si $x \notin (I)_0$.

78. Probar que $(I \cdot M)_S = I_S \cdot M_S = I \cdot M_S$.

79. Sea A un anillo íntegro, e $I \neq 0$ un ideal. Probar que I es libre si y sólo si $I = aA$ $(a \neq 0)$.

80. Sea M un A-módulo finito generado y $S \subset A$ un sistema multiplicativo de A. Probar que si $M_S = 0$ entonces existe un $s \in S$ tal que $s \cdot m = 0$ para todo $m \in M$.

81. Sea $I \subseteq A$ un ideal y M un A-módulo finito generado. Probar que $IM = M \iff M_{1+I} = 0$.

82. Probar que si un endomorfismo $T\colon M \to M$ de un A-módulo finito generado es epiyectivo entonces es un isomorfismo.

83. Demostrar que $\mathbb{Z}^n$ es un $\mathbb{Z}$-módulo isomorfo a $\mathbb{Z}^m$ si y sólo si $n = m$.

84. Demostrar que A^n es un A-módulo isomorfo a A^m si y sólo si $n = m$.

85. Sea M un A-módulo finito generado. Probar que si $M \simeq M \oplus N$ entonces $N = 0$. ¿Es siempre cierto este resultado si M no es finito generado?

86. Sea $m_1, \ldots, m_s$ un sistema generador de un A-módulo libre A^n. Probar que $s \geq n$.

87. Probar que todo sistema de n generadores de un módulo libre A^n es base.

88. Sean M y M' dos A-módulos finito generados. Sea $f\colon M \to M'$ un morfismo de A-módulos. Probar que si los morfismos $\bar{f}_x\colon M/\mathfrak{m}_x M \to M'/\mathfrak{m}_x M'$, $\bar{m} \mapsto \overline{f(m)}$ son epiyectivos, para todo punto cerrado $x \in \operatorname{Spec} A$, entonces el morfismo f es epiyectivo.

89. Demostrar que si existe un morfismo $A^m \hookrightarrow A^n$ inyectivo de A-módulos entonces $m \leq n$.

90. Demostrar que la longitud del $k[x]$-módulo $k[x]/(x^n)$ es n.

91. Sea $A \to B$ un morfismo de anillos. Sea Δ el núcleo del morfismo $B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$. Probar 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, probar que

$$M \otimes_B M' \simeq (M \otimes_A M')/\Delta \cdot (M \otimes_A M')$$

92. Demostrar que el morfismo natural $M^* \otimes_A N \to \operatorname{Hom}_A(M,N)$, $w \otimes n \mapsto \phi_{w \otimes n}$, donde $\phi_{w \otimes n}(m) := w(m) \cdot n$ es un isomorfismo lineal si N es un A-módulo libre finito generado. Demostrar 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.

93. Probar que $\mathbb{R}[x]/(p(x)) \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x]/(p(x))$.

94. Probar que $(A[x_1, \ldots, x_n]/I) \otimes_A B = B[x_1, \ldots, x_n]/I \cdot B[x_1, \ldots, x_n]$.

95. Probar que $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \times \mathbb{C}$ como $\mathbb{C}$-álgebra. Calcular $\operatorname{Hom}_{\mathbb{R}-\text{álg.}}(\mathbb{C}, \mathbb{C})$.

96. Probar que $\operatorname{Hom}_{k-\text{álg.}}(A,k)$ es igual al conjunto de ideales primos maximales de A, de conúcleo k.

97. Sea A un anillo íntegro y M un A-módulo plano. Probar que $T(M) = 0$.

98. Probar que si M y N son A-módulos planos, también lo es $M \otimes_A N$. Probar que si B es una A-álgebra plana y M es un B-módulo plano, entonces M es un A-módulo plano.

99. Sea $A \to B$ un morfismo de anillos fielmente plano. Sea M un A-módulo. Probar que si $M \otimes_A B$ es un B-módulo finito generado, entonces M es un A-módulo finito generado.

100. Probar 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, probar que $k[x,y]/(y^2 - x)$ es una $k[x]$-álgebra plana.

101. Sea A un dominio de ideales principales y M un A-módulo sin torsión. Probar que M es unión de módulos libres finito generados.

102. 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. Probar que $\varprojlim_n N_n = \bigcap_n N_n$.

103. 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. Probar que $\varprojlim_{i\in I} M_i = \varprojlim_{j\in J} M_j$.

104. Probar 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.

105. Demostrar que todo módulo es el límite inductivo de sus submódulos finito generados.

106. Demostrar que el límite inductivo de módulos planos es plano.

107. 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.

108. Sea $x \in \operatorname{Spec} A$ y M un A-módulo. Demostrar que $M_x = \varinjlim_{\{x\in U_a\}} M_a$.

109. Sea $M = C_0^\infty(\mathbb{R})$ el anillo de gérmenes de funciones diferenciables reales de la recta real en el origen. Probar que M es un $C^\infty(\mathbb{R})$-módulo plano finito generado, no proyectivo, ni de presentación finita.

110. Probar que si $\operatorname{Hom}_A(N,M) = \operatorname{Hom}_A(N,A) \otimes_A M$ para todo A-módulo N de presentación finita, entonces M es un A-módulo plano (véase 0.8.20 y 0.8.22).

111. Sea $\{A_i\}$ un sistema inductivo de anillos. Probar $\operatorname{Spec} \varinjlim A_i = \varprojlim \operatorname{Spec} A_i$.

112. Sean N,N' submódulos de M, tales que $M = N+N'$. Probar que M es noetheriano si y sólo si N,N' son noetherianos.

113. Sean N,N' submódulos de M, tales que $N \cap N' = 0$. Probar que M es noetheriano si y sólo si $M/N, M/N'$ son noetherianos.

114. Sea M un A-módulo noetheriano. Probar que $A/\operatorname{Anul}(M)$ es un anillo noetheriano.

115. Probar que si M es un A-módulo noetheriano entonces $M[x]$ es un $A[x]$-módulo noetheriano.

116. Probar que si $A[x]$ es noetheriano entonces A es noetheriano.

117. Probar que si $\operatorname{Spec} A = \bigcup_i U_{a_i}$, un A-módulo M es noetheriano si y sólo si M_{a_i} son A_{a_i}-módulos noetherianos para todo i.

118. Demostrar que $\prod^{\infty}\mathbb{Z}$ no es un anillo noetheriano.

119. Sea A un anillo noetheriano. Probar que existe un $n \in \mathbb{N}$ de modo que $(\operatorname{rad} A)^n = 0$.

120. Sea A un anillo noetheriano, e $I \subset A$ un ideal. Probar que existe un $n \in \mathbb{N}$ de modo que $r(I)^n \subseteq I$.

121. Sea A un anillo noetheriano y sea $f = \sum_{i=0}^{\infty} a_i x^i \in A[[x]]$. Demostrar que f es nilpotente si y sólo si cada a_i es nilpotente.

122. Sea A un dominio de ideales principales. Si $aA \cap bA = cA$, pruébese que c es el mínimo común múltiplo de a y b.

123. 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.

124. Sean p y q números primos distintos. Se pide calcular el número de grupos abelianos finitos desisomorfos de orden p^2q.

125. 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.

126. Sea G un grupo abeliano finito. Demostrar que G es cíclico si y sólo si para cada n divisor del orden de G, existe un único subgrupo de G de orden n.

127. 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 $\mathbb{R}$.

128. Clasifíquese el endomorfismo "multiplicar por x" sobre el espacio

$$E = k[x]/(x) \oplus k[x]/(x^3) \oplus k[x]/(x^5)$$

129. Clasifíquense los endomorfismos nilpotentes de un espacio vectorial de dimensión 3. Problema análogo para espacios de dimensión 4 y 5.

130. 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 $T = (x^2+4)^2(x+8)^2$, $\dim E = 8$.

131. Clasificar sobre el cuerpo racional el endomorfismo

$$T = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

132. 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 $T = D^2$.

133. Sea A el $\mathbb{C}$-espacio vectorial de todas las funciones reales a valores complejos infinitamente diferenciables. Se designa por D el operador derivada. Es claro que D es un endomorfismo $\mathbb{C}$ lineal de A.

   a) Probar la fórmula de conmutación

$$P(D)(e^{\alpha x} \cdot y) = e^{\alpha x} P(D+\alpha) y$$

   para $y \in A$ y $\alpha \in \mathbb{C}$.

   b) Probar que $\operatorname{Ker} D^{r+1} = \{\text{Polinomios de grado menor o igual que } r\}$. Calcular $\operatorname{Ker}(D-\alpha)^{r+1}$. Si $p(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_r)^{n_r}$, calcular $\operatorname{Ker} p(D)$.

   c) Resolver las ecuaciones diferenciales: $y'''' - 2y''' + 2y'' = 0$, $y'' + y = 0$.

134. Con las notaciones del ejercicio anterior sea la ecuación $P(D)y = z$, con $z \in A$. Supongamos que existe un polinomio $Q(x)$ primo con $P(x)$ de modo que $Q(D)z = 0$. Pruébese que existe un polinomio $R(x)$, de modo que $R(D)z$ es una solución particular de la ecuación dada. Resolver la ecuación $y^{(n} - y = x^n$.

135. Dada la ecuación diferencial $P(D)y = z$, escribamos $y = \frac{1}{P(D)}z$. Si $P(x) = (x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}$, expresar y en términos de primitivas (reiteradas) de sumas de productos de funciones exponenciales y derivadas de z (úsese la descomposición de fracciones racionales en fracciones simples y la fórmula de conmutación). Resolver $y'' - y = senx$.

136. Sea $Suc(\mathbb{C}) = \{(a_n)\}$ el $\mathbb{C}$-espacio vectorial de las sucesiones de números complejos. Sea $\nabla\colon Suc(\mathbb{C}) \to Suc(\mathbb{C})$ la aplicación $\mathbb{C}$-lineal definida por $\nabla(a_n) = (a'_n)$, donde $a'_n = a_{n+1}$. Sea $\Delta = \nabla - \mathrm{Id}$, el "operador diferencia".

    a) Probar las fórmulas de conmutación

    $$P(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot P(\alpha\nabla)(a_n)$$
    $$P(\nabla-\alpha)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot P(\alpha\cdot\Delta)(a_n)$$

    b) Demostrar que las sucesiones $\{(1),(n),\ldots,(n^r)\}$ son una base de $\mathrm{Ker}\,\Delta^{r+1}$. Calcular $\mathrm{Ker}(\nabla - \alpha)^r$.

    c) Resolver la ecuación $a_{n+2} = a_{n+1} + a_n$, con las condiciones iniciales $a_0 = 0, a_1 = 1, a_2 = 2$ (sucesión de Fibonacci).

137. Dada la ecuación inhomogénea $p(\nabla)(a_n) = (b_n)$, supóngase que existe un polinomio $q(x)$, primo con $p(x)$, tal que $q(\nabla)(b_n) = 0$. Pruébese que existe un polinomio $r(x)$ tal que $r(\nabla)(a_n)$ es una solución particular de la ecuación dada.

    Estúdiese el caso en que $p(x)$ y $q(x)$ no son primos entre sí. Resolver $a_{n+2} + 2a_{n+1} - 8a_n = 2^n$.

138. Probar que un grupo abeliano finito generado es cíclico si y sólo si tiene un único factor invariante no invertible.

139. ¿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?

140. Probar que si el polinomio característico de un endomorfismo lineal tiene todas sus raíces distintas entonces coincide con el primer factor invariante.

141. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Probar 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.

142. 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'. Probar que

    $$c_T(x) = c_{T_{|E'}}(x)\cdot c_{\bar{T}}(x)$$

143. 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 $\mathrm{tr}(p(T)) = \sum_{i=1}^{n} p(\alpha_i)$, $\det(p(T)) = \prod_{i=1}^{n} p(\alpha_i)$.

144. Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita. Sea $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal de E. Demostrar 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 $c_T(x)$).

145. *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. Calcular la matriz columna $C(t)$ tal que $e^{At} \cdot C(t)$ sea una solución del sistema.

146. Resuélvanse los siguientes sistemas de ecuaciones diferenciales

$$\begin{array}{lll} \frac{dx}{dt} = x - 3y + 3z & \frac{dx}{dt} = 3x - y & \frac{dx}{dt} = -11x - 4y \\ \frac{dy}{dt} = -2x - 6y + 13z & \frac{dy}{dt} = x + y & \frac{dy}{dt} = 15x + 6y \\ \frac{dz}{dt} = -x - 4y + 8z & \frac{dy}{dt} = 3x + 5z - 3u & \\ & \frac{du}{dt} = 4x - y + 3z - u & \end{array}$$

147. Sea $P(x) \in \mathbb{R}[x]$ un polinomio de grado n. Probar que la ecuación diferencial $P(D)y = f(x)$ es equivalente a un sistema de ecuaciones diferenciales lineales de n variables.

148. *a*) Sea $P(x) \in \mathbb{R}[x]$ un polinomio de grado n. Sean $s_1(x), \ldots, s_n(x)$ soluciones, linealmente independientes, de la ecuación diferencial $P(D)y = 0$. Probar que si $c_1(x), \ldots, c_n(x)$ cumplen las ecuaciones

$$\begin{array}{l} c_1(x)'s_1(x) + \ldots + c_n(x)'s_n(x) = 0 \\ \ldots \\ c_1(x)'s_1(x)^{n-2)} + \ldots + c_n(x)'s_n(x)^{n-2)} = 0 \\ c_1(x)'s_1(x)^{n-1)} + \ldots + c_n(x)'s_n(x)^{n-1)} = f(x) \end{array}$$

entonces $c_1(x)s_1(x) + \ldots + c_n(x)s_n(x)$ es una solución particular de $P(D)y = f(x)$.

b) Pruébese este resultado como caso particular de 145 (b).

149. 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), demostrar que la matriz (a_{ij}) es triangulable. Si admitimos, además, las mismas transformaciones "elementales" con las columnas, demostrar que (a_{ij}) es diagonalizable. Resolver el sistema de ecuaciones diofánticas

$$\begin{array}{l} 7x + 5y = 1 \\ 5x + 3y = 3 \end{array}$$

150. Clasificar el $\mathbb{Z}$-módulo $(\mathbb{Z} \times \mathbb{Z})/\langle (7,5), (5,3) \rangle$.

151. Sea A una matriz con coeficientes en $k[D]$. Probar 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 de un polinomio

Puede definirse el Álgebra, con ingenua concisión, como la rama de las Matemáticas que estudia las raíces de una ecuación algebraica $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$. Con mayor generalidad, podría decirse que es la disciplina que estudia las soluciones de los sistemas de ecuaciones algebraicas en n indeterminadas

$$\begin{aligned} &p_1(x_1,\ldots,x_n) = 0\\ &p_2(x_1,\ldots,x_n) = 0\\ &\cdots\\ &p_r(x_1,\ldots,x_n) = 0 \end{aligned}$$

Así pues, un primer curso en Álgebra debería estudiar las ecuaciones $p(x) = 0$.

Consideremos un polinomio $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$. El teorema fundamental del Álgebra, que probaremos, afirma que existen $\alpha_1,\ldots,\alpha_n \in \mathbb{C}$ de modo que $p(x) = a_0 \cdot (x-\alpha_1)\cdots(x-\alpha_n)$. En general, dado un cuerpo k existe un cuerpo k' que contiene a k, único salvo isomorfismos, cumpliendo

1. Dado $\alpha \in k'$, existe $p(x) \in k[x]$, tal que $p(\alpha) = 0$.
2. Dado $p(x) \in k'[x]$, existen $\alpha_1,\ldots,\alpha_n \in k'$ de modo 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 y todo polinomio simétrico en las raíces es igual a un polinomio en los coeficientes de las raíces. Vía la teoría del exceso 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. Los teoremas de Sturm y Budan-Fourier permiten calcular el número de raíces reales de un polinomio real en un intervalo $[a,b]$. Para la resolución de los sistemas de ecuaciones algebraicas se introduce la resultante de polinomios. Gracias a ésta, dado un sistema de ecuaciones algebraicas podemos 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.

1.1. Extensiones de cuerpos

1.1.1. Teorema de Kronecker. Cierre algebraico

1. 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.

2. 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 $\dim_k K$.

3. 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 $\alpha_1,\dots,\alpha_n \in K$, denotamos $k(\alpha_1,\dots,\alpha_n)$ a la mínima k-subextensión de K que contiene a $\alpha_1,\dots,\alpha_n$. Explícitamente,

$$k(\alpha_1,\dots,\alpha_n) = \{\frac{p(\alpha_1,\dots,\alpha_n)}{q(\alpha_1,\dots,\alpha_n)} \in K : p(x_1,\dots,x_n), q(x_1,\dots,x_n) \in k[x_1,\dots,x_n] \text{ y } q(\alpha_1,\dots,\alpha_n) \neq 0\}$$

4. 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.

5. 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 con coeficientes en k 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. Además, $p(x)$ ha de ser irreducible, luego $k[x]/(p(x))$ es un cuerpo. Por tanto, $\operatorname{Im}\phi \simeq k[x]/(p(x))$ es un cuerpo y ha de coincidir con $k(\alpha)$. Es decir, $k(\alpha) = k[x]/(p(x))$. Observemos que $k(\alpha) = \{q(\alpha) \in K,\ q(x) \in k[x]\} =: k[\alpha]$.

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

7. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos y $\alpha \in K$. Entonces, α es algebraica sobre k, si y sólo 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 0.3.59). Recíprocamente, si $\dim_k k(\alpha) = n < \infty$ entonces $1, \alpha, \dots, \alpha^n$ son k-linealmente dependientes, luego existe un polinomio de grado n que anula a α. □

8. 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 igualdades 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.

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

10. 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. □

11. Proposición: *Sean $k \hookrightarrow K$ y $k \hookrightarrow K'$ dos extensiones de cuerpos. Entonces, existe una k-extensión de cuerpos L, de modo que tenemos morfismos de k-extensiones $K \hookrightarrow L$ y $K' \hookrightarrow L$.*

Demostración. Sea $\mathfrak{m}$ un ideal maximal de $K \otimes_k K'$ y $L = (K \otimes_k K')/\mathfrak{m}$. L es una k-extensión de cuerpos y tenemos los morfismos naturales de k-extensiones $K \to (K \otimes_k K')/\mathfrak{m}$, $\lambda \mapsto \overline{\lambda \otimes 1}$, $K' \to (K \otimes_k K')/\mathfrak{m}$, $\lambda' \mapsto \overline{1 \otimes \lambda'}$. □

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

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

Si K' es otra extensión de cuerpos k y $\beta \in K'$ es una raíz de $p(x)$, entonces en toda k-extensión L que contenga a K y K' se cumple que $\beta = \alpha_i$, para algún i. Si $\beta_1, \ldots, \beta_n \in K'$ son tales que $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$, entonces en L se tiene que $\alpha_i = \beta_i$, para todo i (reordenando las β_i si es necesario). Se dice que $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$.

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 $K = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K[x]$ tenemos que $p(x) = (x - \alpha_1) \cdot p_2(x)$. Por hipótesis de inducción, existe una extensión finita $K \hookrightarrow K'$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Luego en K', que es una extensión finita de k,

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

En L, $0 = p(\beta) = \lambda \cdot (\beta - \alpha_1) \cdots (\beta - \alpha_n)$, luego $\beta = \alpha_i$, para algún i.

Si $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$ (en L), como $0 = p(\alpha_1) = \lambda \cdot (\alpha_1 - \beta_1) \cdots (\alpha_1 - \beta_n)$, reordenando las β_i, podemos suponer que $\beta_1 = \alpha_1$. Dividiendo por $x - \alpha_1$, tendremos que $\lambda \cdot (x - \beta_2) \cdots (x - \beta_n) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Por inducción sobre n, reordenado $\beta_2, \ldots, \beta_n$, tendremos que $\beta_i = \alpha_i$, para todo $i \geq 2$.

□

13. Observación: Agrupando los factores simples con la misma raíz, tenemos (en $K[x]$) que

$$p(x) = \lambda \cdot (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}, \quad \text{con } \alpha_i \neq \alpha_j \text{ para todo } i \neq j$$

Si $n_i > 1$, se dice que α_i es una raíz múltiple de $p(x)$ de multiplicidad n_i. El máximo común divisor de dos polinomios se puede calcular mediante el algoritmo de Euclides, por tanto, no cambia si hacemos un cambio de cuerpo base. Consideremos una extensión de cuerpos K donde $p(x)$ y $q(x)$ descompongan es factores simples, podemos escribir $p(x) = \lambda \cdot (x - \alpha_1)^{n_1} \cdots (x - \alpha)^{n_r}$ y $q(x) = \mu \cdot (x - \alpha_1)^{m_1} \cdots (x - \alpha)^{m_r}$, con $n_i, m_i \geq 0$ y $\alpha_i \neq \alpha_j$, para todo $i \neq j$. Entonces

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

Los polinomios $p(x)$ y $q(x)$ son primos entre sí si y sólo si no tienen raíces comunes (estamos considerando todas las raíces de $p(x)$ y $q(x)$ en K).

Un polinomio $p(x)$ no tiene raíces múltiples si y sólo si $p(x)$ y $p'(x)$ son primos entre sí.

14. 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 $\bar{k}$.

15. 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 irreducibles de $k[x]$. Para cada $p \in P$ sea por Kronecker K_p una k-extensión finita de cuerpos que contenga a todas las raíces del polinomio p. Para cada subconjunto finito $\{p_1, \ldots, p_n\}$ de P consideremos la k-álgebra $K_{p_1} \otimes \ldots \otimes K_{p_n}$, y para cada inclusión $\{p_1, \ldots, p_n\} \subseteq \{p_1, \ldots, p_n, \ldots, p_m\}$ consideremos el morfismo obvio $K_{p_1} \otimes \ldots \otimes K_{p_n} \to K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m}$. Sea A el límite inductivo de todos estos morfismos. Sea $\bar{k}$ el cociente de A por cualquier ideal maximal. Obviamente, $\bar{k}$ es una extensión algebraica de k, pues está generado algebraicamente por las imágenes de las extensiones K_p. Sea $\bar{k} \hookrightarrow K$ una extensión algebraica de cuerpos y $\alpha \in K$. K es una extensión algebraica de k, así pues α es algebraica sobre k. Sea $p = p(x) \in k[x]$ el polinomio mínimo anulador de α. K_p contiene todas las raíces de $p(x)$, luego $\bar{k}$ también, $\alpha \in \bar{k}$ y $K = \bar{k}$.

Si k' es una extensión algebraica de k, entonces $(\bar{k} \otimes_k k')/\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal, es una extensión algebraica de $\bar{k}$ y k'. Por tanto, $(\bar{k} \otimes_k k')/\mathfrak{m} = \bar{k}$ y ésta contiene a k'. Si k' es algebraicamente cerrado entonces $\bar{k} = k'$.

□

1.1.2. Grado de trascendencia de una extensión de cuerpos

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

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

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

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

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

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

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

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

20. Teorema: *Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos de tipo finito. Existen bases de trascendencia de Σ sobre k y todas tienen el mismo número de elementos, 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 3.3.2, 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 $i \leq n$. Para $i = 0$ es inmediato. Suponemos el enunciado cierto para $i-1 \geq 0$. 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 $\xi_1,\dots,\xi_m,\xi_{m+1}$ son algebraicamente independientes. Luego $m \geq n$. Por la misma razón $n \geq m$ y $n = m$. □

21. 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.

22. 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 $p(x_1,\dots,x_n) = 0$. Entonces $k(\xi_1,\dots,\xi_n)$ 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.

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

1.1.3. Espectro primo y soluciones de un sistema de ecuaciones algebraicas

24. Teorema: *Sea $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ 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 $\alpha = (\alpha_1,\dots,\alpha_n), \beta = (\beta_1,\dots,\beta_n) \in k'^n$, diremos que $\alpha \sim \beta$ si existe $\tau \in Aut_{k-alg}k'$, tal que*

$$\tau(\alpha) := (\tau(\alpha_1),\dots,\tau(\alpha_n)) = \beta$$

Se cumple que

$$\boxed{\operatorname{Spec} A = \{\alpha \in k'^n : p_1(\alpha) = \cdots = p_r(\alpha) = 0\}/\sim}$$

Demostración. Dado $\bar{\alpha} \in \{\alpha \in k'^n : p_i(\alpha) = 0, \forall i\}/\sim$ le asignamos el ideal primo

$$\mathfrak{p}_\alpha := \{\bar{p} \in k[x_1,\dots,x_n]/(p_1,\dots,p_r) : p(\alpha) = 0\}.$$

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 $s = \operatorname{gr\,tr}_k k(y) \le n$ y k' es igual al cierre algebraico de un cuerpo de funciones racionales en 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 $z_1,\dots,z_s \in k'$ 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 $1 \le i \le s$. En efecto, sean $z_{s+1},\dots,z_n \in k'$ y $z'_{s+1},\dots,z'_n \in k'$ de modo que $z_1,\dots,z_n$ y $z'_1,\dots,z'_n$ sean bases de trascendencia de k'. Sea $\sigma : k(z'_1,\dots,z'_n) \to k(z_1,\dots,z_n)$, 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 $h : k(y)(z_{s+1},\dots,z_n) \to k'$ el morfismo definido por $h = g$ sobre $k(y)$ y $h(z_t) = z_t$, para todo $0 < t \le n - s$. Hemos obtenido el cierre algebraico de $k(y)(z_{s+1},\dots,z_n)$ 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 $\pi : A \to k(y)$ el morfismo natural, y sea $f = g \circ \pi : A \to k'$. Asignamos a $\mathfrak{p}_y$, $\bar{\alpha}$, siendo $\alpha := (f(\bar{x}_1),\dots,f(\bar{x}_n))$.

Ambas asignaciones son inversas entre sí.

□

1.2. Teorema de las funciones simétricas

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 $x_1,\dots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\dots,x_n]$ $(i = 1,\dots,n)$ 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:

$$\prod_i (x - x_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$$

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 verifica 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 sólo 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, $H(x_1,\ldots,x_n) = s_n \cdot H'(x_1,\ldots,x_n)$ y, por tanto, $H'(x_1,\ldots,x_n)$ es simétrico también y homogéneo de grado $gr(H') = gr(H) - n = gr(P) - n < gr(P)$, luego por recurrencia sobre el grado m de P se concluye que $H'(x_1,\ldots,x_n) = \widetilde{Q}(s_1,\ldots,s_n)$. 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 $\frac{P}{Q} \in k(x_1,\ldots,x_n)^{S_n}$. 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,

$$\frac{P}{Q} = \frac{\prod_{\sigma\in S_n} \sigma(P)}{Q \cdot \prod_{\mathrm{Id}\neq\sigma\in S_n} \sigma(P)} \in k(s_1,\ldots,s_n)$$

□

1.3. Teorema fundamental del Álgebra

1. 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 $\operatorname{gr} p(x) = r = 2^n \cdot m$, 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 $\alpha_1, \ldots, \alpha_r$ 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 $\alpha_1, \ldots, \alpha_n$, 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 $\alpha_r, \alpha_s = (a \pm \sqrt{a^2 - 4b})/2 \in \mathbb{C}$. □

1.4. Fórmulas de Newton y Girard

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0(x - \alpha_1)\cdots(x - \alpha_n) \in k[x]$.

1. Teorema: *Sea $P'(x)$ la derivada 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 $P'(x) = P(x)\cdot\sum_i \frac{\sigma_i}{x^{i+1}}$.

□

2. 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

$$\boxed{\sum_i f(\alpha_i) = \text{coeficiente en grado } n-1 \text{ de } f(x)P'(x) \bmod P(x)}$$

1.5. El discriminante de un polinomio

Sea $P(x) = \prod_{i=1}^n (x - x_i) = x^n + a_1 x^{n-1} + \cdots + a_n$.

1. 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:

2. Proposición: *El discriminante de un polinomio sobre un cuerpo es cero si y sólo 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:

$$\frac{P'(x)}{P(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \frac{\sigma_2}{x^3} + \cdots$$

3. Teorema:

$$\Delta(P) = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

Demostración. Sea 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

$$V^2 = \left|\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} \circ \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_1 & \cdots & x_1^{n-1} \end{pmatrix}\right| = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

□

4. 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 $\Delta = -4(b - \frac{1}{3}a^2)^3 - 27(\frac{2}{27}a^3 - \frac{1}{3}ab + c)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

□

5. 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, $sig(\sigma) = -1$), entonces:

$$P = \frac{1}{2}((P + \sigma(P)) + (P - \sigma(P)))$$

y basta ver que $Q^+ := P+\sigma(P) \in \mathbb{Z}_2[a_1,\dots,a_n]$ y $Q^- := P-\sigma(P) \in \sqrt{\Delta}\cdot\mathbb{Z}_2[a_1,\dots,a_n]$. 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 $S,T \in \mathbb{Z}_2[a_1,\dots,a_n]$ 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,

$$Q^- = \pm\frac{1}{2^n} S\cdot\sqrt{\Delta} \in \sqrt{\Delta}\cdot\mathbb{Z}_2[a_1,\dots,a_n]$$

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, $\frac{Q^-}{\sqrt{\Delta}} \in \mathbb{Q}(a_1,\dots,a_n)$ y $Q^- = \sqrt{\Delta}\cdot\frac{Q^-}{\sqrt{\Delta}} \in \sqrt{\Delta}\cdot\mathbb{Q}(a_1,\dots,a_n)$. Ahora se procede como en el caso anterior.

□

Caso real: $k = \mathbb{R}$

6. Teorema: *Si $P(x) \in \mathbb{R}[x]$, entonces*

1. $\Delta(P) = 0$ *si y sólo si $P(x)$ tiene una raíz doble.*
2. $\Delta(P) < 0$ *si y sólo 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 sólo 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 1.5.2.

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 $(\alpha_i-\overline{\alpha}_i)^2 = (2i\,Im(\alpha_i))^2 = -4\,Im(\alpha_i)^2 < 0$.

□

1.6. Teoría de la eliminación: Resultante de dos polinomios

Sean $a_0,b_0,x_1,\dots,x_n,y_1,\dots,y_m$ variables independientes ($(n,m) \neq (0,0)$). Sean $s_1,\dots,s_n$ las funciones simétricas elementales en las variables $\{x_i\}_{i=1}^n$ y $\overline{s}_1,\dots,\overline{s}_m$ las funciones simétricas elementales en las variables $\{y_j\}_{j=1}^m$.

Si denotamos $a_i = (-1)^i a_0 s_i$ y $b_i = (-1)^i b_0 \overline{s}_i$, se verifica:

$$P(x) = a_0\prod_{i=1}^{n}(x-x_i) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$
$$Q(x) = b_0\prod_{j=1}^{m}(x-y_j) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

1. Observación: Los coeficientes $a_0,\dots,a_n,b_0,\dots,b_m$ son funciones algebraicamente independientes: la extensión $\mathbb{Q}(a_0,\dots,a_n,b_0,\dots,b_m) \hookrightarrow \mathbb{Q}(a_0,b_0,x_1,\dots,x_n,y_1,\dots,y_m)$ es algebraica, luego

$$\mathrm{gr\,tr}_{\mathbb{Q}}\,\mathbb{Q}(a_0,\dots,a_n,b_0,\dots,b_m) = \mathrm{gr\,tr}_{\mathbb{Q}}\,\mathbb{Q}(a_0,b_0,x_1,\dots,x_n,y_1,\dots,y_m) = n+m+2.$$

2. Definición: Llamaremos resultante genérica a la resultante de P y Q, es decir:

$$R(P,Q) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i-y_j)$$

3. 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. $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$ *y es homogéneo de grado* m *en las variables* a_i *y homogéneo de grado* n *en las* b_j.

Demostración. (1)

$$R(P,Q) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (-1)(y_i - x_j)$$
$$= (-1)^{nm} b_0^n a_0^m \prod_{j=1}^m \prod_{i=1}^n (y_i - x_j) = (-1)^{nm} R(Q,P)$$

(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 $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]_{a_0}$. De (1) se obtiene por la misma razón que $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]_{b_0}$. Por tanto, $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$.

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

$$\left.\begin{aligned} \overline{P}(x) &= \overline{a}_0 x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_n \\ \overline{Q}(x) &= \overline{b}_0 x^m + \overline{b}_1 x^{m-1} + \cdots + \overline{b}_m \end{aligned}\right\} \in \bar{A}[x], \quad \overline{a}_0, \overline{b}_0 \neq 0$$

4. Definición: $R(\overline{P},\overline{Q}) \in \bar{A}$ es el valor obtenido en la resultante genérica $R(P,Q)$ dando a las variables $\{a_0,\dots,a_n,b_0,\dots,b_m\}$ los valores $\{\overline{a}_0,\dots,\overline{a}_n,\overline{b}_0,\dots,\overline{b}_m\}$.

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 $R(\overline{P},\overline{Q}) = \bar{a}_0^m \bar{b}_0^n \prod_{i=1}^n \prod_{j=1}^m (\bar{x}_i - \bar{y}_j)$.

El interés de la resultante lo da el siguiente teorema.

5. Teorema: *Sea* k *un cuerpo. Dos polinomios* $\overline{P}(x),\overline{Q}(x) \in k[x]$*, tienen alguna raíz en común si y sólo si* $R(\overline{P},\overline{Q}) = 0$.

6. Ejercicio: Probar 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 $\mathrm{gr}(P_1P_2) = \mathrm{gr}(P_1) + \mathrm{gr}(P_2)$).

7. Teorema: *La resultante genérica* $R(P,Q)$ *(con* $gr\,P, gr\,Q > 0$*) es un polinomio irreducible como elemento de* $\mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$.

Demostración. En primer lugar $R(P,Q)$ 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 $R(P,Q) \neq 0 \bmod b_0$. 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 $H \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$, 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 $s = 0 = t$.

□

8. 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 sólo 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. Recíprocamente, sea $D(x) = m.c.d.(P,Q)$. Basta elegir, $\lambda(x) = \frac{Q(x)}{D(x)}, \overline{\mu}(x) = -\frac{P(x)}{D(x)}$ y se concluye. □

9. Lema : *Sea k un cuerpo y sean $P(x), Q(x) \in k[x]$ dos polinomios primos entre sí de grados n y m 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 $\mathrm{gr}\,\lambda(x) < \mathrm{gr}\,Q(x) = m$. Sea $\mu(x) = c(x) \cdot P(x) + \mu'(x)$. 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, $\lambda(x) - \lambda_2(x) = 0 = \mu(x) - \mu_2(x)$.

□

10. 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 S' no es divisible por R, a_0, ni b_0. Tenemos que probar que $S' = \pm 1$, $s = t = 0$ y $n = 1$. Sea $S' \in A$ irreducible, que divida a S y no a R, a_0 y b_0. Entonces, en el cuerpo de fracciones de $A/(S')$, 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

$$\lambda'(x) \cdot P(x) + \mu'(x) \cdot Q(x) = R(P,Q)^r$$

Si $r > 1$, derivando respecto de a_n, tenemos

$$\lambda'(x)' \cdot P(x) + \lambda'(x) + \mu'(x)' \cdot Q(x) = r \cdot R(P,Q)^{r-1} \cdot R(P,Q)'$$

Por tanto, 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 $K = \mathbb{Q}(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1})$, 0 es la única raíz común de $P(x)$ y $Q(x)$. Ahora bien, $\lambda'(x) = \lambda \cdot (Q(x)/x)$ y $\mu(x) = -\lambda(P(x)/x)$ para cierto $\lambda \in K$, y el 0 no es una raíz de $\lambda'(x)$. Hemos llegado a contradicción y $r = 1$.

□

11. 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.

□

12. 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: Si f_1 y f_2 son múltiplos de $R(P,Q)$ entonces $R(P,Q)$ divide a S. Supongamos que f_1 ó f_2 no es múltiplo de $R(P,Q)$. 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, $R(P,Q) \in (P,Q) \cap A$.

□

1.6.1. Métodos de cómputo de la resultante

Vamos a dar algoritmos explícitos de cómputo de la resultante.

A. Resultante de Euler:

Sean $P(x) = \sum_{i\geq 0}^{n} a_i x^i$ y $Q(x) = \sum_{i\geq 0}^{m} b_i x^i \in k[x]$.

Por el lema de Euler, estos polinomios tienen una raíz común si y sólo 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 subespacio $k[x]_{<s}$ la base $\{x^{s-1}, x^{s-2}, \ldots, x, 1\}$, y calculando el determinante de esta aplicación lineal en dichas bases, resulta la condición:

$$\mathscr{E}(P,Q) := \begin{vmatrix} a_0 & & \cdots & a_n & & 0 \\ & \ddots & & & \ddots & \\ 0 & & a_0 & & \cdots & a_n \\ b_0 & \cdots & & b_m & & 0 \\ & \ddots & & & \ddots & \\ 0 & & b_0 & \cdots & & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \end{matrix} = 0$$

13. Definición : Diremos que $\mathscr{E}(P,Q)$ es la resultante de Euler (también llamada de Cayley y de Sylvester).

14. 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 $\mathscr{E}(P,Q)$ tiene que ser múltiplo de la resultante como polinomio en las raíces, ya que $\mathscr{E}(P,Q)$ se anula si se hace $x_i = y_j$ (pues entonces P y Q tendrían la raíz común x_i). 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 escalar. 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 escalar es 1.

□

15. Observación: Es fácil ver que este teorema es válido aunque los coeficientes de los polinomios sean de un anillo y no de un cuerpo.

B. Resultante de Bézout:

16. 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, $\overline{Q(x)}=(Q(x_1),\ldots,Q(x_n))$ 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, $a_0^m\cdot|Q(x)\cdot|=R(P,Q)$. □

Consideremos en $k[x]/(P(x))$ las bases $\{a_0, a_0\cdot x+a_1,\ldots,a_0x^{n-1}+\cdots+a_{n-1}\}$ y $\{1,x,\ldots,x^{n-1}\}$ y supongamos que $n=m$. Observemos que

$$Q(x)\cdot(a_0x^i+\cdots+a_i)-P(x)\cdot(b_0x^i+\cdots+b_i)=\sum_{j=0}^{n-1} c_{ij}x^j$$

para ciertos $c_{ij}\in k$ y todo i. Entonces, es fácil ver que

$$R(P,Q)=a_0^m\cdot|Q(x)\cdot|=|(c_{ij})|$$

17. 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).

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 verifica 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:

$$\begin{aligned}R(P,Q)&=(-1)^{nm}R(Q,P)=(-1)^{nm}b_0^n\textstyle\prod_j P(y_j)\\&=(-1)^{nm}b_0^n\textstyle\prod_j R(y_j)=(-1)^{nm}b_0^nb_0^{-grR}R(Q,R)\end{aligned}$$

□

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,

$$R_i(x)=d_ix^{g_i}+\cdots$$

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.

□

1.6.2. 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:

$$\left.\begin{array}{l} P(x,y) = a_0(y)\cdot x^n + \cdots + a_{n-1}(y)\cdot x + a_0(y) = 0 \\ Q(x,y) = b_0(y)\cdot x^m + \cdots + b_{m-1}(y)\cdot x + b_0(y) = 0 \end{array}\right\} \quad a_0(y), b_0(y) \neq 0$$

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 sólo 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 $\bar{R}(y)$.

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 sólo si (a,b) es una solución del sistema de ecuaciones reales

$$\begin{array}{l} U(x,y) = 0 \\ V(x,y) = 0 \end{array}$$

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

$$\begin{array}{l} P_1(x_1,\ldots,x_n) = 0 \\ \cdots \\ P_n(x_1,\ldots,x_n) = 0 \end{array}$$

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 $1 < i \leq n$, 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 $R_2 = \ldots = R_n = 0$.

MANUALES UEX

D. Discriminante.

Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n$.

21. Teorema: *Si denotamos por* $P'(x) = nx^{n-1} + (n-1)a_1 x^{n-2} + \cdots + a_{n-1}$ *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:

$$R(P, P') = \prod_{j=1}^n P'(x_j) = \prod_{j=1}^n \prod_{i \neq j}^n (x_j - x_i) = \prod_{i<j} (x_i - x_j)(x_j - x_i)$$
$$= \prod_{i<j} -(x_i - x_j)^2 = (-1)^{\binom{n}{2}} \prod_{i<j} (x_i - x_j)^2 = (-1)^{\binom{n}{2}} \Delta(P)$$

□

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.

Pues bien,

$$\boxed{\frac{1}{Q(\alpha)} = \frac{1}{R(P,Q)} \cdot R\left(\frac{P(x)}{x - \alpha}, Q\right)}$$

En efecto, $R(P,Q) = R(\frac{P(x)}{x-\alpha}(x-\alpha), Q(x)) = R(\frac{P(x)}{x-\alpha}, Q(x)) \cdot R(x-\alpha, Q(x)) = R(\frac{P(x)}{x-\alpha}, Q(x)) \cdot Q(\alpha)$.

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:

$$\left.\begin{aligned} P(x) &= 0 \\ A(x) - B(x)y &= 0 \end{aligned}\right\}$$

siendo y otra letra.

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 $x = z^2$.)

1.6.3. Ejercicios y ejemplos

Ejemplo 1: Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calcular un polinomio de raíces $\alpha_i + \frac{1}{\alpha_i}$. Sea $y = x + \frac{1}{x}$, es decir, solución de la ecuación $x^2 - yx + 1 = 0$. 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: *Calcular el polinomio cuyas raíces son*

$$cos\,\frac{2k\pi}{5} \quad , \; k = 0,1,2,3,4$$

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

$$cos\,\frac{2k\pi}{5} = \frac{1}{2}(\varepsilon^k + \bar{\varepsilon}^k) = \frac{1}{2}(\varepsilon^k + \frac{1}{\varepsilon^k})$$

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 $sen\,\frac{2k\pi}{5}$, ya que $sen\,\frac{2k\pi}{5} = \frac{1}{2i}(\varepsilon^k - \varepsilon^{-k})$ y se aplica el método del ejemplo 2.

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 $d_0 = 1, d_1 = 2, d_2 = -\frac{a^2}{4} + b$:

$$\Delta = R(P, P') = (-1)^{\binom{2}{2}}(-1)^{2\cdot 1 + 1\cdot 0} \cdot 2^{2-0}(-\frac{a^2}{4} + b)^{1-0} = a^2 - 4b$$

Ejemplo 6: El discriminante de $x^3 + px + q$ es $\Delta = -(4p^3 + 27q^2)$.

Solución: $R_0(x) = x^3 + px + q, R_1(x) = P'(x) = 3x^2 + p, R_2(x) = \frac{2}{3}px + q, R_3(x) = R_2(-\frac{3}{2}\frac{q}{p}) = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$, luego $g_0 = 3, g_1 = 2, g_2 = 1, g_3 = 0$ y $d_0 = 1, d_1 = 3, d_2 = \frac{2}{3}p, d_3 = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$:

$$\Delta = R(P, P') = (-1)^{\binom{3}{2}}(-1)^{3\cdot 2 + 2\cdot 1 + 1\cdot 0} \cdot 3^{3-1}(\frac{2}{3}p)^{2-0}(\frac{3^3}{2^2}\frac{q^2}{p^2} + p) = -(4p^3 + 27q^2)$$

1.7. Exceso. Polinomios de Sturm. Separación de raíces

1.7.1. Acotación de las raíces

1. Sea $P(x) = a_0x^n + \cdots + a_n \in \mathbb{C}[x]$. Queremos encontrar un número real $L > 0$, que llamaremos cota de $P(x)$, de modo que si $z \in \mathbb{C}$ es una raíz compleja de $P(x)$ entonces $|z| < L$.

Dividiendo por a_0, podemos suponer que $a_0 = 1$. Sea $M = \text{máx}\{|a_1|, \ldots, |a_n|\}$

Cota de Mac-Laurin: Una cota de $P(x)$ es $L = 1 + M$, porque si $|z| \geq L$,

$$|P(z)| \geq |z|^n - |a_1||z|^{n-1} - \cdots - |a_n| \geq |z|^n - (|z| - 1)|z|^{n-1} - \cdots - (|z| - 1) = |z|^n - \frac{(|z| - 1)|z|^n - (|z| - 1)}{|z| - 1} = 1$$

2. Sea $P(x) = x^n + a_1x^{n-1} \cdots + a_n \in \mathbb{R}[x]$. Queremos un número real $L > 0$, que llamaremos cota superior de $P(x)$, de modo que si $r \in \mathbb{R}$ es una raíz real de $P(x)$ entonces $r < L$.

Cota superior de Lagrange: Si a_s es el primer coeficiente no negativo, una cota superior de $P(x)$ es $L = 1 + \sqrt[s]{M}$, porque si $r \geq L$,

$$\begin{aligned} P(r) &= r^n + a_1r^{n-1} + \cdots + a_n \geq r^n - (r-1)^s r^{n-s} - \cdots - (r-1)^s = r^n - \frac{(r-1)^s r^{n-s+1} - (r-1)^s}{r-1} \\ &= r^n - (r-1)^{s-1} \cdot (r^{n-s+1} - 1) \geq 0 \end{aligned}$$

1.7.2. Exceso de una función racional real

En esta subsección los polinomios 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 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 del polo en 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 (sin polos en a ni b) 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. Definición: Dados números reales no nulos $a_1,\dots,a_n$ llamaremos variaciones de signo de dicha sucesión al número:

$$V(a_1,\dots,a_n)=\sum_i V(a_i,a_{i+1})$$

siendo $V(a,b)=\begin{cases} 1 \text{ si } sig\, a\neq sig\, b \\ 0 \text{ si } sig\, a=sig\, b \end{cases}$. Si algún término a_i se anula se define igualmente las variaciones de signo suprimiendo los términos nulos.

Dados dos números reales a,b y n polinomios reales $P_1,\dots,P_n$, denotaremos:

$$V_a^b(P_1,\dots,P_n)=V(P_1(a),\dots,P_n(a))-V(P_1(b),\dots,P_n(b))$$

6. Observación: Si $c\neq 0\neq d$, entonces $V(c,d)=\frac{1}{2}(1-sig(cd))$ y en particular:

$$V_a^b(P,Q)=\frac{1}{2}(sig(P(b)Q(b))-sig(P(a)Q(a)))$$

7. Teorema: *Si P,Q son 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. Por tanto, es claro que $E_a^b(\frac{P}{Q})+E_a^b(\frac{Q}{P})=E_a^b(\frac{P}{Q}+\frac{Q}{P})$. Ahora bien, $\frac{P}{Q}+\frac{Q}{P}=\frac{P^2+Q^2}{PQ}$ y, por ser P^2+Q^2 una función estrictamente positiva es claro que

$$E_a^b(\frac{P}{Q}+\frac{Q}{P})=E_a^b(\frac{P^2+Q^2}{PQ})=E_a^b(\frac{1}{PQ})$$

Ahora bien, como $E_a^b(\frac{1}{PQ})$ es el número de veces que PQ pasa de negativo a positivo menos el número de veces que pasa de positivo a negativo y por el teorema de Bolzano el signo de un polinomio permanece constante entre cada raíz y su contigua se concluye que dicha diferencia coincide con $\frac{1}{2}(sig((PQ)(b))-sig((PQ)(a)))\overset{1.7.6}{=\!=}V_a^b(P,Q)$.

□

1.7.3. Vueltas de una curva alrededor del origen. Teorema de D'Alambert

8. Definición: Llamaremos **curva racional** en $\mathbb{C}$ a cualquier aplicación $\sigma:[a,b]\to\mathbb{C}$ definida a trozos por funciones racionales, es decir, una aplicación $\sigma(t)=u(t)+iv(t)$ (con u y v funciones reales) tal que existen un número finito de puntos $a=a_0<a_1<\cdots<a_n=b$ 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 $\sigma(a)=\sigma(b)$ y diremos que además es **simple** cuando la identidad anterior se da únicamente en los extremos a y 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.

9. 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 $x\le c_1$).

Otro ejemplo trivial es un segmento en $\mathbb{C}$ (usando las ecuaciones paramétricas de las rectas). Por tanto, cualquier polígono es un circuito.

10. Definición: Diremos que una curva σ pasa por un punto $z\in\mathbb{C}$ cuando $z\in\operatorname{Im}\sigma$.

11. Definición: Dado un circuito $\sigma\colon[a,b]\to\mathbb{C}$ que no pasa por el origen, llamaremos número de vueltas alrededor del origen (en el sentido de las agujas del reloj) al número:

$$\mathrm{v}(\sigma)=\frac{1}{2}E_a^b\frac{v(t)}{u(t)}$$

siendo $\sigma(t)=u(t)+iv(t)$.

12. Observación: (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, $\sigma(t)$ 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 contabiliza es el número de vueltas en el sentido de las agujas del reloj menos el número de vueltas en sentido contrario.

13. 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 una de ellas:*

$$v(\sigma_1(t)\cdot\sigma_2(t))=v(\sigma_1(t))+v(\sigma_2(t))$$

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 $\mathrm{v}(\sigma(t))=\frac{1}{2}E_a^b\frac{u(t)}{v(t)}=\frac{1}{2}E_a^bf(t)$ (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,

$$\frac{1}{2}E_a^b\frac{f_1f_2-1}{f_1+f_2}=-\frac{1}{2}E_a^b\frac{1}{f_1+f_2}=\frac{1}{2}E_a^b(f_1+f_2)=\frac{1}{2}E_a^bf_1+\frac{1}{2}E_a^bf_2=\mathrm{v}(\sigma_1(t))+\mathrm{v}(\sigma_2(t))$$

En el caso de que $\sigma_1(t),\sigma_2(t)$ corten simultáneamente el eje OY, modificando ligeramente $\sigma_2(t)\mapsto\sigma_2(t+\epsilon)$ se obtiene que el número de vueltas de $\sigma_1(t)\cdot\sigma_2(t+\epsilon)$ es $\mathrm{v}(\sigma_1(t))+\mathrm{v}(\sigma_2(t+\epsilon))=\mathrm{v}(\sigma_1(t))+\mathrm{v}(\sigma_2(t))$. Luego aproximando $\epsilon\to0$ se concluye. □

14. Teorema : *Sea $P(z)$ un polinomio con coeficientes complejos y $\sigma(t)$ 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 de raíces de $P(z)$ (contadas con su multiplicidad) contenidas en el interior del rectángulo coincide con el número de vueltas de $P(\sigma(t))$:*

$$r_\sigma(P(z)) = v(P(\sigma(t)))$$

siendo $r_\sigma(P(z))$, el número de raíces contenidas en el interior del rectángulo σ.

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, $\mathrm{v}(P(\sigma(t))) = \mathrm{v}(H) + \sum_i r_i \cdot \mathrm{v}(z-\alpha_i) = \mathrm{v}(H) + \sum_i r_i$.

Sólo 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, $M = 1 + \text{máx}\{|a_1|,\dots,|a_n|\}$ 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 el teorema fundamental del Álgebra.

15. 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. □

1.7.4. Polinomios de Sturm

Sean P, Q y consideremos los restos R_i obtenidos en el algoritmo de Euclides (cambiados de signo):

$$\begin{aligned}
&P = C_1 Q - R_1\\
&Q = C_2 R_1 - R_2\\
&\cdots\\
&R_{n-2} = C_n R_{n-1} - R_n\\
&R_{n-1} = C_{n+1} R_n
\end{aligned}$$

16. Teorema: *Si P,Q son dos polinomios reales y 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 ni en a ni en b.

En primer lugar se puede suponer que P y Q son primos entre sí, ya que los términos de la igualdad no cambian al suprimir un factor común. Procedamos por inducción sobre n. Para $n=0$, $E_a^b \frac{Q}{P} \overset{1.7.7}{=\!=} V_a^b(P,Q) - E_a^b \frac{P}{Q} = V_a^b(P,Q)$. De la igualdad $P = C_1 Q - R_1$ 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 é inducción se obtiene:

$$\begin{aligned} E_a^b \frac{Q}{P} &\overset{1.7.7}{=\!=} V_a^b(P,Q) - E_a^b \frac{P}{Q} = V_a^b(P,Q) + E_a^b \frac{R_1}{Q} \\ &= V_a^b(P,Q) + V_a^b(Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n) \end{aligned}$$

(2) Supongamos que Q o algún resto de Sturm se anula en a (igualmente para b):

Se observa que no puede haber dos términos consecutivos anulándose en a (o en b), pues entonces $x-a$ sería divisor del máximo común divisor de estos y, por tanto de P, contradiciendo la hipótesis del teorema. Por otro lado, si $R_i(a)=0$, entonces como $R_{i-1} = C_{i+1}R_i - R_{i+1}$, se obtendría que $R_{i-1}(a)$ y $R_{i+1}(a)$ son de signo contrario. Modificando $a \rightsquigarrow a' = a + \epsilon$ ligeramente de manera que no se modifique el exceso, ningún resto se anule (y por tanto, se verifique el teorema) y los no nulos no cambien de signo, se tendría que $V(R_{i-1}(a'),R_i(a'),R_{i+1}(a')) = V(R_{i-1}(a),R_i(a'),R_{i+1}(a)) = 1 = V(R_{i-1}(a),R_{i+1}(a))$, ya que $R_i(a')$ tiene el mismo signo que $R_{i-1}(a)$ o que $R_{i+1}(a)$. Es decir,

$$E_a^b \frac{Q}{P} = E_{a'}^{b'} \frac{Q}{P} \overset{(1)}{=} V_{a'}^{b'}(P,Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n)$$

□

17. Teorema de Sturm: *Sean $\{R_i\}_i$ los restos de Sturm para P y su derivada P'. Si P no se anula en a ni en b entonces verifica:*

$$N^o \text{ de raíces reales distintas de } P \text{ en } [a,b] = V_a^b(P,P',R_1,\ldots,R_n)$$

Demostración. De la igualdad:

$$\frac{P'}{P} = \sum_i \frac{n_i}{x-\alpha_i}$$

siendo n_i la multiplicidad de la raíz α_i en P, se obtiene que si α_i es real, entonces $E_{\alpha_i} \frac{P'}{P} = 1$. Por tanto, el número de raíces distintas en $[a,b]$ coincide con $E_a^b \frac{P'}{P}$ y se concluye por el teorema anterior.

□

18. 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 y calcularlas aproximadamente[1]: 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 separar las raíces distintas y calcularlas aproximadamente.

19. Si $V(P(a),P(b)) = 1$, 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 $V(P(a),P(\frac{a+b}{2})) = 1$. 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 por Análisis Numérico.

20. Si sabemos calcular o separar 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 $Q(x) = m.c.d.(P(x), \overline{P(x)}) \in \mathbb{R}[x]$). Las raíces reales de $p(x) \in \mathbb{C}[x]$ coinciden con las raíces reales de $Q(x) \in \mathbb{R}[x]$.

[1] No hacemos un análisis de la dificultad intrínseca del cálculo de los polinomios de Sturm.

1.7.5. Teorema de Budan-Fourier. Teorema de Descartes

El teorema de Budan-Fourier se basa en la observación:

$$\pm E_a^b \frac{Q}{P} \leq r_a^b(P)$$

siendo $r_a^b(P)$ el número de raíces reales de P (contadas con su multiplicidad) en $[a,b]$. Además, como $1 = -1 \, mod\, 2$, se verifica la igualdad $E_a^b \frac{Q}{P} = r_a^b(P) \, mod\, 2$ (siendo P y Q primos entre sí).

21. Teorema de Budan-Fourier: *Sea P un polinomio con coeficientes reales que no se anula en a ni en b. Se verifica la acotación:*

$$r_a^b(P) \leq V_a^b(P, P', P'', \ldots, P^{n)})$$

siendo n el grado de P, r_a^b el número de raíces reales de P en $[a,b]$ (contadas con su multiplicidad). Además es una igualdad módulo 2.

Demostración. Procedemos por recurrencia sobre el grado n del polinomio P. Si $n = 1$ entonces $P'/P = 1/(x-\alpha)$ y $r_a^b(P) = E_a^b \frac{P'}{P} \overset{1.7.7}{=\!=} V_a^b(P,P') - E_a^b \frac{P}{P'} = V_a^b(P,P')$.

(1) Supongamos que P tiene todas sus raíces simples y que P y sus derivadas no se anula ninguna en a ni en b.

$$\begin{aligned} r_a^b(P) = E_a^b \frac{P'}{P} &\overset{1.7.7}{=\!=} V_a^b(P,P') - E_a^b \frac{P}{P'} \leq V_a^b(P,P') + r_a^b(P') \\ &\leq V_a^b(P,P') + V_a^b(P', P'', \ldots, P^{n)}) = V_a^b(P, P', P'', \ldots, P^{n)}) \end{aligned}$$

Las desigualdades son igualdades módulo 2 por serlo la primera (por lo dicho antes) y serlo la segunda por recurrencia.

(2) Supongamos ahora, sólo, que P y sus derivadas no se anulan en a ni en b. Sustituyendo cada factor $(x-\alpha_i)^{s+1}$ de P 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 de P se anula en a (igualmente en b). Haciendo el cambio $x' = x - a$ se puede suponer $a = 0$. Haciendo el cambio $a = 0 \rightsquigarrow \epsilon > 0$ se puede suponer que los términos no nulos mantienen su signo, que el número de raíces de P en (ϵ, b) es el mismo y que no se anula ninguna derivada (en ϵ). Luego basta ver que $V(P(\epsilon), P'(\epsilon), \ldots, P^{n)}(\epsilon))$ coincide con la variaciones en 0 suprimiendo los términos nulos. Supongamos que

$$P^{i)}(0) = \lambda \neq 0, \quad P^{i+1)}(0) = \cdots = P^{i+h)}(0) = 0, \quad P^{i+h+1)}(0) = h!\mu \neq 0$$

Entonces es $P^{i)}(x) = \lambda + x^h(\mu + \gamma x + \cdots)$ 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 $r \leq h+1$. Por tanto, para ϵ suficientemente pequeño es $sig\, P^{i)}(\epsilon) = sig\, \mu$, de donde:

$$V(P^{i)}(\epsilon), P^{i+1)}(\epsilon), \ldots, P^{h)}(\epsilon), P^{h+1)}(\epsilon)) = V(\lambda, \mu, \ldots, \mu, \mu) = V(\lambda, \mu) = V(P^{i)}(0), P^{i+h+1)}(0))$$

y se concluye. □

22. Teorema de Descartes: *Sea $P(x) = a_0 x^n + \cdots a_{n-1}x + a_n \in \mathbb{R}[x]$ sin la raíz 0 (i.e. $a_n \neq 0$). Denotemos por $r^+(P)$ el número de raíces (reales) positivas de P (contada cada una con su multiplicidad). Entonces,*

$$r^+(P) \leq V(a_0, a_1, \ldots, a_n)$$

y es una igualdad módulo 2 (es decir, ambos números tienen la misma paridad).

Demostración. Basta aplicar el teorema de Budan-Fourier ya que $r^+(P) = r_0^{+\infty}(P)$ y tener en cuenta que $a_i = P^{n-i)}(0)/(n-i)!$ y que $sig\, P^{i)}(+\infty) = sig\, a_0$ (es decir, no depende de i y, por tanto, sus variaciones son nulas).

□

Si denotamos $r^-(P)$ el número de raíces (reales) negativas de P (contada cada una con su multiplicidad), haciendo el cambio $x \mapsto -x$ y aplicando el teorema de Descartes se concluye:

$$r^-(P) \le V(a_0, -a_1, \ldots, (-1)^n a_n)$$

23. Corolario: *Si P tiene todas sus raíces reales (y no nulas), entonces:*

$$r^+(P) = V(a_0, a_1, \ldots, a_n) \quad y \quad r^-(P) = V(a_0, -a_1, \ldots, (-1)^n a_n)$$

y además $P(x)$ no puede tener ternas de coeficientes consecutivos nulos.

Demostración. Sean $a_{i_1}, \ldots, a_{i_r}$ los coeficientes no nulos de $P(x)$ (por tanto, $i_1 = 0, i_r = n$). Por el teorema de Descartes es:

$$\begin{aligned} n = r^+(P) + r^-(P) &\le V(a_0, a_1, \ldots, a_n) + V(a_0, -a_1, \ldots, (-1)^n a_n) \\ &= \sum_j V(a_{i_j}, a_{i_{j+1}}) + V(a_{i_j}, (-1)^{i_{j+1}-i_j} a_{i_{j+1}}) \end{aligned} \qquad (*)$$

Es fácil ver que se verifica la desigualdad $V(a,b) + V(a,(-1)^i b) \le i$ (para todo $i \ge 1$) y que si se da la igualdad, entonces $i \le 2$. Por tanto, $n \le \sum_j V(a_{i_j}, a_{i_{j+1}}) + V(a_{i_j}, (-1)^{i_{j+1}-i_j} a_{i_{j+1}}) \le \sum_j (i_{j+1} - i_j) = i_r - i_0 = n - 0 = n$, luego $n = \sum_j V(a_{i_j}, a_{i_{j+1}}) + V(a_{i_j}, (-1)^{i_{j+1}-i_j} a_{i_{j+1}})$ y no hay ternas de coeficientes consecutivos nulos. Por tanto, se verifica la igualdad de cada sumando de la primera desigualdad $(*)$, es decir, lo que enuncia el corolario.

□

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 sólo si todos los autovalores son estrictamente positivos. Por el corolario, la métrica simétrica es euclídea si y sólo 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.

1.8. 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 $\alpha = \bar{x}$. Racionalizar $1/(\alpha + 2)$ y determinar si $(2 + \alpha)^3$ es la unidad. ¿Tiene el polinomio $x^2 - 2$ alguna raíz en K?. Calcular un polinomio no nulo con coeficientes racionales $p(x)$ que admita la raíz $\beta = \alpha^2 + 1$.

3. Si $a, b \in \mathbb{Q}$, demostrar que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ precisamente cuando a/b sea un cuadrado en $\mathbb{Q}$.

4. Probar que $\mathbb{Q}(\sqrt[n]{2})$ tiene grado n sobre $\mathbb{Q}$.

5. Determinar 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. Demostrar que $x^3 - 3$ no tiene raíces en $k = \mathbb{Q}(\sqrt{2})$. Concluir que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ es una extensión de grado 6 de $\mathbb{Q}$ y hallar una base sobre $\mathbb{Q}$.

   Sea $\alpha = \sqrt{2} + \sqrt[3]{3}$. Probar que el grado de un polinomio irreducible en $\mathbb{Q}[x]$ que admita la raíz α es $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1, 2, 3,$ 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. Calcular tal polinomio.

8. Sea $K = \mathbb{F}_2[x]/(x^3+x+1)$ y sea $\alpha = \bar{x}$. Probar que K es un cuerpo con 8 elementos

$$K = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$$

Calcular 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. Calcular 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. Hallar 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. Calcular 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, probar que $K = k(\sqrt{a}$ para algún $a \in k$. ¿Es cierto también cuando $\operatorname{car} k = 2$?

14. Hallar 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 $p_1(x), \ldots, p_n(x) \in \mathbb{Q}[x]$. Demostrar 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 sólo 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. Probar 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. Probar 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 $\mathbb{C} \times \overset{n}{\ldots} \times \mathbb{C}$. ¿Es cierto que toda $\mathbb{C}$–álgebra finita es trivial?

21. Probar 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 $\mathbb{R} \times \overset{n}{\ldots} \times \mathbb{R} \times \mathbb{C} \times \overset{m}{\ldots} \times \mathbb{C}$ para ciertos $n, m \in \mathbb{N}$.

22. Determinar 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. Determinar 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 $k = \mathbb{Q}(\sqrt[5]{5})$. Probar que el polinomio irreducible de $e^{\frac{2\pi i}{5}}$ sobre k es $x^4+x^3+x^2+x+1$.

Determinar 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. Probar que α es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$. Probar 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. Probar 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. Probar 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. Probar 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. Hallar 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. Encontrar los números complejos x, y, z tales que $x + y + z = 1$, $xyz = 1$ y $|x| = |y| = |z| = 1$.

30. Resolver la ecuación $x^3 - 3\lambda x^2 + 4 = 0$ sabiendo que dos de sus raíces son iguales.

31. Resolver la ecuación $x^3 - 5x^2 + 16x + 8 = 0$ sabiendo que la suma de dos de sus raíces es 0.

32. Resolver la ecuación $x^3 - 9x^2 + 23x - 15 = 0$ sabiendo que sus raíces forman una progresión aritmética.

33. Calcular 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. Expresar 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. Expresar 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. Calcular 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. Calcular 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. Calcular 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. Calcular el valor de la suma: $\sum_{k=1}^4 \frac{3\varepsilon^{3k} + 2\varepsilon^{2k} + \varepsilon^k}{\varepsilon^{2k} + \varepsilon^k + 1}$

41. Calcular 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. Calcular $\prod_{i=1}^n(\varepsilon_i^2 + 1)$ siendo $\{\varepsilon_i\}$ las raíces n-ésimas de la unidad.

43. Calcular la suma $s = \sum_{k=1}^{n-1} k\, cos(\frac{2k\pi}{n})$.

44. Calcular 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. Calcular la suma $\sum_{k=1}^{6} \frac{1}{sen^2 \frac{k\pi}{7}}$.

46. Calcular $\prod_{k=1}^{m-1} sen\, \frac{k\pi}{2m}$.

47. Calcular $\sum_{i\neq j\neq k} \frac{\alpha_i^2}{\alpha_j+\alpha_k}$, donde $\{\alpha_i\}$ son las raíces de x^3+x^2-2x-1.

48. Sea $P(x) \in \mathbb{C}[x]$. Probar 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, demostrar 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. Probar que el polinomio $P(x) = \frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1$ no tiene raíces múltiples.

51. Determinar 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. Demostrar 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. Hallar los valores de m para los cuales $(x+1)^m - x^m - 1$ es divisible por x^2+x+1.

54. Hallar el discriminante de $\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1$.

55. Demostrar que el discriminante de $x^n + qx + p$ es

$$(-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

MANUALES UEX

Capítulo 2

Teoría de Galois

2.1. Introducción

Consideremos un polinomio con coeficientes racionales $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$. 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 y sólo 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 sólo 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, sólo 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

$$\alpha_i = \frac{1}{3}\Bigg(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\Bigg)$$

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, $\mathbb{Q} = \mathbb{Q}(\alpha_1,\dots,\alpha_n)^G$. 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 $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$,

$$\mathbb{Q} = \mathbb{Q}(\alpha_1,\dots,\alpha_n)^G \subset \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_{s-1}} \subset \cdots \subset \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_1} \subset \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_0} = \mathbb{Q}(\alpha_1,\dots,\alpha_n)$$

El teorema 90 de Hilbert, prueba que existen $a_i \in \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_i}$ (calculables) tales que

$$\mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_{i-1}} = \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_i} + \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_i} \cdot \sqrt[p_i]{a_i} + \cdots + \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_i} \cdot (\sqrt[p_i]{a_i})^{p_i-1}$$

Así, $\alpha_1,\dots,\alpha_n \in \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ 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 $n < 50{,}000$ cumplen

$$n = 2^{m_1} \cdot 3^{m_2} \cdot 5^{m_3} \cdot 17^{m_4} \cdot 257^{m_5}, \qquad m_1 \geq 0,\ 0 \leq m_2,\dots,m_5 \leq 1$$

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 conmutativos $A = \mathbb{Q}[x_1,\dots,x_n]/(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))$ 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 sólo 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 sólo 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 sólo 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 y clasifica 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 $f^{-1}(U) = U \coprod \overset{n}{\ldots} \coprod U$. 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 $f^{-1}(U) := Y \times_X U = U \coprod \overset{n}{\ldots} \coprod U$.

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 0.3.60, $\mathrm{Spec}\, A = \{x_1, \ldots, x_n\}$ es un número finito de puntos cerrados y $A = A_{x_1} \times \cdots \times A_{x_n}$. Además, A es reducida si y sólo si es producto directo de un número finito de cuerpos y A es íntegra si y sólo si es cuerpo. Por último, si $f: A \hookrightarrow B$ es un morfismo de anillos inyectivo, entonces $f^*: \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ 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 0.2.33

$$k[x]/(p(x)) = k[x]/(x - \alpha_1) \times \overset{n}{\cdots} \times k[x]/(x - \alpha_n) = k \times \overset{n}{\cdots} \times k$$

es una k-álgebra trivial.

2. Ejercicio: Probar:

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, $A = K_1 \times \cdots K_r$ 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 $K_1 = K_1 \times 0 \times \cdots \times 0 \hookrightarrow A \hookrightarrow k^n \overset{\pi_i}{\to} k$ 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 sólo si A es trivial.

Demostración. Si $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$, entonces (0.3.54)

$$A = A_{x_1} \times \ldots \times A_{x_n}$$

Así pues, $\#\operatorname{Spec} A \leq \dim_k A$. Además, $\#\operatorname{Spec} A = \dim_k A$ si y sólo si $\dim_k A_{x_i} = 1$, para todo i, es decir, si y sólo 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 sólo si $A_{\text{red}} = A/(\operatorname{rad} A)$ 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 de $(\operatorname{rad} A) \otimes_k K$ son nilpotentes, luego $(A \otimes_k K)_{\text{red}}$ 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 $(A \otimes_k K)_{\text{red}}$ 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 $A = k[x]/(p(x))$. Probar que A es racional si y sólo si $p(x)$ descompone en producto de factores simples $(x-\alpha_i)$ (repetidos o no). Probar que $A \otimes_k K$ es una K-álgebra racional si y sólo si K contiene todas las raíces de $p(x)$.

Dado un punto racional $x \in \operatorname{Spec} A$ tenemos 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,

$$\operatorname{Hom}_{k-alg}(A,k) = \{\text{Puntos racionales de } A\} \subseteq \operatorname{Spec} A$$

10. Ejercicio: Demostrar la igualdad $\operatorname{Hom}_{k-alg}(k[x]/(p(x)),K) = \{\text{Raíces de } p(x) \text{ en } K\}$, $f \mapsto f(\bar{x})$.

11. Fórmula de los puntos: *Sea A una k-álgebra y $k \to K$ una extensión de cuerpos. Entonces*

$$\operatorname{Hom}_{k-alg}(A,K) = \operatorname{Hom}_{K-alg}(A \otimes_k K, K) = \{\textit{Puntos } K\textit{-racionales de } A \otimes_k K\}$$

En particular, $\#\operatorname{Hom}_{k-alg}(A,K) \leq \#\operatorname{Spec}(A \otimes_k K)$.

Demostración. Es consecuencia de 0.5.13. □

La fórmula de los puntos puede entenderse como la correspondencia biunívoca que hay entre los morfismos y sus gráficas (véase 5.12.17).

12. 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 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 $A \otimes_k K'' = K''^n$ y $\#\operatorname{Spec}(A \otimes_k K'') = n = \#\operatorname{Spec}(A \otimes_k K)$.

Si K' es una extensión racionalizante de A, sea K'' un compuesto de K y K'. Entonces, $\#\operatorname{Spec}(A \otimes_k K') = \#\operatorname{Spec}(A \otimes_k K'') = \#\operatorname{Spec}(A \otimes_k K)$.

□

13. Definición: Diremos que $\operatorname{Hom}_{k-alg}(A,K)$ 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 sólo si* $\#\operatorname{Hom}_{k-alg}(A,k) = \#\operatorname{Spec} A$. *Una extensión de cuerpos $k \hookrightarrow K$ racionaliza a A si y sólo si* $\#\operatorname{Hom}_{k-alg}(A,K) = \#\operatorname{Spec}(A \otimes_k K)$.

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 $n = \#\operatorname{Spec}(A \otimes_k K) = \#\operatorname{Hom}_{k-alg}(A,K)$. Dada una extensión de cuerpos $k \hookrightarrow \Sigma$ se cumple que*

$$\#\operatorname{Hom}_{k-alg}(A,\Sigma) \leq n$$

y se cumple la igualdad si y sólo si Σ racionaliza a A.

Demostración. Si $k \hookrightarrow K'$ racionaliza a A, entonces

$$\#\mathrm{Hom}_{k-alg}(A,K') = \#\mathrm{Spec}(A \otimes_k K') = \#\mathrm{Spec}(A \otimes_k K) = \#\mathrm{Hom}_{k-alg}(A,K).$$

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 racionalizado 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.*

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 sólo K la racionaliza. Por el Lema 2.2.15, K racionaliza a K si y sólo 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 0.3.57. □

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 sólo 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 también trivializa a A, porque $A \otimes_k \Sigma' = (A \otimes_k \Sigma) \otimes_\Sigma \Sigma'$.

4. Ejercicio: Probar:

- $A \times B$ es separable si y sólo 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 sólo 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 K-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 sólo 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 sólo 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 sólo 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 racionales. 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 K-racionales, 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 sólo 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

$$\varphi\colon \mathbb{Z} \to k,\ \varphi(n) = \begin{cases} 1 + \overset{n}{\dots} + 1 & \text{si } n > 0 \\ -\varphi(-n) & \text{si } n < 0 \\ 0 & \text{si } n = 0 \end{cases}$$

11. Definición: Si $\mathrm{Ker}\,\varphi = 0$, se dice que k es un cuerpo de característica cero. En este caso, tendremos una inyección canónica $\mathbb{Q} \hookrightarrow k$. Si $\mathrm{Ker}\,\varphi \neq 0$, entonces $\mathrm{Ker}\,\varphi = (p)$, 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 sólo 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. Notación: Sea k un cuerpo de característica $p > 0$ y A una k-álgebra finita. Denotemos $A^p := \{a^p \in A$, 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: $(k \cdot A^p) \otimes_k K = K \cdot (A \otimes_k K)^p$.

14. Proposición: *Sea k un cuerpo de característica $p > 0$ y A una k-álgebra finita. A es separable si y sólo 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 tanto, $A = k \cdot A^p$ si y sólo si $A = k$, es decir, si y sólo si A es separable. □

2.3.1. Cuerpos perfectos

15. Definición: Un cuerpo k se dice que es perfecto si y sólo si toda extensión finita de k es separable.

16. 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.

17. Proposición: *Sea k un cuerpo de característica $p > 0$. Entonces k es perfecto si y sólo 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 $x^p - a$, que sólo 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, α es separable y K es separable. □

2.3.2. Subálgebra separable maximal

18. 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 $\pi_0^k(A) = A$.

19. 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, $\pi_0^k(A) \subseteq k \cdot A^{p^n}$, 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 $\pi_0^k(A)$. □

20. 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 sólo si $k \cdot A^{p^n} = k$, para $n >> 0$.

21. 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 (que son nilpotentes), $\mu(\bar{a})p'(\bar{a}) = 1$, 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,

$$\pi_0^k(A/I) = \pi_0^k(A/I^2) = \pi_0^k(A/I^4) = ... = \pi_0^k(A/I^{2^m}) = \pi_0^k(A).$$

□

22. 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. □

23. Corolario: *Sea A una k-álgebra finita y K una extensión de k que racionalice a A. Entonces,*

$$\dim_k \pi_0^k(A) = \#\mathrm{Spec}(A \otimes_k K).$$

Demostración. En efecto,

$$\dim_k \pi_0^k(A) = \dim_K(\pi_0^k(A) \otimes_k K) = \dim_K(\pi_0^K(A \otimes_k K)) = \dim_K((A \otimes_k K)/\mathrm{rad}(A \otimes_k K)) = \#\mathrm{Spec}(A \otimes_k K).$$

□

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. 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 sólo si K racionaliza a A (en este caso $\mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{k-alg}(\pi_0^k(A),K)$).

Demostración. $\mathrm{Spec}(A \otimes_k K) = \mathrm{Spec}\,\pi_0^K(A \otimes_k K) = \mathrm{Spec}(\pi_0^k(A) \otimes_k K)$. Por tanto, el conjunto de los puntos K-racionales de $\mathrm{Spec}(A \otimes_k K)$ se inyecta en el conjunto de los puntos K-racionales de $\mathrm{Spec}(\pi_0^k(A) \otimes_k K)$ y se obtiene la desigualdad.

Si $A \otimes_k K$ es K-racional entonces $\pi_0^K(A \otimes_k K) = \pi_0^k((A \otimes_k K)_{red})$ es trivial y

$$\#\mathrm{Hom}_{k-alg}(A,K) = \mathrm{Spec}(A \otimes_k K) = \mathrm{Spec}(\pi_0^k(A) \otimes_k K) = \#\mathrm{Hom}_{k-alg}(\pi_0^k(A),K) = \dim_k \pi_0^k(A)$$

Por último, si $\#\mathrm{Hom}_{k-alg}(A,K) = \dim_k \pi_0^k(A)$, por 2.2.15, K racionaliza a A.

□

2.3.3. Métrica de la traza

26. 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

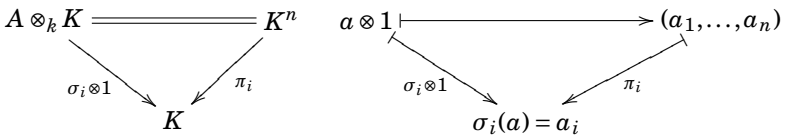
$$N: A \to k,\ a \mapsto N(a) := \det(h_a)$$

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 $(\sigma_1(a) \cdot \lambda, \ldots, \sigma_n(a) \cdot \lambda)$.

27. Proposición: *Sea A una k-álgebra finita separable. Sea K una extensión finita de cuerpos de k, que trivialice a A. Escribamos $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{k-alg}(A,K)$. Entonces,* $\mathrm{tr}(a) = \sum_i \sigma_i(a)$ *y* $N(a) = \prod_i \sigma_i(a)$.

Demostración. Consideremos isomorfismo $\phi: A \otimes_k K = K \times \overset{m}{\cdots} \times K$, $\phi(a \otimes 1) := (\sigma_1(a), \ldots, \sigma_n(a))$. Por tanto, $\mathrm{tr}(a) = Tr(h_a) = \mathrm{Tr}(h_{a \otimes 1}) = \mathrm{Tr}_{h_{(\sigma_1(a), \ldots, \sigma_n(a))}} = \sum_i \sigma_i(a)$ 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]

$$\begin{array}{ccc} A \otimes_k K & \xrightarrow{T_2^K} & A^* \otimes_k K = \mathrm{Hom}_K(A \otimes_k K, K) \\ \uparrow & & \uparrow \\ A & \xrightarrow{T_2^k} & A^* = \mathrm{Hom}_k(A,k) \end{array}$$

28. Proposición: *Sea A una k-álgebra finita. Entonces A es separable si y sólo si la métrica de la traza no tiene radical.*

Demostración. Tanto la separabilidad como el radical de la métrica cambian 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.

29. 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, si $T: E \to E$ es un endomorfismo cuyo polinomio característico tiene raíces $\alpha_1, \ldots, \alpha_n$, entonces el polinomio característico de $p(T)$ tiene raíces $p(\alpha_1), \ldots, p(\alpha_n)$. En particular, la traza de $p(T)$ es $p(\alpha_1) + \cdots + p(\alpha_n)$. Ahora, teniendo en cuenta que el polinomio característico de $h_x: k[x]/(p(x)) \to k[x]/(p(x))$ es precisamente $p(x)$, se cumple que

$$T_2^k(x^i, x^j) = Tr(h_{x^{i+j}}) = Tr(h_x^{i+j}) = \alpha_1^{i+j} + \cdots + \alpha_n^{i+j} = \sigma_{i+j}$$

y se concluye.

Consideremos, ahora, la matriz

$$B = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

Es claro que

$$B \cdot B^T = \begin{pmatrix} \sigma_0 & \sigma_1 & \ldots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \ldots & \sigma_n \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_{n-1} & \sigma_n & \ldots & \sigma_{2n-2} \end{pmatrix}$$

luego

$$|T_2^k| = |B|^2$$

30. Ejercicio: Pruébese que $|B| = \prod_{i>j} (\alpha_i - \alpha_j)$, y por tanto

$$|T_2^k| = \Delta$$

siendo $\Delta = \prod_{i>j} (\alpha_i - \alpha_j)^2$.

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 sólo 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 sólo 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 $k[x]/p(x) \otimes \overset{n}{\cdots} \otimes k[x]/p(x)$) 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 sólo 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 sólo 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 $p\mathbb{Z}$, con $p > 0$, primo. Por tanto, K es una $\mathbb{Z}/p\mathbb{Z}$ extensión finita de cuerpos. 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, sólo 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 Frobenius* 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 Frobenius,*

$$\mathrm{Aut}_{k-alg} K =< F^n >$$

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 $\mathrm{Id} \overset{\theta'}{\simeq} F' \circ F$.

Tenemos el morfismo natural $\theta_A : A \to (F \circ F')(A) = \mathrm{Aplic}(\mathrm{Hom}_{k-alg}(A, k), k)$, $\theta_A(a) := \tilde{a}$, 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 el caso $A = k$ que es obvio.

En conclusión, $\mathrm{Id} \overset{\theta}{\simeq} F \circ F'$.

Tenemos el morfismo natural $\theta'_X : X \to (F' \circ F)(X) = \mathrm{Hom}_{k-alg}(\mathrm{Aplic}(X, k), k)$, $\theta'_X(x) := \tilde{x}$, 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 el caso $X = \{x\}$ que 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 morfismo 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*

$$F\colon \mathscr{C}_{G-Conj} \rightsquigarrow \mathscr{C}_{GK-Trv},\ F(X) := \mathrm{Aplic}(X,K),$$

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*

$$F'\colon \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{G-Conj},\ F'(A) := \mathrm{Hom}_{K-alg}(A,K) = \mathrm{Spec}\,A,$$

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 $B^G := \{b\in B\colon g(b)=b,$ 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

$$\begin{array}{ccccccc} 0 & \to & B^G & \to & B & \to & B\oplus \overset{G}{\ldots}\oplus B \\ & & & & b & \to & (g(b))_{g\in G} \end{array}$$

es exacta, luego

$$0\to B^G\otimes_A C\to B\otimes_A C\to (B\otimes_A C)\oplus \overset{G}{\ldots}\oplus (B\otimes_A C)$$

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. $B\otimes_k K = B\otimes_K (K\otimes_k K) = B\otimes_K \prod^G K = \prod^G B$. 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. Como $(\prod^G B)^G = \{(g(b))_{g\in G}\in \prod^G B,$ con $b\in B\} = B$, entonces

$$B^G\otimes_k K = (B\otimes_k K)^G = (\overset{G}{\prod} B)^G = B$$

□

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 $H = \{g\in G\colon g(\lambda)=\lambda,\ \forall\lambda\in K'\}$. 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*

$$H\colon \mathscr{C}_{K/k} \rightsquigarrow \mathscr{C}_{GK-Trv},\ H(A) := A\otimes_k K, \quad H'\colon \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{K/k},\ H'(B) = B^G$$

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*

$$\begin{array}{ll} P\colon C_{K/k} \rightsquigarrow C_{G-conj} & P(A) := \mathrm{Hom}_{k-alg}(A,K) \\ \bar{P}\colon C_{G-conj} \rightsquigarrow C_{K/k} & \bar{P}(Z) := \mathrm{Hom}_G(Z,K) \end{array}$$

establecen una anti-equivalencia entre las categorías $C_{K/k}$ y C_{G-conj}.

Demostración. Tenemos las equivalencias

$$\begin{array}{ccccc} \mathscr{C}_{K/k} & \overset{H}{\rightsquigarrow} & \mathscr{C}_{GK-Trv} & \overset{F'}{\rightsquigarrow} & \mathscr{C}_{G-conj} \\ \mathscr{C}_{K/k} & \overset{H'}{\leftsquigarrow} & \mathscr{C}_{GK-Trv} & \overset{F}{\leftsquigarrow} & \mathscr{C}_{G-conj} \end{array}$$

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 $a_i\in K$, para $i = 1,\dots,n$ y $H_i\subseteq G$ 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 $p(x) := m.c.m.(p_1(x),\dots,p_n(x))$,

$$K' := K^G[g(a_i)]_{i\in\{1,\dots,n\},\bar{g}\in G/H_i}\subseteq K$$

es una K^G-extensión de Galois, que contiene a $K^G(a_1,\dots,a_n)$. Si $H := \{g\in G\colon g(\lambda) = \lambda \text{ para todo } \lambda\in K'\}$, entonces $K'^{G/H} = K'^G = K^G$, luego $\dim_{K^G}K' = \#G/\#H \le \#G$. Luego, $\dim_{K^G}K\le \#G$. 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 sólo 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 sólo 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. 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.

Supongamos ahora que K es normal. 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.

□

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 $k[x_1, \ldots, x_n] \to k(\alpha_1, \ldots, \alpha_n)$, $x_i \mapsto \alpha_i$ es epiyectivo, por tanto, $k(\alpha_1, \ldots, \alpha_n) = k[x_1, \ldots, x_n]/I$, donde I es el ideal (maximal) formado por todos los polinomios $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ tales que $p(\alpha_1, \ldots, \alpha_n) = 0$. Sea $G = \mathrm{Aut}_{k-alg} k(\alpha_1, \ldots, \alpha_n)$ *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 $k[x_1, \ldots, x_n]$, $\sigma(q(x_1, \ldots, x_n)) = q(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, tenemos que

$$\mathrm{Aut}_{k-alg} k(\alpha_1, \ldots, \alpha_n) = \{\sigma \in S_n : \sigma(I) = I\}$$

Es decir, el grupo asociado a $p(x)$ es el conjunto de permutaciones σ de las raíces de $p(x)$, tales que si $q(\alpha_1, \ldots, \alpha_n) = 0$ entonces $q(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$.

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 sólo si G es resoluble.

Extensiones de cuerpos cíclicas y extensiones por radicales.

1. Definición: Diremos que una extensión $k \to K$ 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 verifica que $g_1,\dots,g_n$ son K-linealmente independientes.*

Demostración. Por la fórmula de los puntos, $\mathrm{Aut}_{k-alg} K = \mathrm{Hom}_{K-alg}(K \otimes_k K, K)$. Ahora, como $K \underset{k}{\otimes} K = K \times \overset{n}{\dots} \times K$, los automorfismos de K se corresponden con las proyecciones de $K \times \overset{n}{\dots} \times K$ en cada uno de los factores, que son claramente linealmente independientes. □

A. Caso primo con la característica.

3. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos de grado n y supongamos k contiene todas las raíces n-ésimas de la unidad. Entonces, $k \to K$ es una extensión cíclica si y sólo 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 $g \in \mathrm{Aut}_{k-alg}(k(\sqrt[n]{a})) = G$, tenemos que $g(\sqrt[n]{a}) = \epsilon^i \sqrt[n]{a}$, para cierto $0 \le i < n$ 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, $\mathrm{Id}, \sigma, \dots, \sigma^{n-1}$ 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 sólo si $\sigma(R) = \epsilon R$, siendo ϵ una raíz n-ésima de la unidad.

Calculemos un vector propio de σ, R, de valor propio ϵ. Observemos que $x^n - 1 = (x - \epsilon)\cdot(1 + \epsilon^{-1}\cdot x + \dots + \epsilon^{-(n-1)}x^{n-1})$. Por tanto, $\mathrm{Im}((1 + \epsilon^{-1}\cdot\sigma + \dots + \epsilon^{-(n-1)}\sigma^{n-1}) \subseteq \mathrm{Ker}(\sigma - \epsilon)$ (de hecho son iguales). Sea $\alpha \in K$, tal que $R := (1 + \epsilon^{-1}\cdot\sigma + \dots + \epsilon^{-(n-1)}\sigma^{n-1})(\alpha) \neq 0$, entonces $\sigma(R) = \epsilon \cdot R$.

5. Definición: Supongamos que $k \hookrightarrow K$ sea una extensión de Galois cíclica de grupo $G = \langle\sigma\rangle$. Sea $n = \dim_k K$ y $\epsilon \in K$ una raíz n-ésima de la unidad y $\alpha \in K$. Llamaremos resolvente de Lagrange de α por ϵ, que denotaremos $R(\alpha,\epsilon)$, a

$$R(\alpha,\epsilon) := \sum_{i=0}^{n-1} \epsilon^i \sigma^i(\alpha)$$

Observemos que $\sigma(R(\alpha,\epsilon)) = \epsilon^{-1}\cdot R(\alpha,\epsilon)$. Por tanto, $\sigma(R(\alpha,\epsilon)^n) = R(\alpha,\epsilon)^n$, luego $R(\alpha,\epsilon)^n \in k$.

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 $\sqrt[p]{\backslash a}$, a una raíz de $x^p - x - a$. Diremos además que $\sqrt[p]{\backslash a}$ es un radical modificado *propio* si $x^p - x - a$ es irreducible.

Si $/_p\underline{\backslash a}$ es una raíz de $x^p - x - a$, las demás raíces son $/_p\underline{\backslash a} + 1, /_p\underline{\backslash a} + 2, ..., /_p\underline{\backslash a} + p - 1$. En efecto, basta ver que si α es raíz de $x^p - x - a$, entonces $\alpha + 1$ también; pero

$$(\alpha+1)^p - (\alpha+1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = 0$$

luego se concluye. Por tanto el cuerpo de descomposición del polinomio $x^p - x - a$ es $k(/_p\underline{\backslash a})$.

7. Ejercicio: Probar 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 $k \to k(/_p\underline{\backslash a})$ 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 $k(/_p\underline{\backslash a})$ que define es

$$\begin{aligned} \tau_i : k(/_p\underline{\backslash a}) &\longrightarrow k(/_p\underline{\backslash a}) \\ /_p\underline{\backslash a} &\longmapsto /_p\underline{\backslash a} + i \end{aligned}$$

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 sólo si existe $a \in k$ de modo que $K = k(/_p\underline{\backslash a})$.*

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 $K = k(/_p\underline{\backslash a})$. Entonces, K es una extensión de Galois, porque es el cuerpo de descomposición de $x^p - x - a$. Su grupo de Galois, G, es un subgrupo de $\mathbb{Z}/p\mathbb{Z}$: dado $g \in G$, $g(/_p\underline{\backslash a}) = /_p\underline{\backslash a} + i$ y tenemos un morfismo inyectivo $G \hookrightarrow \mathbb{Z}/p\mathbb{Z}$, $g \mapsto \bar{i}$. Por órdenes, $G = \mathbb{Z}/p\mathbb{Z}$.

□

9. Definición: Diremos que una extensión finita $k \to K$ es *radical* si $K \simeq k(\sqrt[n]{a})$ ó $K \simeq k(/_p\underline{\backslash a})$.

10. 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 $\mathrm{car}\, k = p$ y $k \hookrightarrow K$ es puramente inseparable, entonces es una extensión por radicales, porque $K^{p^n} = k$, para $n >> 0$.

Si $\mathrm{car}\, k = p$, $n = p^r \cdot m$, $(m,p) = 1$ 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.

11. 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 sólo 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 sólo 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 sólo 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 sólo si H_1 es normal en H_2.

Sea $\{\mathrm{Id}\} = G_1 \subset G_2 \subset \cdots \subset G_r = G$ una cadena de subgrupos de G. 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 si y sólo si $K^{G_i} \hookrightarrow K^{G_{i-1}}$ es una extensión de Galois de grupo cíclico, para todo i (corolarios de los teoremas 90 de Hilbert, aditivo y multiplicativo), que equivale a decir que G_{i-1} es normal en G_i y G_i/G_{i-1} es cíclico, para todo i. □

12. Proposición: *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. La sucesión*

$$1 \to \mathrm{Aut}_{L-alg}(L \cdot K) \to \mathrm{Aut}_{k-alg}(K) \to \mathrm{Hom}_{k-alg}(L \cap K, K) \to 1$$

es exacta.

Demostración. Denotemos $G' = \mathrm{Aut}_{L-alg}(L \cdot K)$. Observemos que $K^{G'} = (K \cdot L)^{G'} \cap K = L \cap K$. Es decir, G' se identifica con el subgrupo de $\mathrm{Aut}_{k-alg}(K)$ que dejan invariante a $K \cap L$. Se concluye por el teorema de prolongación. □

13. Teorema: *Sea $k \to K$ una extensión finita de cuerpos. Entonces, K está incluida en una extensión de k por radicales si y sólo 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 sólo 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 2.6.12, 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 sólo 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''.

□

14. 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.

15. Definición: Sea $p(x) \in k[x]$, llamaremos grupo asociado a $p(x)$ al grupo de automorfismos del cuerpo de descomposición de $p(x)$.

16. Corolario: *Un polinomio $p(x) \in k[x]$ es resoluble por radicales si y sólo si el grupo asociado al polinomio es resoluble.*

17. 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 $\alpha_1,\dots,\alpha_n$ a las raíces de este polinomio (que también son variables libres sobre k). El grupo simétrico de n letras, S_n, opera en $k(\alpha_1,\dots,\alpha_n)$ de modo natural (por automorfismos de k-álgebras), permutando las α_i. Obviamente

$$k(a_1,\dots,a_n)\subseteq k(\alpha_1,\dots,\alpha_n)^{S_n}$$

y $k(a_1,\dots,a_n)\hookrightarrow k(\alpha_1,\dots,\alpha_n)$ 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

$$k(a_1,\dots,a_n)\to k(\alpha_1,\dots,\alpha_n)$$

es una extensión de Galois de grupo S_n. Es decir, *el grupo de la ecuación general de grado n es* S_n.

18. Teorema : *La ecuación general de grado n es resoluble por radicales para* $n\le 4$ *y no es resoluble por radicales para* $n>4$.

Demostración. Se deduce de que el grupo simétrico S_n es resoluble si y sólo si $n\le 4$. □

19. 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 2.9.26, G está incluido en el metacíclico $N\subset S_p=\mathrm{Biy}(\mathbb{Z}/p\mathbb{Z})$, donde $N=\{\sigma_{i,j},\text{ con }(i,j)\in\mathbb{Z}/p\mathbb{Z}\rtimes(\mathbb{Z}/p\mathbb{Z})^*\}$, 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 sólo si $\sigma_{i,j}(x)=x$ y $\sigma_{i,j}(x')=x'$. Por tanto, la extensión generada por dos raíces cualesquiera sólo 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 p 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.

□

20. 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.*

Apéndice: Teorema 90 de Hilbert.

21. Teorema (90 de Hilbert multiplicativo): *Sea* $k\to K$ *una extensión cíclica de grado n y grupo* $G=<\sigma>$*. Entonces,*

$$N(\alpha)=1\Leftrightarrow\alpha=\frac{\beta}{\sigma(\beta)},\ \textit{para cierto }\beta\in K$$

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, $1,T,\dots,T^{n-1}$ 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. □

22. Teorema (90 de Hilbert aditivo): *Sea* $k\to K$ *una extensión cíclica de grado n y sea* σ *un generador del grupo de automorfismos. Entonces,*

$$Tr(\alpha)=0\Leftrightarrow\alpha=\sigma(\beta)-\beta,\ \textit{para cierto }\beta\in K$$

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 sólo si $q(x)$ es múltiplo de $(x-1)$. Por tanto, $\operatorname{Ker} Tr = \operatorname{Im}(\sigma - \mathrm{Id})$.

□

2.7. Resolución de ecuaciones polinómicas por radicales

Fórmula de Lagrange.

Sea $k \to K$ una extensión cíclica de grado n, primo con la característica, supongamos que k contiene a las raíces n-ésimas de la unidad y fijemos una raíz n-ésima primitiva de la unidad, ϵ. Sea σ un generador del grupo de la extensión y $\beta \in K$, tal que $\sigma(\beta) = \epsilon\cdot\beta$, luego $a := \beta^n \in k$ y $\beta = \sqrt[n]{a}$. Sabemos que $K = k(\beta)$.

Veamos ahora cómo expresar, de modo explícito, un elemento α de una extensión cíclica en función de radicales de elementos de k (obtenidos a partir de α y el grupo de Galois 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 $\frac{\sigma^n-1}{\sigma-\epsilon^i}(R_i) = n\cdot(\epsilon^i)^{n-1}\cdot R_i = n\cdot\epsilon^{-i}\cdot R_i$. 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

$$\alpha = \sum_i \lambda_i R_i = \sum_i \frac{1}{n}(\mathrm{Id} + \epsilon^{-i}\sigma + \cdots + \epsilon^{-(n-1)\cdot i}\sigma^{n-1})(\alpha) = \frac{1}{n}\sum_i(\alpha + \epsilon^{-i}\sigma(\alpha) + \cdots + \epsilon^{-i(n-1)}\sigma^{n-1}(\alpha))$$

1. 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.*

2. 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 $1 \le i \le r$. Dado $\alpha \in K$, denotemos*

$$R(\alpha,\varepsilon_1^{j_1},\ldots,\varepsilon_r^{j_r}) = \sum_{i_1<n_1,\ldots,i_r<n_r}\varepsilon_1^{i_1j_1}\cdots\varepsilon_r^{i_rj_r}(\sigma_1^{i_1}\circ\cdots\circ\sigma_r^{i_r})(\alpha)$$

$R(\alpha,\varepsilon_1^{j_1},\ldots,\varepsilon_r^{j_r})$ son radicales d-ésimos (d el mínimo común múltiplo de $n_1,\ldots,n_r$) y se verifica 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 $R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r}) \overset{*}{=} R(R(\alpha,\varepsilon_1^{j_1}),\varepsilon_2^{j_2}\dots,\varepsilon_r^{j_r})$. Procedamos por inducción sobre r. Sea $n' = n_2\cdots n_r$. Entonces,

$$\alpha = \frac{1}{n_1}\sum_{j_1<n_1} R(\alpha,\varepsilon_1^{j_1}) = \frac{1}{n_1}\sum_{j_1<n_1}\left(\frac{1}{n'}\sum_{j_2<n_2,\dots,j_r<n_r} R(R(\alpha,\varepsilon_1^{j_1}),\varepsilon_2^{j_2},\dots,\varepsilon_r^{j_r})\right) = \frac{1}{n}\sum_{j_1<n_1,\dots,j_r<n_r} R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$$

Denotemos $G_i = \langle\sigma_i\rangle$. Denotemos $R = R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$. Por la igualdad $\overset{*}{=}$, $R^{n_1} \in K^{G_1}$. 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, $R^d \in \cap_i K^{G_i} = K^{\langle G_1,\dots,G_r\rangle} = K^G = k$.

□

Sea ahora $k \to K$ una extensión cíclica de grado p = característica de k. Veamos cómo expresar un elemento de K en función de radicales modificados. Denotemos por σ un generador del grupo de automorfismos de K. Sea $\beta \in K$ tal que $\sigma(\beta) = \beta + 1$, entonces $a := \beta^p - \beta \in k$, $\beta = \sqrt[p]{\underline{a}}$ y $K = k(\beta) = k[x]/(x^p - x - a)$.

Veamos cómo encontrar un radical modificado β. Ha de cumplir que $(\sigma - \mathrm{Id})(\beta) = 1$. Ahora bien, $k = \mathrm{Ker}(\sigma - \mathrm{Id}) = \mathrm{Im}(\sigma - \mathrm{Id})^{p-1}$. Obsérvese que

$$Tr = \sigma^{p-1} + \sigma^{p-2} + \cdots + \sigma + 1 = \frac{\sigma^p - 1}{\sigma - 1} = (\sigma - 1)^{p-1}$$

Sea $\gamma \in K$ un elemento cualquiera de traza no nula. Si definimos $\beta := \frac{(\sigma-1)^{p-2}(\gamma)}{Tr(\gamma)}$, entonces $(\sigma-1)(\beta) = 1$ y β 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 $0 \le i < 2p-2$ y $i \ne p-1$; 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 $i \ne 0$ y $c_0 = -a\cdot Tr(\alpha/\bar{x})$.

3. Por tanto,

$$\boxed{\alpha = -a\cdot Tr(\alpha/\beta) - \sum_{i=1}^{p-1} Tr(\alpha\cdot\beta^{p-1-i})\cdot\beta^i}$$

4. 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: $Tr(\alpha_1) = \alpha_1+\alpha_2 = a \ne 0$. 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, $\frac{\alpha_1}{a} = \wp\underline{b/a^2}$. Por tanto,

$$\alpha_1 = a\wp\underline{b/a^2}, \quad \alpha_2 = a(1+\wp\underline{b/a^2})$$

5. Resolución de la cúbica, $x^3+a_1x^2+a_2x+a_3=0$**.**

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 $\tau=(1,2)$.

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

$$\begin{aligned}R(x_i,1)&=x_i+\sigma(x_i)+\sigma^2(x_i)=x_1+x_2+x_3=-a_1\\ R(x_i,\varepsilon)&=x_i+\sigma(x_i)\varepsilon+\sigma^2(x_i)\varepsilon^2=\sigma^{i-1}(R(x_1,\varepsilon))=\varepsilon^{2(i-1)}R(x_1,\varepsilon)\\ R(x_i,\varepsilon^2)&=x_i+\sigma(x_i)\varepsilon^2+\sigma^2(x_i)\varepsilon=\sigma^{i-1}(R(x_1,\varepsilon^2))=\varepsilon^{i-1}R(x_1,\varepsilon^2)\end{aligned}$$

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 $\tau(R_2)=\varepsilon^2R_1$ 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:

$$\begin{aligned}\frac{1}{2}(R_1^3+\tau(R_1^3))&=\frac{-2a_1^3+9a_1a_2-27a_3}{2}\\ \frac{1}{2}(R_1^3-\tau(R_1^3))&=\frac{3}{2}\sqrt{-3\Delta}\end{aligned}$$

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:

$$\boxed{\begin{aligned}x_i=\frac{1}{3}(-a_1+&\sqrt[3]{\frac{-2a_1^3+9a_1a_2-27a_3}{2}+\frac{3}{2}\sqrt{-3(a_1^2a_2^2-4a_1^3a_3+18a_1a_2a_3-4a_2^3-27a_3^2)}}+\\ &\sqrt[3]{\frac{-2a_1^3+9a_1a_2-27a_3}{2}-\frac{3}{2}\sqrt{-3(a_1^2a_2^2-4a_1^3a_3+18a_1a_2a_3-4a_2^3-27a_3^2)}}\,)\end{aligned}}$$

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:

$$\boxed{\begin{aligned}x_i=a_1+&\sqrt[3]{(a_1a_2+a_3)\cdot\left(\wp\left(\frac{(a_1^2+a_2)^3}{(a_1a_2+a_3)^2}\right)\right)}\ +\\ &\sqrt[3]{(a_1a_2+a_3)\cdot\left(\wp\left(\frac{(a_1^2+a_2)^3}{(a_1a_2+a_3)^2}\right)+1\right)}\end{aligned}}\qquad(\text{car. } k=2)$$

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, $\beta = (\sigma - \mathrm{Id})(x_1)/Tr(\alpha_1) = \frac{x_1 - x_2}{a_1}$ 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 2.7.3,

$$x_1 = -a \cdot Tr(x_1/\beta) - Tr(x_1 \cdot \beta) \cdot \beta - Tr(x_1) \cdot \beta^2$$

$Tr(x_1) = -a_1$. $Tr(x_1\beta) = x_1\beta + x_2(\beta+1) + x_3(\beta+2) = -a_1\beta + x_2 + 2x_3 = -x_1 + 2x_2 + 2x_3 = a_1$. $Tr(x_1/\beta) = a_1 \cdot Tr(\frac{x_1}{x_1-x_2}) = a_1 \cdot \frac{x_1(x_2-x_3)(x_3-x_1) + x_2(x_1-x_2)(x_3-x_1) + x_3(x_1-x_2)(x_2-x_3)}{(x_1-x_2)(x_2-x_3)(x_3-x_1)} = \frac{-a_1^2a_2}{\sqrt{\Delta}}$. Luego, $x_1 = \frac{a_2}{a_1} - a_1\beta + a_1\beta^2$ y

$$\boxed{x_1 = a_2/a_1 - a_1 \cdot \sqrt[3]{\sqrt{a_1^2a_2^2 - a_1^3a_3 - a_2^3}/a_1^3} + a_1 \cdot \left(\sqrt[3]{\sqrt{a_1^2a_2^2 - a_1^3a_3 - a_2^3}/a_1^3}\right)^2} \qquad \begin{array}{l}\text{car } k = 3\\ a_1 \neq 0\end{array}$$

Supongamos ahora que $a_1 = 0$.

Si hacemos el cambio de variable $x = \sqrt{-a_2}y$, entonces $x^3 + a_2x + a_3 = (-a_2)^{3/2} \cdot (y^3 - y + (a_3/(-a_2)^{3/2}))$, cuyas raíces son $y_i = \sqrt[3]{-a_3/(-a_2)^{3/2}} + i$ y

$$\boxed{x_i = \sqrt{-a_2} \cdot \left(\sqrt[3]{-a_3/(-a_2)^{3/2}} + i\right)}, \qquad \text{car. } k = 3, a_1 = 0$$

6. Resolución de la cuártica, $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$.

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 $s_2 = (1,3)(2,4)$.

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 sólo 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:

$$R(x_1, 1, 1) = x_1 + x_2 + x_3 + x_4 = -a_1$$
$$R(x_1, 1, -1) = x_1 + x_2 - x_3 - x_4 = \xi_1$$
$$R(x_1, -1, 1) = x_1 - x_2 + x_3 - x_4 = \xi_2$$
$$R(x_1, -1, -1) = x_1 - x_2 - x_3 + x_4 = \xi_3$$

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 $\beta_1=\wp\backslash\underline{b_1}$. Equivalentemente, $\beta_2=\frac{x_1+x_3}{a_1}$ y $\beta_2=\wp\backslash\underline{b_2}$, 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,

$$\boxed{x_1=\theta_3/a_1+a_1\cdot\wp\backslash\underline{(a_2+\theta_1)/a_1^2}\cdot\wp\backslash\underline{(a_2+\theta_2)/a_1^2}}\quad(\text{car } k=2,a_1\neq 0)$$

$\underline{a_1=0}$ (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 $\boxed{x_1=\sqrt[2]{a_2\wp\backslash\underline{a_4/a_2^2}}}$, (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 $\beta_1=\wp\backslash\underline{b_1}$. Igualmente, $\beta_2=x_1x_2x_3+x_1x_3x_4$ y $\beta_2=\wp\backslash\underline{b_2}$, 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,

$$\boxed{x_1=a_4/a_3+(a_3/\theta_2)\cdot\wp\backslash\underline{a_4/\theta_1^2}+(a_3/\theta_1)\cdot\wp\backslash\underline{a_4/\theta_2^2}}\quad(\text{car } k=2,a_1=0,a_3\neq 0)$$

2.7.1. 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 sólo si tiene raíces en k y esto sucede cuando $\sqrt{a_1^2-4a_2}\in k$.

7. 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 sólo 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 $\alpha_1,\dots,\alpha_n$ son las raíces de $p(x)$, entonces $\sqrt{\Delta}=\prod_{i<j}(\alpha_i-\alpha_j)\in k(\alpha_1,\dots,\alpha_n)$. Además, dado $\sigma\in G\subseteq S_n$, $\sigma(\sqrt{\Delta})=\operatorname{sign}(\sigma)\cdot\sqrt{\Delta}$. Entonces, $\sqrt{\Delta}\in k=k(\alpha_1,\dots,\alpha_n)^G \iff \sigma(\sqrt{\Delta})=\sqrt{\Delta}$, para todo $\sigma\in G \iff \operatorname{sign}(\sigma)=1$, 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 $k(\alpha_1,\dots,\alpha_4)^{G\cap K_4}=k(\theta_1,\theta_2,\theta_3)=K'$. 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 $G=K_4$.

2.8. 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 $K=k(\alpha_1,\dots,\alpha_n)$, donde $\alpha_i^2\in k(\alpha_1,\dots,\alpha_{i-1})$, 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 sólo si es de grado una potencia de 2.*

Demostración. Sólo 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, $K=k(\alpha_1,\dots,\alpha_n)$ es una extensión por radicales cuadráticos. □

3. Ejercicio: Sea $K=k(x_1,\dots,x_4)$ el cuerpo descomposición de la ecuación general de grado 4. Sea $H=\langle(1,2,3)\rangle\subset S_4$. Probar 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. Probar 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 sólo 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 sólo 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 sólo 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.

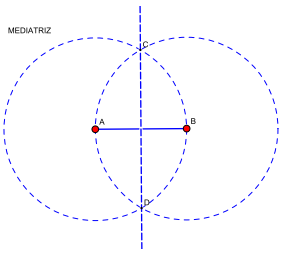
□

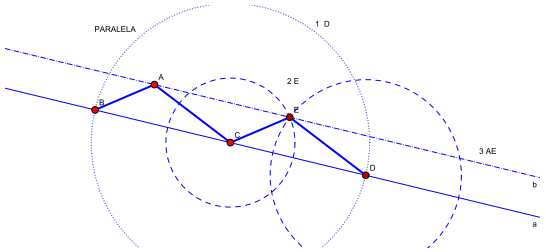
2.8.1. Construcciones con regla y compás

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.:

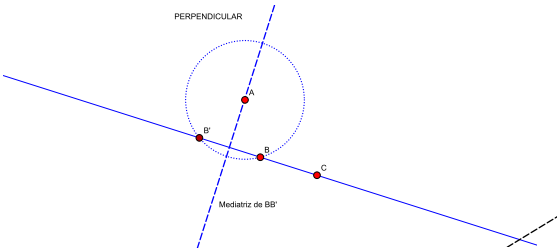
1. Diremos que los puntos de $\mathbb{P}$ son constructibles.
2. Diremos que las rectas que pasan por un par de puntos constructibles son constructibles.
3. Diremos que las circunferencias de centro un punto constructible y radio la distancia entre dos puntos constructibles son constructibles.
4. Diremos 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 $\mathbb{P}$).

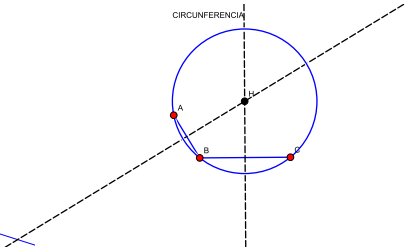
Es bien conocido que las siguiente construcciones pueden realizarse con regla y compás:
- Trazar la perpendicular por su punto medio a un segmento dado.
- Dados tres puntos no alineados A, B, C, trazar la paralela a la recta BC que pasa por A.



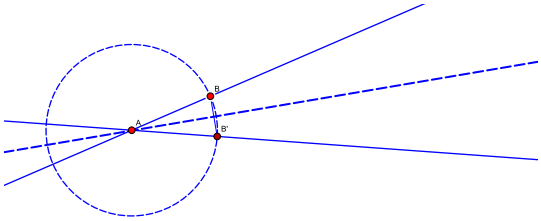


- Dados tres puntos no alineados A,B,C, trazar la perpendicular a la recta BC que pasa por A.
- Trazar la circunferencia que pasa por tres puntos no alineados A, B y C





- 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.

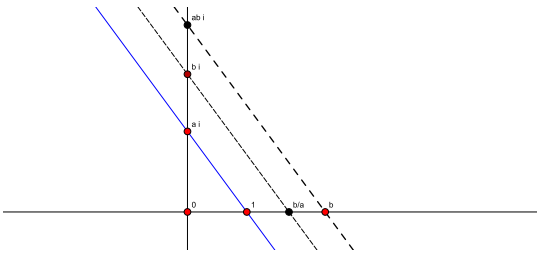
9. Lema: *La condición necesaria y suficiente para que un número complejo $a+bi$ sea constructible es que lo sean su parte real a y su parte imaginaria b.*

Demostración. Es consecuencia directa de la posibilidad de trazar paralelas y perpendiculares con regla y compás. □

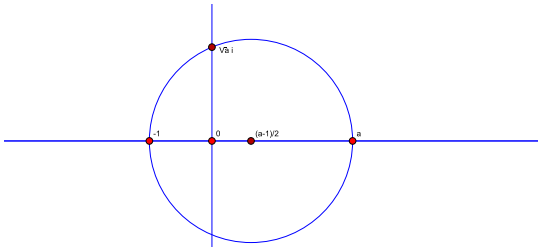
10. Lema: *Los números complejos constructibles $\mathscr{C}(\mathbb{P})$, forman un subcuerpo de $\mathbb{C}$, estable por toma de raíces cuadradas.*

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 sólo 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 sólo si $e^{2\pi i/n}$ es constructible con regla y compás. Por los teoremas 2.8.8, 2.8.11, el polígono de n lados es constructible con regla y compás si y sólo 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,

$$\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/n}) = |(\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/2^m\mathbb{Z})^*| \cdot |(\mathbb{Z}/p_1^{n_1}\mathbb{Z})^*| \cdots |(\mathbb{Z}/p_r^{n_r}\mathbb{Z})^*| = 2^{m-1} \cdot p_1^{n_1-1}(p_1-1) \cdots p_r^{n_r-1}(p_r-1),$$

que es una potencia de dos si y sólo si n es producto de una potencia de 2 y de números primos de Fermat distintos. □

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 sólo 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 sólo 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 $\dim_{\mathbb{Q}(e^{\pi/3 \cdot i})} \mathbb{Q}(e^{\pi/9 \cdot i}) = 3$.

2.9. 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 sólo 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 sólo 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 $long(N), long(G/N) < long(G)$.

Demostración. (1) Si $h_2 \in H_2$, es $h_2 H_1 h_2^{-1} = H_1$ 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 $\pi(H_2)$.

Sea 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 es $H_2/H_1 \approx \pi(H_2)/\pi(H_1)$.

(2) Cada serie normal en H, digamos $1 \subset H_1 \subset \cdots \subset H_r = N$, y en G/N, $1 \subset \overline{N}_1 \subset \cdots \subset \overline{N}_s = G/N$, ambas de términos distintos, da una serie normal en G:

$$1 \subset H_1 \subset \cdots \subset H_r \subset N_1 \subset \cdots \subset N_s = G$$

(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 permutaciones de éstos).*

Demostración. Por inducción sobre $long(G)$. Se observa que $long(G) = 1$ si y sólo 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 cadena de composición $1 \subset M_1 \subset \cdots \subset M_l = M$. Se verifica que M es normal en G por ser intersección de dos subgrupos normales. Se tienen las cadenas:

$$1 \subset H_1 \subset \cdots \subset H_{r-1} \subset G$$
$$1 \subset M_1 \subset \cdots \subset M_{l-1} \subset M \subset H_{r-1} \subset G$$
$$1 \subset M_1 \subset \cdots \subset M_{l-1} \subset M \subset N_{s-1} \subset G$$
$$1 \subset N_1 \subset \cdots \subset N_{s-1} \subset G$$

Si probamos que estas cadenas 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. Intercambiando H por N se demuestra igualmente 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. Si 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 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 $n \geq 4$.

Por ser $H \subset S_n$ normal y 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 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 $\overline{\sigma}_1 = (a_{n_1}, \ldots, a_3, a_1, a_2)$. 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 2.9.18, 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 $\overline{\sigma} = (a_1, a_3) \circ (a_2, a_1) \circ \sigma_3^{-1} \circ \cdots \circ \sigma_h^{-1}$, 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: Hallar 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. Se trata de encontrar 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 $\sigma = (1, \ldots, n) \in S_n$ 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 $N_n = \mathbb{Z}/n\mathbb{Z}$ se verifica 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 $N_n = \mathbb{Z}/n\mathbb{Z}$. Si $\sigma' \in S_n$ conmuta con σ, entonces $(\bar{1}, \ldots, \bar{n}) = \sigma'\sigma\sigma'^{-1} = (\sigma'(\bar{1}), \ldots, \sigma'(\bar{n}))$. 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 sólo 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 teorema 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 N_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, $<\sigma> \subseteq G \subseteq N_{S_p}(<\sigma>)$.

□

2.10. Problemas

1. Sea A una k-álgebra finita reducida. Probar que todo ideal es idempotente.
2. Sea k-algebraicamente cerrado y A una k-álgebra finita. Probar que
$$(A \otimes_k A)_{\text{red}} = A_{\text{red}} \otimes_k A_{\text{red}}$$
3. Sea $k \to K$ una extensión finita. Probar que $K \otimes_k K$ es cuerpo si y sólo si $K = k$.
4. Sea A una k-álgebra finita e I un ideal. Probar:
   a) Si A es local, A/I es plano $\Leftrightarrow I = 0$.
   b) Si A es cualquiera, A/I es plano $\Leftrightarrow I = I^2$.
5. Probar que la localización de una k-álgebra finita es una k-álgebra finita.
6. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcular $\text{Hom}_{k-\text{alg.}}(A, K)$.
7. Sea $k \to K$ una extensión trivializante de la k-álgebra finita A. Probar que el polinomio característico de todo elemento de A (considerando como endomorfismo la multiplicación) 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 $A_\lambda = A/(x - \lambda)$. Calcular
$$\text{Spec} A_\lambda,\ \text{Hom}_{\mathbb{R}-\text{alg.}}(A_\lambda, \mathbb{R}),\ \text{Hom}_{\mathbb{R}-\text{alg.}}(A_\lambda, \mathbb{C}).$$
9. Sea ω una raíz primitiva cúbica de la unidad. Hallar los siguientes grupos:
$$\text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\omega), \quad \text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[4]{2}), \quad \text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(i, \sqrt[2]{2}), \quad \text{Aut}_{\mathbb{Q}(\omega)}\, \mathbb{Q}(\omega, \sqrt[3]{2})$$
10. Sea $A = k[x]/(p(x))$. Probar que A es puramente inseparable si y sólo si $\text{car}\, k = p > 0$ 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 de cuerpos de k y B una K-álgebra finita. Probar:
   a) $[A_K : K]_s = [A : k]_s$.
   b) $[A : k]_s$ = orden de $\text{Hom}_{k-alg}(A, \overline{k})$, 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 K de k se dice simple cuando $K = k(\alpha)$. Probar: K es simple $\Leftrightarrow$ 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. Probar:
   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. Probar 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. Probar:
   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, probar que $k(u,v) = k(u \cdot v) = k(u+v)$.

17. Sea A una k-álgebra finita, siendo k de característica cero. Probar: $A = \pi_0^k(A) \oplus \mathrm{Rad}$ (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. Probar que $\pi_0^k(K)$ se trivializa a sí mismo.

19. Sea $k \to K$ una extensión finita. Probar: k es perfecto $\Leftrightarrow$ K es perfecto.

20. Determinar 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. Determinar el grupo de Galois de $x^4 + ax^3 + bx^2 + ax + 1$ sobre $\mathbb{Q}(a,b)$.

22. (Lagrange) 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 $K^G = k(c)$.

    Demostrar que, si c pertenece a G, d pertenece a H y $G \subset H$, entonces existe una función racional $R(x)$ tal que $d = R(c)$. Determínese $R(x)$ en función de d y de c.

23. Sea $p(x)$ un polinomio de grado n, separable sobre k. Probar que su cuerpo de descomposición es una extensión de k de grado menor o igual a $n!$.

24. 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, probar que toda extensión finita de K es cíclica.

25. Si el grupo de Galois de K sobre k es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, y car $k \neq 2$, entonces $K = k(\alpha, \beta)$, con $\alpha^2, \beta^2 \in k$. Probar también el recíproco.

26. (Teorema de los irracionales de Lagrange) Si $k \to K$ es una extensión de Galois y $k \to F$ una extensión cualquiera, entonces todo compuesto de K y F es de Galois sobre F y su grupo es el grupo de Galois de K sobre $K \cap F$.

27. Se dice que dos extensiones K y F de k son linealmente disjuntas sobre k cuando $K \otimes_k F$ es cuerpo. Probar 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.

28. Sea $k \to K$ una extensión de Galois y $k \to L$ una extensión. Probar 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 primos de $f(x)$ en $K[x]$, probar que existe un automorfismo σ de K sobre k tal que $\sigma(g) = h$.

29. Probar que todo compuesto de dos extensiones de Galois es una extensión de Galois.

30. Probar que todo grupo finito es el grupo de Galois de alguna extensión.

31. 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 $f(x)$ es un polinomio unitario y separable de $A[x]$, 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 $f(x)$.

32. Sea k un cuerpo finito con q elementos. Si $f(x) \in k[x]$ es irreducible, demostrar que $f(x)$ divide a $x^{q^n} - x$ si y sólo si el grado de $f(x)$ divide a n.

33. Sean p, q primos diferentes. Probar que $\frac{x^p - 1}{x - 1}$ es irreducible sobre $\mathbb{F}_q \Leftrightarrow q^d - 1$ no es divisible por p, para $d < p - 1$.

34. Probar que en un cuerpo finito todo elemento es suma de cuadrados.

35. Sea $p(x)$ un polinomio irreducible y separable de grado 3 sobre k. Probar que su grupo de Galois es A_3 si y sólo si su discriminante es un cuadrado en k (car $k \neq 2$).

36. 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. Probar:

    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 $G = D_4$.

37. 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. Probar:

    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 $G = D_4$.

38. Si n, m son primos entre sí, probar:

$$\mathbb{Q}(\epsilon_n) \cap \mathbb{Q}(\epsilon_m) = \mathbb{Q}, \quad \mathbb{Q}(\epsilon_n, \epsilon_m) = \mathbb{Q}(\epsilon_n \cdot \epsilon_m) = \mathbb{Q}(\epsilon_{n \cdot m})$$

39. 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 $\phi_i(\alpha) \neq \phi_j(\alpha)$, $i \neq j$. Probar: 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.

40. 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.

41. Si el polinomio $x^5 + px + q$ es irreducible sobre k, probar que entonces es resoluble por radicales si y sólo 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 discriminate de la quíntica.

42. (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:

$$G \simeq \mathrm{Hom}(A/k^{*n}, \mu_n)$$

    Probar 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.

43. Si k contiene las raíces n-ésimas de la unidad y n es primo con car k, probar:

$$k(\sqrt[n]{a}) = k(\sqrt[n]{b}) \Leftrightarrow a = \lambda^n \cdot b^m, \quad (n, m) = 1$$

44. 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, probar que el grupo de automorfismos de K es $G = \varprojlim G_i$. Determinar el grupo de automorfismos del cierre algebraico de un cuerpo finito.

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 $\mathbb{C}[x_1,\dots,x_n]$ está generado por un número finito de elementos? ¿Están los ideales de $\mathbb{C}[x_1,\dots,x_n]$ 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 $I\subseteq\mathbb{C}[x_1,\dots,x_n]$ si consideramos el ideal $r(I):=\{q\in\mathbb{C}[x_1,\dots,x_n],\text{ tales que } q^m\in I,\text{ para algún } m\}$, 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 sólo 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 sólo 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 sólo el conjunto de soluciones del sistema de ecuaciones (o equivalentemente, consideramos sólo $r(I)$) 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 irreducibles. 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 sólo 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 $\mathfrak{m}_\alpha = (t_1, \ldots, t_n)$,

$$A/\mathfrak{m}_\alpha^r = \mathbb{C}[t_1, \ldots, t_n]/(t_1, \ldots, t_n)^r = \left[\begin{array}{l}\text{Polinomios de grado} \\ < r \text{ en } t_1, \ldots, t_n\end{array}\right]$$

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 $\bar{f} \in A/\mathfrak{m}_\alpha^r$, en el punto definido por α, satisface las relaciones impuestas por cierto ideal $\bar{\mathfrak{q}}$ 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

$$\sum_{|\beta|<r} \lambda_{i,\beta}\omega_\beta(\bar{f}) = 0,\ \ 1 \leq i \leq s$$

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

$$\begin{array}{l}\displaystyle\sum_{0<|\beta|<r} \lambda_{i,\beta} \frac{\partial^{|\beta|} f}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_n} x_n}(\alpha_1, \ldots, \alpha_n) = 0,\ \ 1 \leq i \leq s \\ f(\alpha_1, \ldots, \alpha_n) = 0\end{array}$$

(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 $(\alpha_1, \dots, \alpha_n)$.

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. 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. □

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".

7. Ejemplo: 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, la ecuación del plano tangente al cono a lo largo de la generatriz está en $A \cap {\mathfrak{p}_{gt}}^2 A_{gt}$ pero no está en ${\mathfrak{p}_{gt}}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal ${\mathfrak{p}_{gt}}^2$ no es primario.

8. 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.

9. 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 noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún n. Por 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. □

10. 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 propios: $I = I_1 \cap J_1$. 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. □

11. 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 $i \neq j$).

12. 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.*

13. 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 $I = \bigcap_i \mathfrak{q}_i$ 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 3.2.6, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_x) = A \cap (IA_x)$. □

14. 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 $(I)_0$, mientras que las componentes sumergidas están asociadas a puntos más pequeños de $(I)_0$.

15. 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

$$(I : a) = \{b \in A : a \cdot b \in I\}$$

16. 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. □

17. 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 sólo 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 $(I : ab) = (\mathfrak{q}_1 : ab) = \mathfrak{p}$. □

18. 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.

19. 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 $\pi : A \to A/I$ 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 $\phi : M \to M/M_1$ 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.

20. 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).

21. Definición: Un submódulo $M' \subseteq M$ diremos que es irreducible si no es intersección de dos submódulos estrictamente mayores de M.

22. Proposición: *Los submódulos irreducibles de un módulo noetheriano son primarios.*

23. Teorema: *Todo submódulo de un módulo noetheriano es intersección de un número finito de submódulos primarios.*

24. 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'.

25. 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 $(M' : m) = \{a \in A : am \in M'\}$.

26. 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*

$$(M' : m) = \begin{cases} A & \text{si } a \in M'. \\ \mathfrak{q}' & \text{si } a \notin M', \text{ siendo } \mathfrak{q}' \text{ un ideal } \mathfrak{p}\text{-primario, que contiene a } \mathfrak{q}. \end{cases}$$

27. Proposición: *Sea M' un submódulo de un módulo noetheriano M y $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida de M'. Un ideal primo $\mathfrak{p}$ es un ideal primo asociado a la descomposición primaria de M' si y sólo si existe $m \in M$ tal que $(M' : m) = \mathfrak{p}$.*

28. 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 $\mathfrak{p}_x$ un ideal primo minimal entre los ideales primos asociados a la descomposición primaria de M'. Entonces*

$$M_i = M \cap M'_x$$

29. Ejercicio: Probar 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

30. Proposición: *Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida y $\mathfrak{p}_x$ un ideal primo. Denotemos por J la intersección de los $\mathfrak{q}_i$ contenidos en $\mathfrak{p}_x$. 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 3.2.6 □

31. 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 verifica*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j \cap \mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$$

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 de I, entonces

$$I = \mathfrak{q}''_1 \cap \cdots \cap \mathfrak{q}''_n$$

Demostración. Reordenado, podemos suponer que $\mathfrak{q}_i \subseteq \mathfrak{p}_{x_j} \Leftrightarrow i \leq j$. 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,

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1} \cap \mathfrak{q}'_j = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

Cortando con $\mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$ concluimos. □

32. Proposición: *Sea A un anillo noetheriano. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m \subset A$ una descomposición primaria reducida de radicales $\mathfrak{p}_{x_i}$. Sea $n_i \in \mathbb{N}$ tal que $\mathfrak{p}_{x_i}^{n_i} \subseteq \mathfrak{q}_i$ y denotemos $\alpha_i^{n_i}$ el ideal $\mathfrak{p}_{x_i}$-primario antimagen de $(I_{x_i} + \mathfrak{p}_{x_i}^{n_i}) \cdot A_{x_i}$ por el morfismo de localización $A \to A_{x_i}$. Entonces*

$$I = \mathfrak{q}_1 \cap \cdots \cap \alpha_i^{n_i} \cap \cdots \cap \mathfrak{q}_m$$

Demostración. Denotemos por J la intersección de los $\mathfrak{q}_j$ distintos de $\mathfrak{q}_i$. Como $I \subseteq \alpha_i^{n_i} \subseteq \mathfrak{q}_i$,

$$I = I \cap J \subseteq \alpha_i^{n_i} \cap J \subseteq \mathfrak{q}_i \cap J = I$$

luego las inclusiones son igualdades y concluimos.

□

El ideal $\alpha_i^{n_i}$ es el ideal de funciones de A cuyo desarrollo de Taylor de orden $n_i - 1$ en x_i coincide con el desarrollo de Taylor de orden $n_i - 1$ en x_i de alguna función de I.

Procedamos a ver que entre las descomposiciones primarias de I hay una canónica. Siguiendo las notaciones anteriores, para cada i, sea n_i el mínimo tal que $\alpha_i^{n_i}$ aparezca en alguna descomposición primaria de I. Entonces

$$I = \alpha_1^{n_1} \cap \cdots \cap \alpha_m^{n_m}$$

Demos un método de cálculo. Procedemos recurrentemente. Dado $\mathfrak{p}_{x_j}$, supongamos que ya tenemos calculados los $\alpha_i^{n_i}$, para todo $\mathfrak{p}_{x_i}$ contenido en $\mathfrak{p}_{x_j}$. Reordenando, supongamos que son $\alpha_1^{n_1}, \ldots, \alpha_{j-1}^{n_{j-1}}$ y escribamos $\alpha = \alpha_1^{n_1} \cap \cdots \cap \alpha_{j-1}^{n_{j-1}} \supseteq I$. Entonces n_j es el mínimo número natural tal que en A_{x_j}, $\alpha \cap (I + \mathfrak{p}_{x_j}^{n_j}) \subseteq I$, que equivale a que $\alpha \cap \mathfrak{p}_{x_j}^{n_j} \subseteq I$, que equivale a $\alpha \cap \mathfrak{p}_{x_j}^{n_j} \subseteq I \cap \mathfrak{p}_{x_j}^{n_j}$, es decir, $\alpha \cap \mathfrak{p}_{x_j}^{n_j} = I \cap \mathfrak{p}_{x_j}^{n_j}$. Supongamos que el lector conoce la teoría de la compleción y graduados. Si consideramos en los ideales $I_{x_j} \subseteq \alpha_{x_j}$ la filtración inducida por la filtración $\mathfrak{p}_{x_j}$-ádica de A_{x_j} y consideramos los graduados $GI_{x_j} := \oplus_i (I_{x_j} \cap \mathfrak{p}_{x_j}^i)/(I_{x_j} \cap \mathfrak{p}_{x_j}^{i+1}) \hookrightarrow G\alpha = \oplus_i (\alpha_{x_j} \cap \mathfrak{p}_{x_j}^i)/(\alpha_{x_j} \cap \mathfrak{p}_{x_j}^{i+1})$, entonces n_j es él mínimo número natural tal que $[GI_{x_j}]_n = [G\alpha_{x_j}]_n$, para todo $n \geq n_j$. Así sucesivamente vamos determinando los n_j y obteniendo la descomposición primaria canónica

$$I = \alpha_1^{n_1} \cap \cdots \cap \alpha_m^{n_m}$$

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.

33. 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.

34. 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

$$M' = L_1 \cap \cdots \cap L_n$$

35. 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 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 $A \xrightarrow{\text{finito}} B \xrightarrow{\text{finito}} C$. 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; si $p_c(x)$ es 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 $A[b] = \{p(b) \in B$, 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 0.3.59) se concluye.

□

7. Observación: Para la demostración de $\Rightarrow$) sólo 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 $\mathrm{Spec}k[x,y]/(y^2 - x^2 + x^3) \to \mathrm{Spec}k[x]$ definido por $(\alpha, \beta) \mapsto \alpha$ es un morfismo finito.

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 $p(c) = 0$. Sea $B' := A[b_i]_i$. 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: Demostrar que $\mathbb{Z}$ es un anillo íntegramente cerrado en $\mathbb{Q}$.

14. Proposición: *Si $f\colon A \hookrightarrow B$ es un morfismo entero e inyectivo, entonces el morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ 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.

□

15. 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.

16. Ejercicio: Probar que el supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$ es igual a $\dim \operatorname{Spec} A$.

17. Ejercicio: Demostrar que la dimensión de Krull de $\mathbb{Z}$ y $k[x]$ es uno y la de $\mathbb{C}[x, y]$ dos.

18. Teorema: *Sea $f\colon A \to B$ es un morfismo entero. El morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ 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 3.3.14 $f^*{}_{|C}$ 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 0.3.60,

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. □

19. Ejercicio: Probar que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

3.4. Teoremas de ascenso y descenso de ideales

1. 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 $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$.

2. Teorema del ascenso: *Si $f: A \to B$ es un morfismo entero entonces cumple el teorema del ascenso de ideales.*

Demostración. El morfismo $A/\mathfrak{p}_y \to B/\mathfrak{p}_x$ es entero e inyectivo, luego epiyectivo entre espectros (3.3.14); es decir, $f^*: (\mathfrak{p}_x)_0 \to (\mathfrak{p}_y)_0$ es epiyectivo y existe $x' \in (\mathfrak{p}_x)_0$ tal que $f^*(x') = y'$. □

3. Corolario: *Si $f: A \hookrightarrow B$ es un morfismo entero inyectivo, entonces* $\dim A = \dim B$. *Geométricamente, si $\pi: \operatorname{Spec} B \to \operatorname{Spec} A$ es un morfismo entero y $C \subseteq \operatorname{Spec} B$ 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 3.3.18. 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 3.3.14). 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 sólo si existe $g \in G$ tal que $x' = g(x')\}$, con la topología final del morfismo de paso a cociente, $\pi: X \to X/G$, $\pi(x) = [x]$, es decir, $U \subset X/G$ es un abierto si y sólo 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 $\pi(x') = \pi(x'') = y'$.

4. Proposición: *Sea G un grupo finito de automorfismos de un anillo B. Se verifica que*

$$\operatorname{Spec}(B^G) = (\operatorname{Spec} B)/G$$

donde $B^G = \{b \in B : g(b) = b$, para todo $g \in G\}$.

En consecuencia, el morfismo natural $\pi: \operatorname{Spec} B \to \operatorname{Spec} B^G$ 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.

□

5. 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 Σ'^G. Es fácil ver que $\bar{A} = A'^G$. Por la proposición 3.4.4, 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 todo $b \in \bar{A}$, existe $n \in \mathbb{N}$ tal que $b^{p^n} \in A$ (pues b^{p^n} es entero sobre A). Entonces $\operatorname{Spec}\bar{A} \to \operatorname{Spec}A$ es biyectiva, pues la aplicación $\operatorname{Spec}A \to \operatorname{Spec}\bar{A}$, $\mathfrak{p} \mapsto \mathfrak{p}' = \{b \in \bar{A} : b^{p^n} \in \mathfrak{p} \text{ para algún } n\}$, es su inversa. □

6. 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 $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$. □

7. 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.

8. 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*

$$\dim B_x = \dim A_y$$

3.5. Lema de Normalización de Noether. Teorema de los ceros de Hilbert

1. Definición: 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 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.

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, $V = (p_1,\ldots,p_r)_0$.

2. 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,

$$p(x_1' + \lambda_1 x_n, \ldots, x_{n-1}' + \lambda_{n-1} x_n, x_n) = p_s(\lambda_1,\ldots,\lambda_{n-1},1)x_n^s + \text{polinomio en } x_1',\ldots,x_{n-1}',x_n \text{ de grado en } x_n \text{ menor que } s$$

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

$$k[x_1,\ldots,x_r] \overset{\text{finito}}{\underset{\text{Hip.ind.}}{\hookrightarrow}} k[\xi_1',\ldots,\xi_{n-1}'] \overset{\text{finito}}{\hookrightarrow} k[\xi_1',\ldots,\xi_{n-1}',\xi_n] = k[\xi_1,\ldots,\xi_{n-1},\xi_n]$$

es un morfismo finito. □

[1] Esta hipótesis no es necesaria, sólo la imponemos porque la demostración del lema es algo más sencilla.

3. 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

$$k[x_1,\dots,x_r] \hookrightarrow A/\mathfrak{m}$$

Por tanto, $k[x_1,\dots,x_r]$ ha de tener dimensión de Krull cero, luego $r = 0$ y concluimos. □

4. 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 k-variedad 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 por el teorema de los ceros de Hilbert con el conjunto de las soluciones con valores en $\bar{k}$ del sistema $p_1 = \cdots = p_r = 0$. Sólo nos falta probar que dos soluciones α, β cumplen que $\pi(\alpha) = \pi(\beta)$ si y sólo 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 $\tau(\alpha) = \beta$.

□

5. Ejercicio : Sean $X = \operatorname{Spec} A$ y $Y = \operatorname{Spec} B$ dos k-variedades algebraicas. Sea $X \times_k Y := \operatorname{Spec}(A \otimes_k B)$. Probar que si k es algebraicamente cerrado, entonces los puntos cerrados de $X \times_k Y$ es igual al producto cartesiano del conjunto de puntos cerrado de X y el conjunto de los puntos cerrados de Y.

6. 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. □

7. Corolario : *Sea $U \subset X$ un abierto de una variedad algebraica afín. Un punto $x \in U$ es cerrado en U si y sólo 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 $U_a \hookrightarrow X$. □

8. Definición : Diremos que $X = \operatorname{Spec} A$ es íntegra si A es un anillo íntegro. Diremos que $X = \operatorname{Spec} A$ es reducida si A es un anillo reducido.

9. Forma fuerte de los ceros de Hilbert : *Sea $X = \operatorname{Spec} A$ una variedad algebraica. Si $f \in A$ se anula en todo punto cerrado de X, entonces es nilpotente. En particular, si $X = \operatorname{Spec} A$ es una variedad algebraica reducida sobre un cuerpo algebraicamente cerrado, entonces una función es nula si y sólo 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. □

10. Corolario : *Dos subconjuntos cerrados de una variedad algebraica afín son iguales si y sólo si contienen los mismos puntos cerrados.*

Demostración. Una función se anula sobre todos los puntos de un cerrado de una variedad algebraica si y sólo 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. □

3.6. Teoría de la dimensión en variedades algebraicas

1. 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. Vamos a demostrarlo por inducción sobre el grado de trascendencia. Si el grado de trascendencia del cuerpo de fracciones es cero, entonces es una extensión finita de k, luego A es una k-álgebra finita íntegra. Por tanto, A es un cuerpo y su dimensión de Krull es cero.

Supongamos $n >> 0$. Por el lema de Noether, existe un morfismo finito $k[x_1,\dots,x_n] \hookrightarrow A$, que induce un morfismo finito entre sus cuerpos de fracciones (pruébese)

$$k(x_1,\dots,x_n) \hookrightarrow \Sigma$$

luego $\operatorname{gr\,tr}\Sigma = \operatorname{gr\,tr} k(x_1,\dots,x_n) = n$. Por otra parte, $\dim k[x_1,\dots,x_n] = \dim A$, por 3.4.3. Por tanto, podemos suponer que $A = k[x_1,\dots,x_n]$ y tenemos que ver que su dimensión de Krull es n. Sea

$$0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$$

una cadena irrefinable 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, luego $(p) = \mathfrak{p}_1$. El anillo $k[x_1,\dots,x_n]/(p)$ es íntegro y su cuerpo de fracciones es de grado de trascendencia $n-1$. Por inducción sobre el grado de trascendencia, 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

$$\bar{0} \subset \bar{\mathfrak{p}}_2 \subset \cdots \subset \bar{\mathfrak{p}}_m$$

luego $m-1 \leq n-1$ y $\dim A \leq n$. 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 $\dim A \geq n$. En conclusión A tiene dimensión de Krull n. □

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. 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.

2. Ejercicio : Sean $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $X \times_k Y := \operatorname{Spec}(A \otimes_k B)$ variedades algebraicas. Demostrar que

$$\dim(X \times_k Y) = \dim X + \dim Y$$

3. Ejercicio : Sea $f : X \to Y$ un morfismo entre variedades algebraicas y $C \subset X$ un cerrado. Demostrar que

$$\dim C \geq \dim \overline{f(C)}$$

4. 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 3.6.1, $\dim X = \dim U_a$ 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 $(f)_0$ sólo tiene una única componente irreducible.

Consideremos, por el lema de normalización de Noether, un morfismo finito $k[x_1,\dots,x_n]\hookrightarrow A$. 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,

$$\begin{aligned}\dim(f)_0 &= \dim A/(f) = \dim k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}),x_{n+1})\\ &= \dim k[x_1,\dots,x_n]/(p(x_1,\dots,x_n,0)) = n-1\end{aligned}$$

□

5. Definición: Una cadena de cerrados irreducibles diremos que es maximal si no está incluida en ninguna otra mayor.

6. 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 inducción sobre la dimensión $m-1 = \dim X_1 = \dim X - 1$, y por tanto $m = \dim X$. □

7. 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.

8. Corolario: *Las variedades algebraicas son catenarias.*

Demostración. Sean $Y\supset Y'$ cerrados irreducibles de una variedad algebraica X. Toda cadena maximal de extremos Y e Y' induce, adjuntando una cadena maximal de Y', una cadena maximal de Y, luego tiene longitud $\dim Y - \dim Y'$, por el corolario anterior. □

9. 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 $\dim X$.

□

10. 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 $f_1, \dots f_r$ de X tales que una de las componentes irreducibles de $(f_1, \dots, f_r)_0$ 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 $(f_1, \dots, f_r)_0$ tienen dimensión mayor o igual que $n - r$. Por tanto, tenemos que probar sólo 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 $f_1, \dots, f_r$ requeridas.

□

11. Corolario : *Sea X una variedad algebraica irreducible de dimensión n y $x \in X$ un punto cerrado. El número mínimo de funciones $f_1, \dots, f_r$ tales que $(f_1, \dots, f_r)_0 \cap U = \{x\}$, en algún entorno abierto U de x, es n.*

12. Ejercicio : Sean Y, Y' subvariedades irreducibles de $\mathbb{A}^n$. Llamemos codimensión de Y en $\mathbb{A}^n$, que denotaremos $\operatorname{codim} Y$, a $n - \dim Y$. Supongamos que $Y \cap Y' \neq 0$. Demuéstrese que

$$\operatorname{codim} Y + \operatorname{codim} Y' \geq \operatorname{codim}(Y \cap Y')$$

13. Ejercicio : Sea $f : X \to Y$ un morfismo entre variedades algebraicas irreducibles. Sea $y \in f(X)$ un punto cerrado. Demuéstrese que

$$\dim f^{-1}(y) \geq \dim X - \dim \overline{f(X)}$$

3.7. 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.

3.7.1. 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 diferenciable f, en un punto $\alpha \in \mathbb{R}$, se define como $d_\alpha f = f - f(\alpha) \bmod (x - \alpha)^2$. 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 $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, al que pertenecen las diferenciales de funciones en α, 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 y $k[x] \otimes_k k[x]$ el anillo de funciones algebraicas de $\mathbb{A}_1 \times_k \mathbb{A}_1 = \mathbb{A}_2$. Los morfismos $k[x] \to k[x, \bar{x}] = k[x] \otimes_k k[x]$, $p(x) \mapsto p(x)$, $p(x) \mapsto p(\bar{x})$ son obviamente los morfismos $p(x) \mapsto p(x) \otimes 1$ 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 $\operatorname{Spec} A \times_k \operatorname{Spec} A := \operatorname{Spec}(A \otimes_k A)$, 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 $\operatorname{Spec} A$, las funciones de $\operatorname{Spec} A \times_k \operatorname{Spec} A$ $f(x)$ y $f(\bar{x})$. Diremos que el morfismo $\operatorname{Spec} A \hookrightarrow \operatorname{Spec} A \times \operatorname{Spec} A$, 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 $\operatorname{Spec} A$ en $\operatorname{Spec} A \times \operatorname{Spec} A$.

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 verifica 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 $d: A \to \Omega_{A/k}$ 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

$$d_\alpha: A \to \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

que se denomina diferencial en α, y que vale $d_\alpha(A) = \overline{f - f(\alpha)}$, 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 $Der_k(A, M)$. Si definimos

$$(D + D')(a) := D(a) + D'(a) \qquad (aD)(b) := aDb$$

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 inmediato que $\delta(ab) = (a\otimes 1)\cdot\delta b + (\delta a)\cdot(1\otimes b)$. Haciendo módulo Δ^2 se concluye que $d(ab) = adb + bda$. □

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 verifica que*

$$Der_k(A,M) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, M)$$

En particular,

$$Der_k(A,k) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k) \underset{Not}{=} (\mathfrak{m}/\mathfrak{m}^2)^*$$

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: *Existe un isomorfismo canónico*

$$\mathrm{Hom}_A(\Omega_{A/k}, M) = Der_k(A,M),\ w \mapsto w\circ d.$$

Demostración. Por la proposición anterior, para todo A-módulo M se cumple que

$$Der_A(A\otimes_k A, M) = \mathrm{Hom}_A(\Delta/\Delta^2, M).$$

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

$$Der_k(A,M) \simeq Der_{k'}(A\otimes_k k', M)$$

Dada una k-derivación $D : A \to M$, define una 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 $Der_k(A,M) = Der_k(A_S,M)$. Basta ver para ello, que toda derivación $D \in Der_k(A,M)$ 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

$$\begin{aligned}\mathrm{Hom}_{A_S}(\Omega_{A_S/k}, M) = Der_k(A_S,M) = Der_k(A,M) = \mathrm{Hom}_A(\Omega_{A/k}, M)\\ = \mathrm{Hom}_{A_S}((\Omega_{A/k})_S, M)\end{aligned}$$

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:*

$$\begin{array}{ccccccc} 0 & \to & Der_A(B,N) & \to & Der_k(B,N) & \to & Der_k(A,N) \\ & & D & \mapsto & D & & \\ & & & & D & \mapsto & D_{|A} \end{array}$$

Demostración. Es evidente. □

Si B es una A-álgebra, el morfismo $A \to \Omega_{B/k}, a \mapsto da$ induce por 3.7.12, 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 3.7.12, 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

$$0 \to \underset{\| Der_A(B,N)}{\mathrm{Hom}_B(\Omega_{B/A},N)} \to \underset{\| Der_k(B,N)}{\mathrm{Hom}_B(\Omega_{B/k},N)} \to \underset{\| \mathrm{Hom}_A(\Omega_{A/k},N) \| Der_k(A,N)}{\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B,N)}$$

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*

$$0 \to Der_k(A/I,N) \to Der_k(A,N) \to \mathrm{Hom}_A(I,N)$$

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

$$0 \to \underset{\| Der_k(A/I,N)}{\mathrm{Hom}_{A/I}(\Omega_{(A/I)/k},N)} \to \underset{\| \mathrm{Hom}_A(\Omega_{A/k},N) \| Der_k(A,N)}{\mathrm{Hom}_{A/I}(\Omega_{A/k} \otimes_A (A/I),N)} \to \underset{\| \mathrm{Hom}_A(I,N)}{\mathrm{Hom}_{A/I}(I/I^2,N)}$$

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

$$D: k[x_1,\ldots,x_n] \to M$$

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: $\mathrm{Der}_k(k[x_1,\dots,x_n],M) = M\frac{\partial}{\partial x_1} \oplus \cdots \oplus M\frac{\partial}{\partial x_n}$.

21. Proposición: $\Omega_{k[x_1,\dots,x_n]/k} = k[x_1,\dots,x_n]dx_1 \oplus \cdots \oplus k[x_1,\dots,x_n]dx_n$, $dp \mapsto \sum_i \frac{\partial f}{\partial x_i} dx_i$.

Demostración. Se deduce de las igualdades

$$\begin{aligned} Hom_{k[x_1,\dots,x_n]}(\Omega_{k[x_1,\dots,x_n]/k}, M) &= \mathrm{Der}_k(k[x_1,\dots,x_n],M) = M\frac{\partial}{\partial x_1} \oplus \cdots \oplus M\frac{\partial}{\partial x_n} \\ &= \mathrm{Hom}_{k[x_1,\dots,x_n]}(k[x_1,\dots,x_n]dx_1 \oplus \cdots \oplus k[x_1,\dots,x_n]dx_n, M) \end{aligned}$$

□

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 3.7.19. □

23. Teorema: *Sea k un cuerpo. Una k-álgebra finita A es separable si y sólo $\Omega_{A/k} = 0$.*

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 sólo 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 $A = k[x](p(x))$. Probar que $\Omega_{A/k} = k[x]/(p,p')dx$. Probar que $\Omega_{A/k} = 0 \Leftrightarrow p(x)$ tiene raíces dobles.
2. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcular $\Omega_{A/k}$, $\Omega_{A/K}$ y $\Omega_{K/k}$.
3. Probar que $\Omega_{\varinjlim A_i/k} = \varinjlim \Omega_{A_i/k}$.
4. Sea A una k-álgebra finita y racional. Probar que $\Omega_{A/k} = 0 \Leftrightarrow A = k$.
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, probar 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. Probar: 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. Probar: $B \xrightarrow{\text{traza}} \mathrm{Hom}_A(B,A)$ es isomorfismo si y sólo si $\Omega_{B/A} = 0$.
9. Sea $A = k[x]/(p(x))$, siendo k de característica cero. Probar 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. Probar:
   a) Si $\overline{K}$ es separable, $\Omega_{\overline{K}[x]/K} = \overline{K}[x]$.
   b) Si $\overline{K}$ no es separable, $\Omega_{\overline{K}[x]/K} = \overline{K}[x] \oplus \overline{K}[x]$.

3.7.2. 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 $\mathbb{A}^n = \operatorname{Spec} k[x_1,\dots,x_n]$ 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 3.7.29, 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 $\{\bar f_1,\dots,\bar f_n\}$ es una base de $\mathfrak{m}_x/\mathfrak{m}_x^2$, entonces $\mathfrak{m}_x = (f_1\dots,f_n)$ y $0 = \dim(A_x/(f_1,\dots,f_n)) \geq \dim A_x - n$.

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 $f\colon M \to L$ un morfismo en un libre finito generado. Si $\bar f\colon M/\mathfrak{m}M \to L/\mathfrak{m}L$ es inyectivo, entonces f es inyectivo y los módulos M y $\operatorname{Coker} f$ son libres.*

Demostración. Sean $m_1,\dots,m_r \in M$ tales que $\bar m_1,\dots,\bar m_r \in M/\mathfrak{m}M$ es una base. Por el lema de Nakayama, $m_1,\dots,m_r$ es un sistema generador de M. Sea $\overline{f(m_1)},\dots,\overline{f(m_r)},\bar l_1,\dots,\bar l_r$ una base de $L/\mathfrak{m}L$. Por el lema 0.7.3, $f(m_1),\dots,f(m_r),l_1,\dots,l_s$ es una base de L. Luego, $m_1,\dots,m_r$ es una base de M, f es inyectivo y $\operatorname{Coker} f$ es libre de base $l_1,\dots,l_s$. □

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.

$\Leftarrow$) $I_x = (f_1,\dots,f_r)$, con $d_x f_1,\dots,d_x f_r \in \mathfrak{m}_x/\mathfrak{m}_x^2$ 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

$$0 \to \langle d_x f_1, \dots, d_x f_r \rangle \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Por el lema 3.7.29, $(\Omega_{(A/I)/k})_x$ 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 $\dim(A/J)_x = \dim(A/I)_x$, $(A/J)_x$ es íntegra y el epimorfismo de paso al cociente $\pi\colon (A/J)_x \to (A/I)_x$. 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 $\dim X = n-r$. Probar que X es liso en x si y sólo 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 sólo 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 sólo 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 sólo 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 3.7.30, 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 3.7.30. □

3.7.3. 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*

$$\dim_K \Omega_{K/k} \geq \operatorname{grtr}_k K$$

Además, la desigualdad es una igualdad si y sólo 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 verifica 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

$$\begin{array}{ccccc} (p(x))/(p(x)^2) & \to & \Omega_{\Sigma[x]/k} \underset{\Sigma[x]}{\otimes} \Sigma(\xi) \to \Omega_{\Sigma(\xi)/k} \to 0 \\ p(x) & \mapsto & dp(x) \end{array}$$

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 $dx_1,\dots,dx_n$ 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 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 $\dim_K\Omega_{K/k}\geq \mathrm{gr\,tr}_k K=\mathrm{gr\,tr}_k k(\xi_1,\dots,\xi_n)=n$, $\{d\xi_1,\dots,d\xi_n\}$ es una base del K-espacio vectorial $\Omega_{K/k}$. □

36. Proposición: *Sea $X=\mathrm{Spec}A$ 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 $\dim_\Sigma\Omega_{\Sigma/k}=\mathrm{gr\,tr}\,\Sigma=\dim X$. 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. □

3.8. 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.

Del modo más simple, podemos decir que la Geometría Algebraica es el estudio de las soluciones de un sistema de ecuaciones polinómicas en un espacio proyectivo, es decir, el estudio de las variedades algebraicas proyectivas.

En Geometría Proyectiva el espacio proyectivo de dimensión n se define como el conjunto de rectas (que pasan por el origen) de un espacio vectorial de dimensión $n+1$. En Geometría Algebraica vamos a definir de modo equivalente, a partir de $\mathbb{A}^{n+1}=\mathrm{Spec}\,\mathbb{C}[x_0,\dots,x_n]$, 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. Así, las subvariedades 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 $\mathbb{A}^{n+1}$.

Si $p(x_0,\dots,x_n)\in k[x_0,\dots,x_n]$ es una función que se anula en la 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.

Denotaremos por $\mathbb{P}^n=\mathrm{Proj}\,\mathbb{C}[x_0,\dots,x_n]$ el conjunto de ideales primos homogéneos (= generados por polinomios homogéneos) de $\mathbb{C}[x_0,\dots,x_n]$.

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 $U_i = \{$rectas de $\mathbb{C}^{n+1}$ 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

$$U_i = \{\text{rectas } \lambda(\alpha_0,\dots,\alpha_n) \mid \alpha_i \neq 0\} \longleftrightarrow \mathbb{A}^n$$

$$\lambda(\alpha_0,\dots,\alpha_n) \longmapsto (\tfrac{\alpha_0}{\alpha_i},\dots,\tfrac{\alpha_n}{\alpha_i})$$

En Álgebra Conmutativa, veremos que el conjunto $U_i = \{x \in \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]$ que no yacen en $(x_i)_0\}$ se identifica con $\operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]_{x_i}$ (se dota a $\frac{1}{x_i}$ de grado -1), y la composición de los morfismos

$$U_i \hookrightarrow \mathbb{A}^{n+1} - (x_i)_0 \longrightarrow \mathbb{A}^n$$

$$(\alpha_0,\dots,\alpha_n) \longmapsto (\tfrac{\alpha_0}{\alpha_i},\dots,\tfrac{\alpha_n}{\alpha_i})$$

$$\mathbb{C}[x_0,\dots,x_n]_{x_i} \hookleftarrow \mathbb{C}[\tfrac{x_0}{x_i},\dots,\tfrac{x_n}{x_i}]$$

induce un homeomorfismo $U_i = \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]_{x_i} \simeq \operatorname{Spec}\mathbb{C}[\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}]$. Además se prueba que $\mathbb{P}^n = \underset{i}{\cup} U_i$.

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 un anillo $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ es un álgebra graduada, si para cada $r_i \in R_i$ y $r_j \in R_j$, entonces $r_i \cdot r_j \in R_{i+j}$. Diremos que $r_i \in R_i$ es un elemento homogéneo de grado i.

2. 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.

3. Ejercicio: Probar que un ideal $I \subseteq R$ es homogéneo si y sólo si $I = \underset{n}{\oplus} I_n$, siendo $I_n = I \cap R_n$.

4. Ejercicio: Probar que un ideal homogéneo $\mathfrak{p} \subseteq R$ es primo si y sólo si cumple que si el producto de dos elementos homogéneos pertenece a $\mathfrak{p}$ entonces uno de los dos pertenece a $\mathfrak{p}$.

5. Definición: Llamaremos ideal irrelevante de R al ideal $(\underset{n\neq 0}{\oplus} R_n) \subseteq R$.

6. 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.

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 $\operatorname{Spec}R$. Si denotamos $(f)_0^h = \{x \in \operatorname{Proj}R, f \in \mathfrak{p}_x\}$ y escribimos $f = f_n + f_{n+1}\cdots + f_m$, es obvio que $(f)_0^h = (f_n,\dots,f_m)_0^h = (f_n)_0^h \cap \cdots \cap (f_m)_0^h$. Por tanto, una base de abiertos de la topología de $\operatorname{Proj}R$ son los abiertos

$$U_f^h = \{x \in \operatorname{Proj}R, f \notin \mathfrak{p}_x\},\ \ (f \text{ homogéneo})$$

7. Definición: Llamaremos espacio proyectivo de dimensión n (sobre k) a

$$\mathbb{P}_k^n = \operatorname{Proj} k[x_0,\dots,x_n]$$

8. Definición: Diremos que un morfismo de álgebras $\phi\colon R \to R'$ graduadas es un morfismo graduado (de grado r) si transforma funciones homogéneas de grado n en funciones homogéneas de grado nr, para todo $n \in \mathbb{Z}$.

Si $\phi\colon R \to R'$ es un morfismo graduado entonces el morfismo inducido $\phi^*\colon \mathrm{Spec}R' \to \mathrm{Spec}R$, aplica ideales primos homogéneos en ideales primos homogéneos. Si suponemos que la imagen del ideal irrelevante de R por ϕ, no está contenido en más ideal primo homogéneo que los que contengan al irrelevante de R', tenemos definido un morfismo

$$\phi^*\colon \mathrm{Proj}R' \to \mathrm{Proj}R, x \mapsto \phi^*(x), \text{ donde } \mathfrak{p}_{\phi*(x)} = \phi^{-1}(\mathfrak{p}_x)$$

9. Ejemplo: Sea $\phi\colon k[x_0,x_1,x_2] \to k[x_0,x_1,x_2]$, $\phi(x_i) = \sum_j \lambda_{ij}x_j$, de modo que $\det(\lambda_{ij}) \neq 0$. Entonces ϕ es un isomorfismo graduado, que induce un isomorfismo $\phi^*\colon \mathbb{P}^2 \to \mathbb{P}^2$. Diremos que ϕ es un cambio de coordenadas homogéneo.

Si $f_m \in R$ es un elemento homogéneo de grado m, entonces R_{f_m} es una álgebra graduada, diciendo que el grado de $\frac{g_n}{f_m^r}$ es $n - mr$, para cada $g_n \in R_n$. Dejamos que el lector demuestre la siguiente proposición.

10. Proposición: *1. El morfismo de localización $R \to R_f$ (f homogénea) es un morfismo graduado que induce un isomorfismo*

$$\mathrm{Proj}R_f = U_f^h = \mathrm{Proj}R\backslash(f)_0^h$$

2. Si I es un ideal homogéneo de R entonces R/I es un álgebra graduada homogénea, de modo que el morfismo $R \to R/I$ es un morfismo graduado que induce un isomorfismo

$$\mathrm{Proj}(R/I) = (I)_0^h$$

Dada un álgebra graduada R denotaremos por R_n al conjunto de los elementos homogéneos de grado n de R. Observemos que R_0 es un subanillo de R.

11. Proposición: *Sea R un álgebra graduada y $f \in R$ un elemento homogéneo de grado $r > 0$. Entonces,*

$$U_f^h = \mathrm{Proj}R_f = \mathrm{Spec}[R_f]_0$$

Demostración. Veamos que la composición de los morfismos naturales

$$\mathrm{Proj}R_f \hookrightarrow \mathrm{Spec}R_f \to \mathrm{Spec}[R_f]_0,$$

que asigna a cada ideal primo homogéneo $\mathfrak{p} \subset R_f$ el ideal primo $[\mathfrak{p}]_0 := \mathfrak{p} \cap [R_f]_0$, es el homeomorfismo buscado. Observemos que el ideal primo $\mathfrak{p} \subset R_f$ está determinado por sus elementos homogéneos de grado cero: un elemento homogéneo $g \in R_f$ de grado m pertenece a $\mathfrak{p}$ si y sólo si g^r/f^m pertenece a $[\mathfrak{p}]_0$. Por tanto, $\mathrm{Proj}R_f \to \mathrm{Spec}[R_f]_0$ es inyectivo. Si $\mathfrak{q} \subset [R_f]_0$ es un ideal primo, entonces $\mathfrak{p} := \oplus_m \mathfrak{p}_m$ con $\mathfrak{p}_m := \{g \in [R_f]_m \mid g^r \cdot f^{-m} \in \mathfrak{q}\}$, es un ideal primo homogéneo: Si $g, g' \in R_f$ son dos elementos homogéneos de grados m y m' respectivamente, tales que $g \cdot g' \in \mathfrak{p}$, entonces $(g^r/f^m)\cdot(g'^r/f^{m'}) = (gg')^r/f^{m+m'} \in \mathfrak{q}$, luego g^r/f^m ó $g'^r/f^{m'}$ pertenece a $\mathfrak{q}$, y por tanto g ó g' pertenece a $\mathfrak{p}$. Observemos que $\mathfrak{p} \cap [R_f]_0 = \mathfrak{q}$. En conclusión, $\mathrm{Proj}R_f \to \mathrm{Spec}[R_f]_0$ es biyectivo. Finalmente, si $g \in R$ es homogénea de grado m, la biyección anterior transforma $(g)_0^h = (g^r/f^m)_0^h$ en $(g^r/f^m)_0$. Luego la biyección continua dada es un homeomorfismo.

□

Por sencillez, supondremos a partir de ahora que $R = R_0[\xi_0,\ldots,\xi_n]$, donde cada ξ_i es de grado 1. En este caso, $[R_0[\xi_0,\ldots,\xi_n]_{\xi_i}]_0 = R_0[\xi_0/\xi_i,\ldots,\xi_n/\xi_i]$ donde $R_0[\xi_0/\xi_i,\ldots,\xi_n/\xi_i]$ es la R_0-subálgebra de $R_0[\xi_0,\ldots,\xi_n]_{\xi_i}$ generada por $\xi_0/\xi_i,\ldots,\xi_n/\xi_i$.

12. Teorema: *Sea $R = R_0[\xi_0,\ldots,\xi_n]$. Denotemos U_i al abierto básico* $\mathrm{Proj}R\backslash(\xi_i)_0^h$. *Entonces,*

1. $\mathrm{Proj}R = \bigcup_{i=0}^{n} U_i$.

2. U_i es homeomorfo a $\mathrm{Spec}R_0[\frac{\xi_0}{\xi_i},\ldots,\frac{\xi_n}{\xi_i}]$.

Diremos que U_i es un abierto afín de $\mathrm{Proj}R$. *Por tanto, el espectro proyectivo admite un recubrimiento por abiertos afines.*

Demostración. 1. $\operatorname{Proj} R = \bigcup_{i=0}^{n} U_i$, ya que $\bigcap_{i=0}^{n} (\xi_i)_0^h = (\xi_0,\dots,\xi_n)_0^h = \emptyset$, pues $(\xi_0,\dots,\xi_n)$ es el ideal irrelevante.

2. Es consecuencia de la proposición 3.8.11.

□

Si C es un cerrado de $\operatorname{Proj} R$, entonces $C = (J)_0^h$, donde podemos suponer que J es un ideal homogéneo de R; de hecho el ideal I de todas las funciones de R que se anulan en C es homogéneo y $C = (I)_0^h$. Si C es irreducible, entonces $I = \mathfrak{p}_x$ es primo (y homogéneo) y C es el cierre de x en $\operatorname{Proj} R$.

Todo subespacio de un espacio noetheriano es noetheriano. Por tanto, si $R = k[\xi_0,\dots,\xi_n]$ 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.

13. Definición: Llamaremos dimensión de $\operatorname{Proj} R$ al máximo de las longitudes de sus cadenas de cerrados irreducibles, que coincide con el máximo de las longitudes de las cadenas de ideales primos homogéneos de R que no contengan al ideal irrelevante.

Si $\bar{x}_1 \supset \cdots \supset \bar{x}_m$ es una cadena de cerrados irreducibles de longitud máxima de $\operatorname{Proj} R$ y $x_m \in U_{\xi_i}^h \subseteq \operatorname{Proj} R$, entonces $\bar{x}_1 \cap U_{\xi_i}^h \supset \cdots \supset \bar{x}_m \cap U_{\xi_i}^h$ es una cadena de cerrados irreducibles en $U_{\xi_i}^h$. Como la dimensión de un abierto es siempre menor o igual que la del espacio, tenemos que

$$\dim \operatorname{Proj} R = \dim U_{\xi_i}^h = \dim k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$$

14. 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 $\mathbb{P}^n$. Si además es de dimensión 1, diremos que es una curva proyectiva.

15. Proposición: *Las variedades proyectivas son catenarias.*

Demostración. Dados dos cerrados irreducibles $\bar{x}_1 \supset \bar{x}_2$, sea $U = U_{\xi_i}^h$ un abierto afín que contenga a x_2. Toda cadena maximal de cerrados irreducibles de extremos $\bar{x}_1$ y $\bar{x}_2$ induce, cortando con U, una cadena maximal en U (de extremos dados). Se concluye por 3.6.8, pues U es una variedad algebraica afín. □

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 sólo 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 que $m \sim m'$ si y sólo 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

$$\operatorname{Hom}_{\mathscr{C}^\infty(X)}(\Omega_{\mathscr{C}^\infty(X)/\mathbb{R}}/\sim, \mathscr{C}^\infty(X)) = \operatorname{Hom}_{\mathscr{C}^\infty(X)}(\Omega_{\mathscr{C}^\infty(X)/\mathbb{R}}, \mathscr{C}^\infty(X)) = \operatorname{Der}_{\mathbb{R}}(\mathscr{C}^\infty(X), \mathscr{C}^\infty(X))$$

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

$$i_w : M \otimes_A \overset{n}{\cdots} \otimes_A M \to M \otimes_A \overset{n-1}{\cdots} \otimes_A M,\ i_w(m_1 \otimes \cdots \otimes m_n) := \sum_{i=1}^{n} (-1)^i w(m_i) \cdot w_1 \otimes \cdots \otimes \widehat{m_i} \otimes \cdots \otimes m_n$$

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 finito generado, 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

$$i_{\tilde{w}} : \mathrm{Hem}_A(M^*, \overset{n}{\ldots}, M^*; A) \to \mathrm{Hem}_A(M^*, \overset{n-1}{\ldots}, M^*; A), \quad (i_{\tilde{w}} F)(w_2, \ldots, w_n) := F(w, w_2, \ldots, w_n).$$

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, 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, $\Omega_{A/k} \simeq L/N$, $adb \mapsto ad\mathbf{b}$.*

Demostración. Sea M un A-módulo. Entonces,

$$\mathrm{Hom}_A(L/N, M) = \{f \in \mathrm{Hom}_A(L, M) :\ f_{|N} = 0\} = \{f \in \mathrm{Aplic}(A, M) :\ f(a+b) = f(a) + f(b),\ f(\lambda a) = \lambda f(a),$$
$$f(ab) = af(b) + bf(a) \mid \forall a, b \in A, \lambda \in k\} = \mathrm{Der}_k(A, M) = \mathrm{Hom}_A(\Omega_{A/k}, M)$$

Luego, $\Omega_{A/k} \simeq L/N$. □

4. Teorema: *El morfismo natural $d : A \to \Omega_{A/k}$, $a \mapsto da$ 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 $d_i : \Lambda^i \Omega_{A/k} \to \Lambda^{i+1} \Omega_{A/k}$, 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 $d_1 : \Omega_{A/k} \to \Lambda^2 \Omega_{A/k}$, $adb \mapsto da \wedge db$ (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 $d : \Omega^{\cdot} \to \Omega^{\cdot}$ 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 $\{e_1, \ldots, e_n\}$ y sea $\{w_1, \ldots, w_n\}$ 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. Teorema: *La sucesión*

$$0 \to S^\cdot_k E^* \overset{\mathrm{Id}^\wedge}{\to} S^\cdot_k E^* \otimes E \overset{\mathrm{Id}^\wedge}{\to} S^\cdot_k E^* \otimes \Lambda^2 E \overset{\mathrm{Id}^\wedge}{\to} \cdots \overset{\mathrm{Id}^\wedge}{\to} S^\cdot_k E^* \otimes \Lambda^{n-1} E \overset{\mathrm{Id}^\wedge}{\to} S^\cdot_k E^* \otimes \Lambda^n E$$

es exacta y $(S^\cdot_k E^* \otimes \Lambda^n E)/\mathrm{Id}^\wedge(S^\cdot_k E^* \otimes \Lambda^{n-1} E) = \Lambda^n E$.

Demostración. Dada $s_m \otimes \Omega_r \in S^m_k E^* \otimes_k \Lambda^r_k E$ se cumple que

$$\begin{aligned}(i_{\mathrm{Id}} \circ \mathrm{Id}^\wedge + \mathrm{Id}^\wedge \circ i_{\mathrm{Id}})(s_m \otimes \Omega_r) &= \sum_i i_{\mathrm{Id}}(w_i \cdot s_m \otimes e_i \wedge \Omega_r) + \mathrm{Id}^\wedge(i_{e_i} s_m \otimes i_{w_i}\Omega_r)\\ &= \sum_{ij}(\delta_{ij}s_m + w_i \cdot i_{e_j} s_m) \otimes (\delta_{ij}\Omega_r - e_i \wedge i_{w_j}\Omega_r) + w_j \cdot i_{e_i} s_m \otimes e_j \wedge i_{w_i}\Omega_r\\ &= \sum_{ij} \delta_{ij} s_m \otimes (\delta_{ij}\Omega_r - e_i \wedge i_{w_j}\Omega_r) + w_i \cdot i_{e_j} s_m \otimes \delta_{ij}\Omega_r\\ &= \sum_i (s_m \otimes \Omega_r - s_m \otimes (e_i \wedge i_{w_i}\Omega_r) + i_{w_i} s_m \otimes \Omega_r) = (n-r+m)\cdot s_m \otimes \Omega_r\end{aligned}$$

El núcleo de $\mathrm{Id}^\wedge$ es la suma directa de los núcleos de los morfismos $\mathrm{Id}^\wedge : S^m_k E^* \otimes_k \Lambda^r_k E \to S^{m+1}_k E^* \otimes_k \Lambda^{r+1}_k E$. Si $s_m \otimes \Omega_r \in \operatorname{Ker}\mathrm{Id}^\wedge$, entonces

$$(n-r+m)\cdot s_m \otimes \Omega_r = (i_{\mathrm{Id}} \circ \mathrm{Id}^\wedge + \mathrm{Id}^\wedge \circ i_{\mathrm{Id}})(s_m \otimes \Omega_r) = \mathrm{Id}^\wedge \circ i_{\mathrm{Id}}(s_m \otimes \Omega_r) \in \operatorname{Im}\mathrm{Id}^\wedge$$

Luego, si $r \neq n$ y $m \neq 0$, $s_m \otimes \Omega_r \in \operatorname{Im}\mathrm{Id}^\wedge$. Por último, $S^0E^* \otimes \Lambda^n E^* \subset \operatorname{Ker}\mathrm{Id}^\wedge$ y $\operatorname{Im}\mathrm{Id}^\wedge \cap (S^0E^* \otimes \Lambda^n E^*) = 0$. □

11. 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.

Tenemos isomorfismos canónicos $\Lambda^p E \otimes_k \Lambda^n E^* = \Lambda^{n-p} E^*$, luego $(S^\cdot_k E^* \otimes \Lambda^\cdot E) \otimes \Lambda^n E^* = S^\cdot_k E^* \otimes \Lambda^\cdot E^*$. 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 3.9.11, obtenemos el teorema de De Rham.

12. 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

13. Ejercicio: Sea $A = k[x, 1/x]$. Probar 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

14. 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. $d(am) = a\,dm + m \otimes da$, para todo $a \in A$ y $m \in M$.

15. Ejemplo: La diferencial canónica $d : A \to \Omega_{A/k} = A \otimes_A \Omega_{A/k}, a \mapsto da$, es una diferencial en A.

16. 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.

17. 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 $\{m_1,\dots,m_r\}$, $\Omega_{A/k}$ es una A-módulo libre de base $da_1,\dots,da_n$ 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 $m'\otimes\Omega_j \in M'\otimes\Omega^j$ denotemos $(m\otimes\Omega_i)\wedge(m'\otimes\Omega_j) := m\otimes m'\otimes\Omega_i\wedge\Omega_j \in M\otimes M'\otimes\Omega^{i+j}$. Tenemos un morfismo

$$\begin{array}{ccc} (M\otimes\Omega^\cdot)\otimes(M'\otimes\Omega^\cdot) & \xrightarrow{\wedge} & M\otimes M'\otimes\Omega^\cdot \\ w_i\otimes w_j & \mapsto & w_i\wedge w_j \end{array}$$

La diferencial $d: M\to M\otimes\Omega_{A/k}$ extiende a $d: M\otimes\Omega^\cdot \to M\otimes\Omega^\cdot$: $d(m\otimes\Omega_i) := dm\wedge\Omega_i + m\otimes d\Omega_i$. Los elementos de $M\otimes\Omega^i$ los llamaremos i-formas valoradas en M.

Dada otra diferencial $d: M'\to M'\otimes\Omega$, tenemos la diferencial $d: M\otimes_A M' \to M\otimes_A M'\otimes_A\Omega$, $d(m\otimes m') := dm\wedge m' + m\wedge dm'$, 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

$$\boxed{D^L\circ i_{D'} - i_{D'}\circ D^L = i_{[D,D']}}$$

18. Definición: Una conexión ∇ en un A-módulo M es una aplicación $\mathrm{Der}_k(A,A)\times M\to M$, donde seguimos la notación $(D,m)\mapsto D^\nabla m$, cumpliendo, 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. $D^\nabla(m+m') = D^\nabla m + D^\nabla m'$.

19. Proposición: *Supongamos que $\Omega_{A/k}$ es un A-módulo libre finito generado. Existe una correspondencia biunívoca entre conexiones en M y diferenciales de M.*

Demostración. Dada una diferencial $d: M\to M\otimes_A\Omega_{A/k}$, le asignamos la conexión ∇ definida por $D^\nabla m := i_D(dm)$, que cumple que $D^\nabla(am) = i_D(d(am)) = i_D(m\otimes da + a\,dm) = (Da)m + a\,i_D dm = (Da)m + aD^\nabla m$ 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.

□

20. Notación: A partir de ahora, supondremos que $\Omega_{A/k}$ es un A-módulo libre finito generado (como sucede cuando $X = \mathrm{Spec}\,A$ es una variedad lisa).

$\mathrm{Der}_k(A,A)$ es un A-módulo libre finito generado y $\Omega_{A/k}$ y $\mathrm{Der}_k(A,A)$ son duales entre sí. Recordemos que $\Omega^i = \mathrm{Hem}_A(\mathrm{Der}_k(A,A),\overset{i}{\ldots},\mathrm{Der}_k(A,A);A)$, luego $M\otimes_A\Omega^i = \mathrm{Hem}_A(\mathrm{Der}_k(A,A),\overset{i}{\ldots},\mathrm{Der}_k(A,A);M)$: $m\otimes\Omega_i \in M\otimes_A\Omega^i$ pensado en $\mathrm{Hem}_A(\mathrm{Der}_k(A,A),\overset{i}{\ldots},\mathrm{Der}_k(A,A);M)$ es la aplicación multilineal hemisimétrica $(m\otimes\Omega_i)(D_1,\ldots,D_i) := \Omega_i(D_1,\ldots,D_i)\cdot m$.

Dada una 1-forma valorada $w\in M\otimes\Omega$, tenemos que

$$(dw)(D_1,D_2) = i_{D_2}(i_{D_1}dw) = i_{D_2}(-d(w(D_1)) + D_1^L w) = D_1^\nabla(w(D_2)) - D_2^\nabla(w(D_1)) - w([D_1,D_2])$$

En particular,

$$d^2(m)(D_1,D_2) = D_1^\nabla D_2^\nabla m - D_2^\nabla D_1^\nabla m - [D_1,D_2]^\nabla m \tag{3.9.1}$$

21. 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 $\mathrm{Hom}_A(M,N)$ 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, $R\wedge m = d^2m$. Observemos que

$$R(D_1,D_2,m) = d^2(m)(D_1,D_2) = D_1^\nabla D_2^\nabla m - D_2^\nabla D_1^\nabla m - [D_1,D_2]^\nabla m.$$

22. Proposición: *Dada $w\in M\otimes\Omega^i$, entonces*

$$\boxed{d^2w = R\wedge w}$$

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 de S como elemento de $\mathrm{Hom}_A(M,N\otimes\Omega^n)$, coincide con la diferencial de S como elemento de $\mathrm{Hom}_A(M,N)\otimes\Omega^n\subset\mathrm{Hom}_A(M,N)\otimes\Omega^\cdot$.

23. 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

$$\begin{array}{ccc} M & \xrightarrow{d^2} & M\otimes\Omega^2 \\ {\scriptstyle d}\downarrow & & \downarrow{\scriptstyle d} \\ M\otimes\Omega & \xrightarrow{d^2} & M\otimes\Omega^3 \end{array}$$

es conmutativo. □

24. Definición: Una conexión sobre $M=\mathrm{Der}_k(A,A)$ se llama conexión lineal.

25. Definición: Sea ∇ una conexión lineal. Pensemos $\mathrm{Id} \in \mathrm{Hom}_A(\mathrm{Der}_k(A,A),\mathrm{Der}_k(A,A)) = \mathrm{Der}_k(A,A)\otimes\Omega$ como una 1-forma valorada (no como endomorfismo). Definimos $\mathrm{Tor}_\nabla := d\,\mathrm{Id} \in \mathrm{Der}_k(A,A)\otimes\Omega^2$

Explícitamente,

$$\mathrm{Tor}_\nabla(D_1,D_2) = (d\,\mathrm{Id})(D_1,D_2) = D_1^\nabla(\mathrm{Id}(D_2)) - D_2^\nabla(\mathrm{Id}(D_1)) - \mathrm{Id}([D_1,D_2]) = D_1^\nabla D_2 - D_2^\nabla D_1 - [D_1,D_2]$$

Observemos que la curvatura $R \in \mathrm{End}_A(\mathrm{Der}_k(A,A))\otimes_A\Omega^2$.

26. Definición: Se dice que una conexión lineal ∇ es simétrica si $\mathrm{Tor}_\nabla = 0$.

27. 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,

$$\boxed{R(D_1,D_2)(D_3) + R(D_3,D_1)(D_2) + R(D_2,D_3)(D_1) = 0}$$

28. 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 sólo si $\pi\circ d^\nabla = -d_C$.

Demostración. $\pi(d^\nabla w)(D_1,D_2) = (d^\nabla w)(D_1,D_2) - (d^\nabla w)(D_2,D_1) = (D_2^\nabla w)(D_1) - (D_1^\nabla w)(D_2) = D_2(w(D_1)) - w(D_2^\nabla D_1) - D_1(w(D_2)) + w(D_1^\nabla D_2)$. 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.

29. Proposición: *Se cumple que*

$$[\textit{Conj. conexiones lineales}] = [\textit{Conj. conexiones lineales simétricas}]\times[\mathrm{Der}_k(A,A)\otimes_A\Omega^2],\ \nabla\mapsto(\nabla_s,\mathrm{Tor}_\nabla)$$

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,

$$\begin{aligned}d_s^\nabla(w)(D_1,D_2) &= (D_1^\nabla w)(D_2) + (D_2^\nabla w)(D_1) = D_1(w(D_2)) - w(D_1^\nabla D_2) + D_2(w(D_1)) - w(D_2^\nabla D_1)\\ &= D_1(w(D_2)) + D_2(w(D_1)) - w(D_1^\nabla D_2 + D_2^\nabla D_1)\end{aligned}$$

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.

30. Proposición: *Se cumple que*

$$[\textit{Conj. de conexiones lineales simétricas}] = [\textit{Conj. de diferenciales simétricas } d_s\colon\Omega\to S^2\Omega],\ \nabla\mapsto d_s^\nabla$$

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 $d_s\colon S^\cdot\Omega\to S^\cdot\Omega$, $d_s(w_1\cdots w_m) := \sum_i w_1\cdots d_s w_i\cdots w_m$ (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: $D^\nabla(w_1\cdots w_r):=\sum_{i=1}^r w_1\cdots D^\nabla w_i\cdots w_r$, para todo $w_i\in\Omega$ y $D\in\mathrm{Der}_k(A,A)$.

31. 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 M y N dos A-módulos. Se dice que $F\colon N\to M$ 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.

32. 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 $n\in N$.

33. Ejemplo: Las derivaciones $D\in\mathrm{Der}_k(A,M)$ son operadores diferenciales de orden 1.

34. Proposición: *$F\colon N\to M$ es un operador diferencial de orden $n>0$ si y sólo si $[F,a]:=F\circ a\cdot-a\cdot F$ es un operador diferencial de orden $n-1$ para todo $a\in A$.*

35. 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 $r+s$.

□

36. Notación: $\mathrm{Diff}_k^n(N,M)$ denota el conjunto de operadores diferenciales de N en M de orden n.

37. Proposición: *Sea $\mathfrak{m}\subset A$ un ideal tal que $A/\mathfrak{m}=k$. Supongamos que M es un $A/\mathfrak{m}$-módulo. Entonces,*

$$\mathrm{Diff}_k^n(N,M)=\mathrm{Hom}_k(N/\mathfrak{m}^{n+1}\cdot N,M)$$

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.

□

38. 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 $a\in A$).

39. 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 $j^r_N : N \to J^r_{N/k}$, $j^r_N(n) := \overline{1\otimes n}$.

40. 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

$$\begin{aligned}\mathrm{Diff}^n_k(N,M) = \mathrm{Diff}^n_A(A\otimes_k N, M) &\overset{3.9.37}{=} \mathrm{Hom}_A((A\otimes_k N)/(\Delta^{n+1}\cdot(A\otimes_k N)), M)\\ &= \mathrm{Hom}_A((A\otimes_k A/\Delta^{n+1})\otimes_A N, M) = \mathrm{Hom}_A(J^n_{N/k}, M)\end{aligned}$$

□

Tenemos la cadena de inclusiones (en $\mathrm{Hom}_k(A,A)$)

$$\mathrm{Diff}^1_k(A,A)\hookrightarrow \mathrm{Diff}^2_k(A,A)\hookrightarrow\cdots\hookrightarrow \mathrm{Diff}^n_k(A,A)\hookrightarrow\cdots$$

41. Definición: $\mathrm{Diff}_k(A,A) = \bigcup_{i=0}^{\infty}\mathrm{Diff}^i_k(A,A)$.

42. 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 (4.3.13). 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.

□

43. Notación: A partir de ahora supondremos que $X = \mathrm{Spec}\,A$ es lisa y que $\mathrm{car}\,k = 0$.

44. 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

$$0\to\mathrm{Diff}^{n-1}_k(A,A)\to\mathrm{Diff}^n_k(A,A)\overset{\mathrm{simb}_n}{\to} S^n\,\mathrm{Der}_k(A,A)\to 0$$

Se dice que $\mathrm{simb}_n(F)$ es el símbolo del operador $F\in\mathrm{Diff}^n_k(A,A)$.

Tenemos que $\mathrm{Diff}^n_k(A,A) = \mathrm{Diff}^{n-1}_k(A,A)\oplus S^n\,\mathrm{Der}_k(A,A) = \cdots = \oplus_{i=0}^n S^i\,\mathrm{Der}_k(A,A)$.

45. Proposición: *Sean $D_1,\dots,D_r\in\mathrm{Der}_k(A,A)$. 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 $\mathrm{Diff}_+^r(A,A) := \{F\in\mathrm{Diff}_k^r(A,A)\colon F(1)=0\}$.

46. Proposición: *Se cumple que*

$$[\textit{Conjunto de conexiones lineales simétricas}] = \{s\in \mathrm{Hom}_A(S^2\mathrm{Der}(A,A),\mathrm{Diff}_+^2(A,A))\colon \mathrm{simb}_2\circ s=\mathrm{Id}\}$$

Demostración. Dada una conexión lineal simétrica, ∇, definimos $s\colon S^2\mathrm{Der}(A,A)\to\mathrm{Diff}_+^2(A,A)$ por $s(D_1\cdot D_2) := D_1\circ D_2 - D_1^\nabla D_2$. 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 $\mathrm{Der}_k(A,A)$.

□

47. Teorema: *Sea d_s la diferencial simétrica asociada a una conexión lineal simétrica. Los morfismos*

$$(A\otimes A)/\Delta^{n+1}\overset{\phi_n}{\to} A\oplus\Omega\oplus\cdots\oplus S^n\Omega,\quad \overline{a\otimes b}\mapsto a\cdot(b,db,d_s^2b/2,\ldots,d_s^nb/n!)$$

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 $\phi_n(\overline{a\otimes 1-1\otimes a}) = (0,da,-,\ldots,-)$, 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. □

48. Corolario: *El morfismo $A/\mathfrak{m}_x^{n+1}\to k\oplus\mathfrak{m}_x/\mathfrak{m}_x^2\oplus\cdots\oplus\mathfrak{m}_x^n/\mathfrak{m}_x^{n+1}$, $\bar f\mapsto\sum_{i=0}^n \frac{d_s^i f}{i!}(x)$, es un isomorfismo de k-álgebras.*

El enunciado dual del teorema 3.9.47 es el que sigue.

49. Teorema: *Sea d_s la diferencial simétrica asociada a una conexión lineal simétrica. Entonces,*

$$S^{\cdot}\operatorname{Der}_k(A,A) \overset{\varphi}{=} \operatorname{Diff}_k(A,A),\ \varphi(D_1\cdots D_n)(a) := \frac{d_s^n a}{n!}(D_1,\ldots,D_n)$$

y se tiene el diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overset{n-1}{\underset{i=0}{\oplus}} S^i\operatorname{Der}_k(A,A) & \hookrightarrow & \overset{n}{\underset{i=0}{\oplus}} S^i\operatorname{Der}_k(A,A) & \longrightarrow & S^n\operatorname{Der}_k(A,A) & \longrightarrow & 0 \\
 & & \Vert\varphi & & \Vert\varphi & & \Vert\mathrm{Id} & & \\
0 & \longrightarrow & \operatorname{Diff}_k^{n-1}(A,A) & \hookrightarrow & \operatorname{Diff}_k^{n}(A,A) & \longrightarrow & S^n\operatorname{Der}_k(A,A) & \longrightarrow & 0
\end{array}$$

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, $\operatorname{Diff}_k(A,A)$ 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 $\operatorname{Diff}_k(A,A)$ existe una conexión canónica: $D^{\nabla}F := D\circ F$, para todo $F\in\operatorname{Diff}_k(A,A)$ y $D\in\operatorname{Der}_k(A,A)$. Por tanto, existe una diferencial canónica $d\colon \operatorname{Diff}_k(A,A)\otimes\Omega^{\cdot}\to\operatorname{Diff}_k(A,A)\otimes\Omega^{\cdot}$. Observemos que $R = d^2 = 0$, porque $R(D_1,D_2) = D_1\circ D_2\circ -D_2\circ D_1\circ -[D_1,D_2]\circ = 0$.

50. Teorema de Takens: *La sucesión*

$$0\to\operatorname{Diff}_k(A,A)\overset{d}{\to}\operatorname{Diff}_k(A,A)\otimes_A\Omega\overset{d}{\to}\operatorname{Diff}_k(A,A)\otimes_A\Omega^2\overset{d}{\to}\cdots\overset{d}{\to}\operatorname{Diff}_k(A,A)\otimes_A\Omega^{n-1}\overset{d}{\to}\operatorname{Diff}_k(A,A)\otimes_A\Omega^n$$

es exacta y $(\operatorname{Diff}_k(A,A)\otimes_A\Omega^n)/d(\operatorname{Diff}_k(A,A)\otimes_A\Omega^{n-1}) = \Omega^n$.

Demostración. El diagrama

$$\begin{array}{ccc}
\operatorname{Diff}_k^r(A,A)\otimes\Omega^{\cdot} & \xrightarrow{\mathrm{simb}_r\otimes\mathrm{Id}} & S^r\operatorname{Der}_k(A,A)\otimes\Omega^{\cdot} \\
\downarrow d & & \downarrow \mathrm{Id}^{\wedge} \\
\operatorname{Diff}_k^{r+1}(A,A)\otimes\Omega^{\cdot} & \xrightarrow{\mathrm{simb}_{r+1}\otimes\mathrm{Id}} & S^{r+1}\operatorname{Der}_k(A,A)\otimes\Omega^{\cdot}
\end{array}$$

es conmutativo: Denotemos los morfismos simb y simb$\otimes$Id con la notación de toma de clases. Dado $F\in\operatorname{Diff}_k^r(A,A)$, $\mathrm{Id}^{\wedge}(\bar F)(D) = (\mathrm{Id}\wedge\bar F)(D) = D\cdot\bar F = \overline{D\circ F} = \overline{dF(D)} = \overline{dF}(D)$, luego

$$\mathrm{Id}^{\wedge}(\overline{F\otimes\Omega_s}) = \mathrm{Id}^{\wedge}(\bar F\otimes\Omega_s) = \mathrm{Id}\wedge\bar F\wedge\Omega_s = \overline{dF}\wedge\Omega_s = \overline{dF\wedge\Omega_s} = \overline{dF\wedge\Omega_s + F\otimes d\Omega_s} = \overline{d(F\otimes\Omega_s)}$$

Sea $S\in\operatorname{Diff}_k(A,A)\otimes_A\Omega^m$ tal que $dS = 0$ y sea r mínimo tal que $S\in\operatorname{Diff}_k^r(A,A)\otimes_A\Omega^m$, entonces $\mathrm{Id}^{\wedge}(\bar S) = \overline{dS} = 0$. Si $(r,m)\neq(0,n)$, por el teorema 3.9.10, existe $S_{r-1}\in\operatorname{Diff}_k^{r-1}(A,A)\otimes_A\Omega^{m-1}$ tal que $\mathrm{Id}^{\wedge}(\bar S_{r-1}) = \bar S$. Por tanto, $S - dS_{r-1}\in\operatorname{Diff}_k^{r-1}(A,A)\otimes_A\Omega^m$, 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 $S_0\in\operatorname{Diff}_k^0(A,A)\otimes_A\Omega^n$.

Obviamente, $(\operatorname{Diff}_k^0(A,A)\otimes_A\Omega^n)\subset\operatorname{Ker} d$.

Dado $0\neq\lambda\otimes\Omega_n\in\operatorname{Diff}_k^0(A,A)\otimes_A\Omega^n$ supongamos que $\lambda\otimes\Omega_n\in\operatorname{Im} d$. Sea r mínimo para el que existe $S\in\operatorname{Diff}_k^r(A,A)\otimes_A\Omega^{n-1}$ de modo que $dS = \lambda\otimes\Omega_n\in\operatorname{Diff}_k^{r+1}(A,A)\otimes_A\Omega^n$. $\mathrm{Id}^{\wedge}\bar S = \overline{dS} = 0$, luego existe $S_{r-1}\in\operatorname{Diff}_k^{r-1}(A,A)\otimes_A\Omega^{n-2}$ tal que $\mathrm{Id}^{\wedge}(\bar S_{r-1}) = \bar S$. Por tanto, $S' = S - dS_{r-1}\in\operatorname{Diff}_k^{r-1}(A,A)\otimes_A\Omega^{n-1}$ y $dS' = dS$. Hemos llegado a contradicción.

Con todo hemos conluido.

□

51. Consideremos $\mathrm{Hom}_A(J^n_{A/k}, M)$ como A-módulo como sigue $(a\cdot f)(\overline{a_1\otimes a_2}) := f(\overline{a_1\otimes a_2 a})$ para cada $f\in \mathrm{Hom}_A(J^n_{A/k}, M)$ (es decir, $\mathrm{Diff}^n_k(A,M)$ lo consideramos A-módulo por la "derecha" $D\cdot a = D\circ a\cdot$). Entonces,

$$\mathrm{Diff}^n_k(N,M) = \mathrm{Hom}_A(J^n_{N/k}, M) = \mathrm{Hom}_A(N, \mathrm{Hom}_A(J^n_{A/k}, M)) = \mathrm{Hom}_A(N, \mathrm{Diff}^n_k(A,M))$$

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 $\tilde{D}(n)(a) := D(an)$

Dado el morfismo $\mathrm{Id}\colon J^n_{N/k}\to J^n_{N/k}$, tendremos que $j^n_N\colon N\to J^n_{N/k}$, $n\mapsto 1\otimes n$ es un operador diferencial de orden n y todo operador diferencial de orden n, $F\colon N\to N'$, es igual a la composición de j^n_N y un morfismo de A-módulos $f\colon J^n_{N/k}\to N'$.

La composición,

$$N \xrightarrow{j^r_N} J^r_{N/k} \xrightarrow{j^s_{J^r_{N/k}}} J^s_{J^r_{N/k}} = J^s_{A/k}\otimes_A J^r_{A/k}\otimes_A N$$

es un operador diferencial de orden $r+s$, luego tenemos un morfismo natural $J^{r+s}_{N/k}\to J^s_{A/k}\otimes_A J^r_{N/k}$, que dualmente es el morfismo natural $\mathrm{Diff}^s_k(N, \mathrm{Diff}^r_k(A,M))\to \mathrm{Diff}^{r+s}_k(N,M)$, $D\mapsto \tilde{D}$, $\tilde{D}(n) := D(n)(1)$.

3.10. Problemas

1. Probar que si A es un anillo íntegro entonces (0) es irreducible. Probar 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, probar 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 sólo si I es intersección de un número finito de ideales primos.

4. Probar 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 $\mathfrak{p}\subsetneq \mathfrak{m}$ un ideal primo tal que $\mathfrak{p}\not\subseteq \mathfrak{m}^2$. ¿Puede ser $\mathfrak{p}\cap\mathfrak{m}^2$ un ideal primario?

6. Probar 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 $r(I) = \mathfrak{m}$. Probar que $\mathfrak{m}^r\subseteq I$ precisamente cuando $\overline{\mathfrak{m}^r}\subseteq \bar{I}$ en $\mathcal{O}/\mathfrak{m}^{r+1}$.

8. Calcular la descomposición primaria de $I = (xy, -y+x^2+y^2)$ en $\mathbb{C}[x,y]$.

9. Calcular 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. Hallar 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. Calcular 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, calcular $\dim_{\mathbb{C}}(\mathbb{C}[x,y]/(y^2 - x^2 - y^3, y^3 + x^2))_x$, donde x es el origen.

12. Definir el grupo multiplicativo G_m de los elementos no nulos de un cuerpo 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 para el grupo aditivo G_a de los elementos de k con la operación de la suma de k.

13. Sea $\mu_6 = \operatorname{Spec} k[x]/(x^6 - 1)$ el grupo de las raíces sextas de la unidad sobre un cuerpo k. Determinar si es una variedad íntegra o reducida, y calcular el número de componentes irreducibles cuando $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$.

    Definir 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. Definir el concepto de morfismo de grupos $\mu_6 \to \mu_6$ y del núcleo del mismo. Probar entonces que $\psi\colon \mu_6 \to \mu_6, \alpha \mapsto \alpha^2$, es morfismo de grupos y calcular el núcleo.

14. 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, probar que coinciden en X.

15. Poner un ejemplo de variedad algebraica que sea la unión de dos componentes no disjuntas, una de dimensión 2, la otra de dimensión 1.

16. 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 $k(x_1, \ldots, x_n)$ con coeficientes en k.

    a) Sea C la cúbica plana $y^2 = x^2 + x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcular 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 $\mathbb{A}^1 \to C$, $x = t^2$, $y = t^3$.

17. 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 $K = k(\xi)$". Demostrar que toda variedad algebraica íntegra, sobre $\mathbb{C}$, es birracionalmente isomorfa a una hipersuperficie de un espacio afín.

18. Sea $k \hookrightarrow K$ una extensión finita de cuerpos y $X = \operatorname{Spec} A$ una k-variedad algebraica. Probar 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.

19. Sea A un anillo íntegro y $a \in A$ no invertible, ni nula. Probar que el morfismo de localización $A \to A_a$ no es finito.

20. Sean $p(x,y)$ y $q(x,y)$ dos polinomios de $k[x,y]$ sin factores comunes. Demostrar que la k-álgebra $k[x,y]/(p(x,y), q(x,y))$ es una k-álgebra finita.

21. Sea $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ un ideal maximal. Probar que $\mathfrak{m}$ está generado por n funciones. ¿Puede estar generado por $n - 1$ funciones?

22. 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). Probar que el número de puntos (contando multiplicidades) de las fibras de π es constante.

23. Calcular los ideales maximales de $\mathbb{C}[x_1,\dots,x_n]$. Calcular los ideales maximales de $\mathbb{C}[x_1,x_2,x_3]/(x_1^2+x_2^2+x_3^2-1)$.

24. 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 $\mathfrak{p}_y=(px_0-x_1)\subset A[x_0,x_1]$. Probar que y no es un punto cerrado de $\mathbb{P}^1_A$, pero que si es un punto cerrado en $\mathbb{P}^1_A\setminus(x_1)_0$.

25. Probar que si X e Y son variedades algebraicas íntegras sobre un cuerpo k algebraicamente cerrado, entonces $X\times_k Y$ es íntegra. (Indicación: Supongamos que $f(x,y)\cdot g(x,y)=0$ y $f\neq 0$. 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, $g=0$.)

26. Sea $X=\operatorname{Spec}A$ una variedad íntegra sobre un cuerpo k algebraicamente cerrado. Probar 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).

27. Probar que el morfismo $k[x]\hookrightarrow k[x,y]/(p(x,y))$ es finito si y sólo si la curva $p(x,y)=0$ no tiene asíntotas verticales.

28. Calcular las asíntotas imaginarias de la circunferencia $x^2+y^2=1$.

29. Probar 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.

30. Probar 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.

31. Probar 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.

32. Probar que el conjunto de curvas de grado n de $\mathbb{P}^2$ se corresponden con los puntos racionales de un espacio proyectivo.

33. Probar 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.

34. 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. Probar que en general las curvas planas afines de grado n son irreducibles.

35. Demostrar que en general las matrices cuadradas son invertibles. Sean A y B dos matrices cuadradas de orden n, probar que el polinomio característico de $A\cdot B$ es igual al de $B\cdot A$.

36. Demostrar que $R_0[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]\simeq R_0[\xi_0,\dots,\xi_n]/(\xi_i-1)$ y que por tanto, $U^h_{\xi_i}\simeq(\xi_i-1)_0$. Probar que $U^h_{\xi_i}\times(\mathbb{A}^1\setminus\{0\})=U_{\xi_i}$. Dar una interpretación geométrica de estos resultados.

37. Demostrar que el conjunto de puntos cerrados de $\mathbb{P}^n(\mathbb{C})=\operatorname{Proj}\mathbb{C}[x_0,\dots,x_{n+1}]$ es biyectivo con el conjunto $\mathbb{C}^{n+1}\setminus\{0\}/\sim$, donde $(\alpha_0,\dots,\alpha_n)\sim(\alpha'_0,\dots,\alpha'_{n+1})$ si $(\alpha'_0,\dots,\alpha'_n)=\lambda(\alpha_0,\dots,\alpha_{n+1})$.

38. *a*) Escribir 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) Demostrar 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) Definir 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"?

39. Si X e Y son dos subvariedades proyectivas de $\mathbb{P}^n$, y $\operatorname{codim}X+\operatorname{codim}Y\leq n$, probar que $X\cap Y\neq\emptyset$ y que se cumple que

$$\operatorname{codim}X+\operatorname{codim}Y\geq\operatorname{codim}X\cap Y$$

40. Sea $f \in k[\xi_0,\ldots,\xi_n]$ una función homogénea que se anula en algún punto de $X = \operatorname{Proj} k[\xi_0,\ldots,\xi_n]$. Demostrar que
$$\dim(f)_0^h \geq \dim X - 1$$

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 sólo 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 sólo 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 $\mathcal{O}$ considerando el espacio tangente a Spec$\mathcal{O}$ 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 equivalente a $y^2 - x^2 = 0$. Así pues, 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 $X \subset \mathbb{A}_n$, 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

$$T_xX := \operatorname{Proj} G_{\mathfrak{m}}A$$

En general, dado un cerrado $Y = (I)_0 \subset X = \operatorname{Spec}A$, llamaremos cono normal de X a lo largo de Y, que denotamos $C_{X/Y}$, a $C_{X/Y} := \operatorname{Spec}G_IA$; y espacio normal a Y en X, que denotamos $N_{X/Y}$, a $N_{X/Y} := \operatorname{Proj}G_IA$.

4. Ejemplo: El cono tangente de un espacio afín en el origen es isomorfo al espacio afín. Es decir, si $A = k[x_1,\dots,x_n]$ y $\mathfrak{m} = (x_1,\dots,x_n)$, entonces $G_{\mathfrak{m}}A \simeq A$.

[1] Advertamos que debemos tomar todas las $f \in I$ y que no basta con tomar cualquier sistema generador.

5. Proposición: *Sea $I \subset A$ un ideal y $f \in I^r \setminus I^{r+1}$. 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 $(I^n \cap (I^{n+1} + (f))/I^{n+1} = (I^{n+1} + I^n \cap (f))/I^{n+1}$. Por 1., la sucesión

$$0 \to I^{n-r}/I^{n-r+1} \xrightarrow{f \cdot := f_r \cdot} I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1} \to 0$$

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 $\mathfrak{m}_{x_0} = (x,y)$. Demostrar que $G_{\mathfrak{m}_{x_0}}\mathcal{O} = k[x,y]/(p_n(x,y))$.

7. Ejercicio: Probar que el espacio tangente de la intersección de dos hipersuperficies transversales es la intersección de los espacios tangentes. Es decir, considérese el espacio afín $\mathbb{A}_3 = \operatorname{Spec} k[x_1,x_2,x_3]$ 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 $G_{\mathfrak{m}}(k[x_1,x_2,x_3]/(f_1)) = k[x_1,x_2,x_3]/(f_{1,n})$). Probar 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 $M = \oplus M_n$ 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 verifica*

$$S_A(n) = l(R_0) \cdot \binom{n+r-1}{r}$$

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 $\Delta S_A(n) = S_{\bar{A}}(n+1) = l(R_0) \cdot \binom{n+r-1}{r-1}$, 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 $A=R_0[\xi_1,\dots,\xi_r]$.

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 $A=R_0[\xi_1,\dots,\xi_{r-1}]$ 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 $R_0[\xi_1,\dots,\xi_{r-1}]$-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, $M_{n+h}=I^nM_h\subseteq I^nM\subseteq M'_n$ y $M'_{n+h}=I^nM'_h\subseteq I^nM\subseteq M_n$. □

17. Definición: Sea I un ideal de A. Llamaremos dilatado de A por I a

$$D_IA=A\oplus I\oplus I^2\oplus\dots$$

En general, dado un A-módulo M y una I-filtración $\{M_n\}$, llamaremos dilatado de M por la I-filtración a $DM=M\oplus M_1\oplus M_2\oplus\dots$.

Observemos que D_IA es un anillo graduado y que DM es un D_IA-módulo graduado. Si A es noetheriano, entonces $I=(\xi_1,\dots,\xi_r)$ es finito generado. El morfismo

$$\begin{array}{ccc} A[x_1,\dots,x_r] & \to & D_IA=A\oplus I\oplus\dots\oplus I^n\oplus\dots \\ x_i & \mapsto & \xi_i \end{array}$$

es epiyectivo, luego D_IA 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_IA-módulo finito generado.*

Demostración. Observemos que el D_IA-submódulo de DM generado por $M \oplus M_1 \oplus \cdots \oplus M_h$ es igual

$$M \oplus M_1 \oplus \cdots \oplus M_h \oplus IM_h \oplus I^2M_h \oplus \cdots$$

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_IA-módulo, luego es un D_IA-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,

$$DM =< n_1, \ldots, n_s >= D_IA \cdot (M \oplus M_1 \oplus \cdots \oplus M_h)$$

luego $M_{n+h} = I^nM_h$ 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 $\{M' \cap I^nM\}$ es I-estable.*

Demostración. Consideremos en M la filtración I-ádica y en M' la I-filtración $\{M' \cap I^nM\}$. DM' es un D_IA-submódulo de DM. D_IA es noetheriano y, por el lema anterior, DM es finito generado. Por tanto, DM' es finito generado, luego por el lema anterior $\{M' \cap I^nM\}$ es I-estable.

□

20. Corolario (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, $\bigcap_{n\in\mathbb{N}} I^nM = 0$.*

Demostración. Sea $N = \bigcap_{n\in\mathbb{N}} I^nM$. Por Artin-Rees, la filtración $\{N \cap I^nM = N\}$ 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 $\mathcal{O}$ es un anillo local noetheriano de ideal maximal $\mathfrak{m}$, I un ideal $\mathfrak{m}$-primario (es decir, $\mathrm{Spec}\mathcal{O}/I = (I)_0 = \{\mathfrak{m}\}$) y M un $\mathcal{O}$-módulo finito generado.

$\mathcal{O}/I$ es de longitud finita, por 0.3.51. Escribamos $I = (\xi_1, \ldots, \xi_r)$. El graduado de $\mathcal{O}$ por I es $G_I\mathcal{O} = \mathcal{O}/I[\bar{\xi}_1, \ldots, \bar{\xi}_r]$, que es un anillo graduado con $\mathcal{O}/I$ 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 $D_I\mathcal{O}$-módulo finito generado. Por tanto, el graduado de M por la filtración, GM, es un $D_I\mathcal{O}$-módulo finito generado, luego es un $G_I\mathcal{O}$-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 $\{I^nM\}$ y $\{\mathfrak{m}^nM\}$. Por el teorema anterior, basta probar que $S_{M,I}(n) = l(M/I^nM)$ y $S_{M,\mathfrak{m}}(n) = l(M/\mathfrak{m}^nM)$ tienen el mismo grado. Existe un k, tal que $\mathfrak{m}^k \subseteq I$. Por tanto,

$$S_{M,\mathfrak{m}}(kn) = l(M/\mathfrak{m}^{kn}M) \geq l(M/I^nM) = S_{M,I}(n)$$
$$S_{M,I}(n) = l(M/I^nM) \geq l(M/\mathfrak{m}^nM) = S_{M,\mathfrak{m}}(n)$$

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 $a \in \mathcal{O}$ 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 $\mathcal{O}$ ≥ 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

$$\dim \mathcal{O} \geq \text{ número mínimo de parámetros}$$

b) Número mínimo de parámetros de los sistemas de parámetros de $\mathcal{O}$ ≥ grado del polinomio de Samuel de $\mathcal{O}$:

Sea $(f_1, \ldots, f_r) = I$ un sistema de parámetros. Sea $A = (\mathcal{O}/I)[x_1, \ldots, x_r]$, $J = (x_1, \ldots, x_r)$. El morfismo

$$A \longrightarrow G_I\mathcal{O}$$
$$x_i \longmapsto \bar{f}_i \in I/I^2$$

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. Se verifica*

$$\dim \mathcal{O}/(f) \geq \dim \mathcal{O} - 1$$

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 sólo 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 sólo 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 sólo si existe un sistema de n parámetros $f_1,\dots,f_n$ que generan el ideal maximal.*

Demostración. Si $\mathcal{O}$ es un anillo regular entonces $n = \dim\mathcal{O} = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. 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 $\dim\mathcal{O} = n \geq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathcal{O}$ 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 sólo 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 $\mathcal{O}/\mathfrak{m}$-módulos $\mathfrak{m}/\mathfrak{m}^2 \hookrightarrow G_{\mathfrak{m}}\mathcal{O}$ induce el epimorfismo graduado de anillos graduados $S^{\cdot}_{\mathcal{O}/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2 \to G_{\mathfrak{m}}\mathcal{O}$, $\bar{f}_1\cdots\bar{f}_n \mapsto \overline{f_1\cdots f_n}$.

5. Teorema: *$\mathcal{O}$ es regular si y sólo si $G_{\mathfrak{m}}\mathcal{O} = S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. Es decir, $\mathcal{O}$ es regular si y sólo si el cono tangente en el punto cerrado es un espacio afín.*

Demostración. En primer lugar, obsérvese que el polinomio de Samuel de $\mathcal{O}$ coincide con el polinomio de Samuel de $G_{\mathfrak{m}}\mathcal{O}$ respecto del ideal irrelevante.

Si $\mathcal{O}$ es un anillo regular de dimensión r, entonces $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = r$ y $S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \simeq \mathcal{O}/\mathfrak{m}[x_1,\dots,x_r]$. El epimorfismo

$$\begin{array}{rl} S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) & \xrightarrow{\pi} G_{\mathfrak{m}}\mathcal{O} \\ \bar{f}_1\cdots\bar{f}_i & \longmapsto \overline{f_1\cdots f_i} \end{array}$$

es además es inyectivo: porque si $\operatorname{Ker}\pi \neq 0$,

$$r = \operatorname{gr} S_{G_{\mathfrak{m}}\mathcal{O}}(n) = \operatorname{gr} S_{S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)/\operatorname{Ker}\pi}(n) \underset{4.2.23}{\leq} \operatorname{gr} S_{S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)}(n) \underset{4.3.4}{=} r$$

Recíprocamente, si $G_{\mathfrak{m}}\mathcal{O} = S^{\cdot}_{\mathcal{O}/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$, entonces por 4.3.4, el polinomio de Samuel de $\mathcal{O}$ tiene grado $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathcal{O}$ es regular. □

6. Corolario: *Sea $\mathcal{O}$ un anillo local noetheriano. Entonces, $\mathcal{O}$ es un anillo regular de dimensión r si y sólo si $S_{\mathcal{O}}(n) = \binom{n+r-1}{r}$.*

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. □

Sea x el punto cerrado de $\mathrm{Spec}\mathscr{O}$. 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 $\mathscr{O}$ sea una k-álgebra y $\mathscr{O}/\mathfrak{m}_x = k$, estas definiciones coinciden con las del capítulo 3.

9. Teorema: *Sea $\mathscr{O}$ un anillo local regular de ideal maximal $\mathfrak{m}_x$ y sea $I \subset \mathscr{O}$ un ideal. Entonces $\mathscr{O}/I$ 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 $\mathscr{O}/I$.

$\Leftarrow$) 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,

$$\dim_{\mathscr{O}/\mathfrak{m}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim_{\mathscr{O}/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 - r = \dim \mathscr{O} - r \leq \dim \mathscr{O}/I$$

luego $\mathscr{O}/I$ es regular (y de dimensión $\dim \mathscr{O} - r$).

$\Rightarrow$) Supongamos que $\mathscr{O}/I$ es regular. Escribamos $\dim \mathscr{O} = n$ y $\dim \mathscr{O}/I = n - r$. 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 $\mathscr{O}/(f_1, \dots, f_r) \to \mathscr{O}/I$, que es isomorfismo: en efecto, por la implicación anterior, $\mathscr{O}/(f_1, \dots, f_r)$ es regular y de dimensión $n - r$; si hubiese núcleo, la dimensión de $\mathscr{O}/I$ sería menor que $n - r$, por 4.2.29, ya que $\mathscr{O}/(f_1, \dots, f_r)$ 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. □

10. Corolario: *Sea $\mathscr{O}$ 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 $\mathscr{O}/I$ es $n - r$. Entonces $\mathscr{O}/I$ es regular $\Leftrightarrow$ $d_x f_1, \dots, d_x f_r$ son linealmente independientes.*

Demostración. $\Leftarrow$) Es consecuencia inmediata del Teorema 4.3.9.

$\Rightarrow$) $I/\mathfrak{m}_x I = (\bar{f}_1, \dots, \bar{f}_r)$, luego $\dim_{\mathscr{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I \leq r$. De la sucesión exacta

$$I/\mathfrak{m}_x I \xrightarrow{i} \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

$\dim_{\mathscr{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I \geq \dim_{\mathscr{O}/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 - \dim_{\mathscr{O}/\mathfrak{m}} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = r$. Luego, $\dim_{\mathscr{O}/\mathfrak{m}_x} I/\mathfrak{m}_x I = r$ e i es inyectivo. Por tanto, $d_x f_1, \dots, d_x f_r$ son linealmente independientes.

□

11. Definición: Sea A un anillo noetheriano y $X = \mathrm{Spec} A$. 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.

12. Ejercicio: Sea $X = \mathrm{Spec} k[x_1, \dots, x_n]/(p(x_1, \dots, x_n))$. Demostrar que X es regular en un punto $\alpha = (\alpha_1, \dots, \alpha_n)$ si y sólo si $\sum_i \frac{\partial p}{\partial x_i}(\alpha) d_\alpha x_i \neq 0$

13. Teorema: *Sea $x \in \mathrm{Spec} A$ 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 sólo si es lisa.*

Demostración. $\Rightarrow$) Sea Σ el cuerpo de fracciones de A. Como A_x es regular $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x = \mathrm{gr\,tr}\, \Sigma = n$. 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

$$0 \to \mathrm{Ker}\, \phi \to A_x \oplus \overset{n}{\cdots} \oplus A_x \xrightarrow{\phi} \Omega_{A_x/k} \to 0$$
$$(0, \dots, \underset{i}{1}, \dots, 0) \longmapsto \omega_i$$

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 3.7.35, $\dim_\Sigma \Omega_{\Sigma/k} = \operatorname{grtr}\Sigma = n$. 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 4.4.25 veremos que las variedades lisas son regulares. Una k-variedad es lisa si y sólo 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.

14. Ejercicio: Sea $k = \mathbb{Z}/3\mathbb{Z}(t)$ y $A = \operatorname{Spec} k[x,y]/(y^2 + x^3 - t)$. Demostrar 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,

$$\widehat{M} = \{\sum_{i=0}^{\infty} m_i,\ m_i \in M_i\}/\{\text{Series convergentes a cero}\}$$

Si consideramos 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

$$\hat{f}: \widehat{M} \to \widehat{N}$$

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*

$$0 \to \widehat{M'} \to \widehat{M} \xrightarrow{\hat{\pi}} \widehat{M''} \to 0$$

es exacta. "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

$$0 \to \widehat{M'} \to \widehat{M} \xrightarrow{\hat{\pi}} \widehat{M''}$$

Sólo nos falta ver la epiyectividad de $\hat{\pi}$: 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 $\hat{\pi}(\sum_{i=0}^{\infty} m_i) = \sum_{i=0}^{\infty} m_i''$, 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 $\widehat{M}_n \hookrightarrow \widehat{M}$ 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. Completando la sucesión exacta $0 \to M_n/M_{n+1} \to M/M_{n+1} \to M/M_n \to 0$, y por el corolario 4.4.7, se concluye 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 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. $\varprojlim_{n\in\mathbb{N}} \mathscr{C}^\infty(\mathbb{R})/\mathfrak{m}_\alpha^n = \mathbb{R}[[x-\alpha]] = \mathbb{R}[[x]]$, donde el $\mathfrak{m}_\alpha$ es el ideal de funciones diferenciables que se anulan en α. El morfismo natural $\mathscr{C}^\infty(\mathbb{R}) \to \varprojlim_{n\in\mathbb{N}} \mathscr{C}^\infty(\mathbb{R})/\mathfrak{m}_\alpha^n = \mathbb{R}[[x]]$ asigna a cada función su desarrollo de Taylor en α.
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.

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 $\{\widehat{I^nM}\}$ es justamente la I-ádica de $\widehat{M}$, cuando I es un ideal finito generado. La igualdad $\widehat{I^n}\widehat{M} = I^n\widehat{M}$ puede interpretarse intuitivamente como la igualdad: $\sum_{i\ge n} a_i x^i = x^n \cdot \sum_{i\ge 0} a_{n+i} x^i$. Con precisión:

12. Proposición: *Si I es un ideal finito generado (por ejemplo, si A es un anillo noetheriano), entonces $\widehat{I^nM} = I^n\widehat{M}$. Además, $\widehat{M}$ es completo y separado con la topología I-ádica, $\widehat{M}/I^n\widehat{M} = M/I^nM$ y $G_I\widehat{M} = G_IM$.*

Demostración. Consideremos la inyección $I^nM \hookrightarrow M$. Completando tenemos la inyección $\widehat{I^nM} \hookrightarrow \widehat{M}$.

Sea $i_1, \ldots, i_r$ un sistema generador de I^n. Consideremos el epimorfismo

$$M \oplus \overset{r}{\ldots} \oplus M \to I^nM,\ (m_1, \ldots, m_r) \mapsto \sum_j i_j m_j.$$

Completando I-ádicamente tenemos un epimorfismo $\widehat{M} \oplus \overset{r}{\ldots} \oplus \widehat{M} \to \widehat{I^n M}$ y recordemos la inyección $\widehat{I^n}\widehat{M} \hookrightarrow \widehat{M}$. Hemos obtenido que $\widehat{I^n}\widehat{M} = I^n\widehat{M}$.

Todo lo demás es consecuencia de 4.4.7, 4.4.8 y 4.4.9.

□

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 $\{M' \cap I^n M\}$, M por la filtración $\{I^n M\}$ y M'' por la filtración $\{I^n M''\}$, entonces la sucesión completada es exacta. Ahora bien, por Artin-Rees la filtración $\{M' \cap I^n M\}$ 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. □

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 sólo si el morfismo inducido entre los graduados $G_{\mathfrak{m}_{f(x)}}C^\infty(Y) \to G_{\mathfrak{m}_x}C^\infty(X)$ 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.

16. Teorema formal de la función inversa: *Sean $\{M_n\}$ y $\{M'_n\}$ filtraciones de M y M' respectivamente. Supongamos que M y M' son completos y separados. Sea $f: M \to M'$ un morfismo compatible 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 $G(f)$ es epiyectivo. Sea $m' \in M'$. Como $M/M_1 \to M'/M'_1$ es epiyectivo, existe $m_0 \in M$, tal que $m' = f(m_0) + m'_1$, con $m'_1 \in M'_1$. Como $M_1/M_2 \to M'_1/M'_2$ 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 $m_i \in M_i$, de modo que la serie $f(m) = f(\sum_{i=0}^{\infty} m_i) = \sum_{i=0}^{\infty} f(m_i)$ converge a m'. Como M' es completo, $f(m) = m'$ y f es epiyectivo.

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.

□

17. 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. Escribamos cada uno de ellos como suma de sus componentes homogéneas. Sea $\bar{x} \in \mathfrak{q}_n/\mathfrak{q}_{n+1}$ una de esas componentes y $x \in \mathfrak{q}_n$ un representante de la clase de $\bar{x}$. Consideremos en A la siguiente filtración: $A_0 = A, \ldots, A_n = A, A_{n+1} = I, A_{n+2} = I^2, \ldots$. El morfismo $A \to \mathfrak{q}$ dado por $1 \mapsto x$ es compatible con las filtraciones. Haciendo lo mismo con todas las componentes homogéneas del sistema de 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 $i: \mathfrak{q} \hookrightarrow \widehat{\mathfrak{q}}$ 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. □

18. Teorema: *Si A es noetheriano entonces $\widehat{A}$ es noetheriano.*

Demostración. Si A es noetheriano e $I \subset A$ es un ideal, entonces $I = (\xi_1, \ldots, \xi_r)$ es finito generado. El morfismo

$$\begin{aligned} (A/I)[x_1, \ldots, x_r] &\longrightarrow G_I A \\ x_i &\longmapsto \bar{\xi}_i \in I/I^2 \end{aligned}$$

es epiyectivo, luego $G_I A$ es noetheriano.

Por 4.4.12, $G_I \widehat{A} = G_I A$. Por el lema anterior, $\widehat{A}$ es noetheriano. □

19. Proposición: *Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Sea $\widehat{\mathcal{O}}$ la compleción $\mathfrak{m}$-ádica de $\mathcal{O}$. Entonces,*

$$\dim \mathcal{O} = \dim \widehat{\mathcal{O}}$$

Demostración. $\mathcal{O}/\mathfrak{m}^n = \widehat{\mathcal{O}}/\widehat{\mathfrak{m}}^n$, luego $S_{\mathcal{O}}(n) = S_{\widehat{\mathcal{O}}}(n)$ y $\dim \mathcal{O} = \dim \widehat{\mathcal{O}}$. □

20. Proposición: *Sea $\mathcal{O}$ un anillo local noetheriano de maximal $\mathfrak{m}$ y $\widehat{\mathcal{O}}$ el completado $\mathfrak{m}$-ádico de $\mathcal{O}$. Entonces, $\mathcal{O}$ es regular si y sólo si $\widehat{\mathcal{O}}$ es regular.*

Demostración. Se deduce de la igualdad $G_{\mathfrak{m}}\mathcal{O} = G_{\widehat{\mathfrak{m}}}\widehat{\mathcal{O}}$ y del teorema 4.3.5. □

21. 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.

22. 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 $\pi_n : \mathcal{O}/\mathfrak{m}^n \to \mathcal{O}/\mathfrak{m}^{n-1}$, 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 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 $p > 0$.

Sea L un subcuerpo máximo de $\pi_n^{-1}(K)$ que contenga a $(\pi_n^{-1}(K))^p := \{\lambda^p, \lambda \in \pi_n^{-1}(K)\}$. Observemos que $\pi_n^{-1}(K) = \pi_n^{-1}(K\setminus 0) \cup \pi_n^{-1}(0)$, donde los elementos de $\pi_n^{-1}(K\setminus 0)$ son invertibles porque no son nilpotentes, y $\pi_n^{-1}(0) = \mathfrak{m}^{n-1}/\mathfrak{m}^n$. Por tanto, $(\pi_n^{-1}(K))^p = \pi_n^{-1}(K\setminus 0)^p \cup 0$ es un cuerpo y el epimorfismo $\pi_n : (\pi_n^{-1}(K))^p \to K^p$ es un isomorfismo.

Si probamos que $\pi_n : L \hookrightarrow K$ 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 $\pi_n(a) = \bar{a}$. Se verifica que $a^p \in L$. 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. □

23. 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, $\mathcal{O} \simeq \mathcal{O}/\mathfrak{m}[[\xi_1, \ldots, \xi_n]]$. □

24. 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). □

25. 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. □

4.4.4. Lema de Hensel

26. Teorema: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}_x$ y sea $\mathcal{O}'$ una $\mathcal{O}$-álgebra finita, completa y separada por la topología $\mathfrak{m}_x$-ádica. Entonces $\mathcal{O}'$ descompone en producto directo de $\mathcal{O}$-álgebras finitas, locales, completas y separadas.*

Demostración. $\mathcal{O}'/\mathfrak{m}_x\mathcal{O}'$ es una $\mathcal{O}/\mathfrak{m}_x$-álgebra finita. Consideremos el morfismo natural $f : \operatorname{Spec}\mathcal{O}' \to \operatorname{Spec}\mathcal{O}$ y sea $f^{-1}(x) = \operatorname{Spec}\mathcal{O}'/\mathfrak{m}_x\mathcal{O}' = \{y_1, \ldots, y_n\}$, que son los puntos cerrados de $\mathcal{O}'$. Obviamente, se cumple que $\operatorname{Spec}\mathcal{O}'/\mathfrak{m}_x^r\mathcal{O}' = \{y_1, \ldots, y_n\}$ y por tanto,

$$\mathcal{O}'/\mathfrak{m}_x^r\mathcal{O}' = (\mathcal{O}'/\mathfrak{m}_x^r\mathcal{O}')_{y_1} \times \cdots \times (\mathcal{O}'/\mathfrak{m}_x^r\mathcal{O}')_{y_n}$$

Además $\mathfrak{m}_{y_i}^{n_i}\mathcal{O}'_{y_i} \subseteq \mathfrak{m}_x\mathcal{O}'_{y_i}$, para ciertos $n_i \in \mathbb{N}$, pues $\mathfrak{m}_{y_i}$ es nilpotente en $(\mathcal{O}'/\mathfrak{m}_x\mathcal{O}')_{y_i}$. Completando por el ideal $\mathfrak{m}_x$ obtenemos que

$$\mathcal{O}' = \widehat{\mathcal{O}'_{y_1}} \times \cdots \times \widehat{\mathcal{O}'_{y_n}}$$

Esta igualdad muestra que $\widehat{\mathcal{O}'_{y_i}}$ son completos y separados por la topología $\mathfrak{m}_x$-ádica, y son locales de ideal maximal $\mathfrak{m}_{y_i}$. Por tanto, $\widehat{\mathcal{O}'_{y_i}} = \mathcal{O}'_{y_i}$ es completo y separado por la topología $\mathfrak{m}_{y_i}$-ádica. □

27. Definición: Un anillo $\mathcal{O}$ se dice henseliano si toda $\mathcal{O}$-álgebra finita descompone en producto directo de $\mathcal{O}$-álgebras locales.

Los anillos noetherianos locales y completos son henselianos, por el teorema anterior.

28. 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 $\bar{p}(x) \in (\mathcal{O}/\mathfrak{m})[x]$ descompone $\bar{p}(x) = f'(x) \cdot g'(x)$, 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 $\bar{\mathcal{O}}' = \bar{\mathcal{O}}'_1 \times \cdots \times \bar{\mathcal{O}}'_r = (\mathcal{O}/\mathfrak{m})[x]/(\bar{p}(x)) = (\mathcal{O}/\mathfrak{m})[x]/(f'(x)) \times \mathcal{O}/\mathfrak{m}[x]/(g'(x))$. 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. □

4.5. Problemas

1. Probar 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. Probar que $C_{X,x} = \operatorname{Spec} k[x,y,z]/(y+x, y-x) = \mathbb{A}_1$.

3. Calcular 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. Probar 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. Probar que $\dim A[x] = 1 + \dim A$ (Obsérvese que si $\mathfrak{p} \subset A$ es un ideal primo entonces $\mathfrak{p}A[x]$ es un ideal primo de $A[x]$).

6. Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull 2. Probar que el conjunto $\operatorname{Spec}\mathcal{O}$ tiene infinitos puntos.

7. Sea $A = k[x_1, x_2, \ldots, x_n, \ldots]$ un anillo de polinomios de infinitas variables. Sean

$$\mathfrak{p}_i = (x_{2^i}, \ldots, x_{2^{i+1}} - 1)$$

y $S = A \setminus \bigcup_i \mathfrak{p}_i$.

   a) Probar que $\operatorname{Spec}_{max} A_S = \{\mathfrak{p}_i \cdot A_S\}_i$.

   b) Probar que toda función no nula de A_S pertenece a un número finito de ideales maximales.

   c) Probar que A_S es un anillo noetheriano.

   d) Probar que $\dim A_S = \infty$. (Nagata)

8. Sea $A = k[\xi_1, \ldots, \xi_n]$ un anillo graduado, con $\operatorname{gr} \xi_i = 1$. Probar

   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. Probar que

$$C_{(x,y)}(X \times_k Y) = C_x X \times_k C_y Y$$

10. Calcular el polinomio de Samuel de un anillo local regular de dimensión 2.

11. Probar que la localización de $\mathbb{Z}[x]$ en cualquier punto es un anillo regular.

12. Calcular los puntos de $\mathbb{Z}[\sqrt[2]{5}]$ en los que no es regular.

13. Demostrar que todo ideal de $k[[x]]$ es de la forma (x^n).

14. Probar que los ideales de los enteros p-ádicos, $\hat{\mathbb{Z}}_p$, son de la forma (p^n). Expresar $(1-p)^{-1}$ como una serie en p. Probar que el 2 tiene raíz cuadrada en $\hat{\mathbb{Z}}_7$.

15. Sea $\hat{A}$ el completado I-ádico del anillo noetheriano A. Probar 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 $(\bar{x}, \bar{y})$. Probar que $\widehat{A} = k[[x,y]]/(y^2 - x^2 + x^3)$. Probar 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. Calcular 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 $p \in \mathbb{Z}$. Probar 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. Calcular el inverso de $1+x$ en $k[[x]]$. Probar que el único ideal maximal de $k[[x]]$ es (x). ¿Existe la raíz cuadrada de $1+x$ en $k[[x]]$?

21. Sea I un ideal de un anillo noetheriano A, probar que

$$\operatorname{Spec}_{\max} \hat{A} = \operatorname{Spec}_{\max}(A/I)$$

22. Probar que $\dim k[[x_1,\ldots,x_n]] = n$.

23. Sea $x \in \operatorname{Spec} A$ un punto cerrado. Probar

    a) El completado es un concepto local: El completado $\mathfrak{m}_x$-ádico de A coincide con el completado $\mathfrak{m}_x A_x$-ádico de A_x.

    b) El cono tangente es un concepto local: $G_{\mathfrak{m}_x} A = G_{\mathfrak{m}_x A_x} A_x$.

24. *a*) Demostrar que la compleción I-ádica de M coincide con la compleción I-ádica de M_{1+I}.

    b) Probar que $\operatorname{Spec}_{\max} A_{1+I} = \operatorname{Spec}_{\max} A/I$.

    c) Supongamos que A es un anillo noetheriano y M es finito generado. Probar que el núcleo del morfismo $M \to \hat{M}$ coincide con el núcleo del morfismo $M \to M_{1+I}$.

25. Sea A un anillo noetheriano íntegro, $I \subset A$ un ideal propio. Probar que A es separado con la topología I-ádica.

26. Sea A un anillo noetheriano. Probar $\bigcap_{x,n} \mathfrak{m}_x^n = 0$.

27. Sea A un anillo noetheriano y M un A-módulo finito generado. Probar que $M = 0$ si y sólo si sus compleciones en todo punto cerrado de $\operatorname{Spec} A$ son nulas.

28. Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$. Sea N un $\mathcal{O}$-módulo plano. Probar que la compleción $\mathfrak{m}$-ádica de N es isomorfa a la compleción de un $\mathcal{O}$-módulo libre.

Capítulo 5

Anillos de enteros y anillos de curvas

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 sólo 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. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión 1. $\mathcal{O}$ es regular si y sólo 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

MANUALES UEX

un parámetro, $\mathfrak{m} = (t)$. Dado un ideal I, sea n tal que $I \subset (t^n)$ pero $I \not\subset (t^{n+1})$. Existe $f \in I$ que es múltiplo de t^n pero no de t^{n+1}, luego $f = u \cdot t^n$ y u es invertible. Por tanto, $t^n \in I$ e $I = (t^n)$.

Recíprocamente, si $\mathfrak{m}$ es principal, entonces $\dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \leq 1$, luego $\dim \mathscr{O} \geq \dim_{\mathscr{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ y $\mathscr{O}$ es regular.

□

2. Definición: Sea Σ un cuerpo y $\Sigma^* = \Sigma \setminus \{0\}$. Una valoración discreta de Σ es una aplicación epiyectiva $v : \Sigma^* \to \mathbb{Z}$ 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 $v(0) = \infty$).

Sea $\mathscr{O}$ un anillo local y regular de ideal maximal $\mathfrak{m}$ y cuerpo de fracciones Σ. Para cada $f \in \mathscr{O}$ 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

$$\begin{aligned} v_{\mathfrak{m}} : \Sigma^* &\to \mathbb{Z} \\ f/g &\mapsto v_{\mathfrak{m}}(f/g) = v_{\mathfrak{m}}(f) - v_{\mathfrak{m}}(g) \end{aligned}$$

está bien definida y es una valoración discreta de Σ. Esta valoración se denomina valoración $\mathfrak{m}$-ádica.

Si además $\mathscr{O}$ es de dimensión 1, es inmediato ver que $\mathscr{O} = \{f \in \Sigma \mid v_{\mathfrak{m}}(f) \geq 0\}$. Veamos el recíproco.

3. Proposición: *Sea v una valoración discreta de un cuerpo Σ y denotemos $\mathscr{O}_v = \{f \in \Sigma : v(f) \geq 0\}$. Entonces $\mathscr{O}_v$ 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 $\mathscr{O}_v$.*

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 $I \subset \mathscr{O}_v$ 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, $g/f \in \mathscr{O}_v$ y $g = g/f \cdot f$, es decir, $I = (f)$.

Así pues, $\mathscr{O}_v$ es un anillo de ideales principales, luego noetheriano. $\mathscr{O}_v$ es un anillo local que no es un cuerpo, porque los invertibles son precisamente $\{f \in \mathscr{O}_v : v(f) = 0\}$ y el ideal maximal es $\mathfrak{p}_v := \{f \in \mathscr{O}_v : v(f) > 0\}$. Por tanto, $\mathscr{O}_v$ es un anillo local regular de dimensión 1. Además, para toda $f \in \Sigma$, o bien $f \in \mathscr{O}_v$ o bien $f^{-1} \in \mathscr{O}_v$ (pues $v(f) \geq 0$ ó $v(f^{-1}) = -v(f) \geq 0$). Por tanto, el cuerpo de fracciones de $\mathscr{O}_v$ es Σ. Para concluir, veamos que $v = v_{\mathfrak{m}}$. Sea t un parámetro que genere $\mathfrak{p}_v$. Si $f \in \mathscr{O}_v$, 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 $\mathscr{O}_v$ es un anillo de valoración discreta. Por la proposición anterior, un anillo es de valoración discreta si y sólo si es un anillo noetheriano, local y regular de dimensión 1.

5. Ejercicio: Sea $\mathscr{O}_v$ un anillo de valoración discreta y $f \in \mathscr{O}_v$. Probar que $v(f) = l(\mathscr{O}_v/(f))$.

6. Definición: Sea $\mathscr{V}$ un anillo íntegro y Σ su cuerpo de fracciones. Diremos que $\mathscr{V}$ es un anillo de valoración si para todo $f \in \Sigma$, se verifica que $f \in \mathscr{V}$ ó $f^{-1} \in \mathscr{V}$.

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 $\mathscr{V}$ un anillo de valoración e I_1, I_2 ideales de $\mathscr{V}$. Entonces, $I_1 \subseteq I_2$ o $I_2 \subseteq I_1$. En particular, $\mathscr{V}$ 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 $f_1/f_2 \in \mathscr{V}$, entonces $f_1 = (f_1/f_2) \cdot f_2 \in I_2$, contradicción. Análoga contradicción si $f_2/f_1 \in \mathscr{V}$. □

El ideal maximal de un anillo de valoración $\mathscr{V}$ se denota $\mathfrak{p}_{\mathscr{V}}$ y se le llama ideal de valoración.

8. Proposición: *Un anillo noetheriano $\mathscr{V}$ es de valoración (no trivial) si y sólo 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 $\bar{f} \geq g$, 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 verifica:

1. $v(fg) = v(f) + v(g)$ (¡ahora denotamos la operación de $\Sigma^*/\mathcal{V}^*$ aditivamente!).
2. $v(f+g) \geq \min\{v(f), v(g)\}$

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 totalmente ordenado y $v : \Sigma^* \to G$ es una epiyección verificando 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 G sea isomorfo a $\mathbb{Z}$. Denotaremos los anillos de valoración, por razones obvias, $\mathcal{O}_v$.

5.3. Anillos de Dedekind

1. 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.

□

2. 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 $f = -a_1 - a_2 f^{-1} - \cdots - f^{1-n} \in \mathcal{O}_v$. 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:

$$nv(f) = v(f^n) = v(-a_1 f^{n-1} - \ldots - a_n) \geq \min\{v(-a_1 f^{n-1}), \ldots, v(-a_n)\} \geq \min\{(n-1)v(f), \ldots, v(f), 0\},$$

de donde se deduce que $v(f) \geq 0$. □

Si consideramos el nodo $C \equiv y^2 - x^2 + x^3 = 0$, la curva $\tilde{C}$ que se obtiene de "despegar las dos ramas" y el morfismo natural $\tilde{C} \to C$ "pegar las dos ramas", resulta que este morfismo finito fuera del nodo es isomorfismo, luego es birracional. Parece claro intuitivamente que para las curvas regulares en todo punto, no existen más morfismos finitos birracionales que los isomorfismos. En términos matemáticos precisos:

3. Teorema: *Sea $\mathcal{O}$ un anillo íntegro local noetheriano de dimensión* 1. *Las siguientes condiciones son equivalentes:*

1. *$\mathcal{O}$ es regular.*
2. *$\mathcal{O}$ es un anillo de valoración.*
3. *$\mathcal{O}$ es íntegramente cerrado en su cuerpo de fracciones* Σ.

Demostración. 1. $\Rightarrow$ 2. Si $\mathcal{O}$ es regular entonces es un anillo de valoración discreta, por 5.2.3. Luego, $\mathcal{O}$ es un anillo de valoración.

2. $\Rightarrow$ 3. Es el lema anterior.

3. $\Rightarrow$ 1. 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 $\mathcal{O}$ un anillo regular. 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 $g \notin f\mathcal{O}$.

□

4. 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.

5. 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 sólo 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

$$f^n + a_1/s_1 \cdot f^{n-1} + \cdots + a_n/s_n = 0 \qquad \text{con} a_i, s_i \in A \text{ y } s_i(x) \neq 0$$

Sea $s = s_1 \cdots s_n$ (luego $s \in S$). Multiplicando la relación anterior por s^n obtenemos una relación entera de sf con coeficientes en A, luego $sf \in \bar{A}$ y $f \in (\bar{A})_S$. Luego, $(\bar{A})_S = \overline{A_S}$.

Sea A localmente íntegramente cerrado. Sea $f \in A_{A\setminus\{0\}}$ entero sobre A. El morfismo $A \to A[f]$ es localmente isomorfismo. Por tanto, $A = A[f]$ y $f \in A$, es decir, A es íntegramente cerrado.

□

6. Proposición: *Sea A un anillo íntegro, que no sea un cuerpo. A es un dominio de Dedekind si y sólo si A_x es un dominio de ideales principales para todo punto cerrado $x \in \operatorname{Spec} A$.*

7. Definición: Diremos que un punto cerrado $x \in \operatorname{Spec} A$ es no singular si A_x es un anillo regular. Diremos que es singular si A_x no es regular.

8. Ejemplo: $\operatorname{Spec} k[x,y]/(y^2 - x^3)$ tiene un único punto singular: el origen.

9. Ejemplo: Sea $\xi_m = e^{2\pi i/m} \in \mathbb{C}$ una raíz primitiva m-ésima de la unidad. Veamos que $\mathbb{Z}[\xi_m]$ es de Dedekind. 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.

10. Proposición: *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 el teorema y lema anteriores 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

$$\mathfrak{p}_{x_1}^{n_1} \cdot \cdots \cdot \mathfrak{p}_{x_m}^{n_m}$$

es igual localmente a I, luego son iguales globalmente. Los exponentes n_i están determinados porque lo están al localizar. □

11. 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 ($x, y \neq 0$) hizo la descomposición*

$$x^n = z^n - y^n = (z - \xi^1 y) \cdots (z - \xi^n y),$$

siendo ξ una raíz primitiva n-ésima de la unidad 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) de enteros $\mathbb{Z}[\xi]$. 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 de enteros eran dominios de factorización única. Consideremos por sencillez el anillo $\mathbb{Z}[\sqrt{-5}]$, 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 $(a_1, \ldots, a_n) = (m.c.d.(a_1, \ldots, a_n))$, 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.

Conviene que el lector lea la definición 0.3.61.

12. 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,

$$\text{Nº de puntos contando mult. y grd. de } f^{-1}(x) = \dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x = \sum_{y \in f^{-1}(x)} l_{A_x}(B_x/\mathfrak{p}_x B_x)_y$$

$$= \sum_{y \in f^{-1}(x)} l_{B_y}(B_y/\mathfrak{p}_x B_y) \cdot \operatorname{gr}_x y = \sum_{y \in f^{-1}(x)} m_y \cdot \operatorname{gr}_x y$$

13. 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 constante.*

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 $B_{B\setminus\{0\}} = \Sigma_B$. 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,

$$n = \dim_{A/\mathfrak{m}_x}(A_x^n/\mathfrak{m}_x A_x^n) = \dim_{A/\mathfrak{m}_x}(B_x/\mathfrak{m}_x B_x)$$

□

14. 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 $l(B_y/\mathfrak{m}_x B_y) > 1$ y en este caso se dice que y es un punto de ramificación de π y que x es un punto rama de π.

15. 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.

16. 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.

□

5.4. Desingularización

5.4.1. Finitud del morfismo de cierre entero

1. Lema: *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 5.3.5, 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 $\lambda_i \in A$.

□

2. 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 de números enteros si el morfismo $\mathbb{Z} \hookrightarrow A$ es inyectivo y finito.

3. Ejemplos: $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$ y $\mathbb{Z}[\sqrt{-5}, \sqrt[7]{3}]$ son anillos de números enteros.

4. 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 números 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 $S := \mathbb{Z}\setminus 0$, 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 el lema anterior, $\bar{A}$ es una $\mathbb{Z}$-álgebra finita, luego es un anillo de números enteros, de cuerpo de fracciones $\bar{\Sigma}$. En particular, $A \to \bar{A}$ es un morfismo finito. □

5. Definición: Dado un cuerpo de números K, diremos que el cierre entero de $\mathbb{Z}$ en K es el anillo de enteros de K.

6. 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 $k[x_1,\dots,x_n] \hookrightarrow A$ finito e inyectivo. El cierre entero de A en $\bar{\Sigma}$ coincide con el cierre entero de $k[x_1,\dots,x_n]$ en $\bar{\Sigma}$, luego podemos suponer que $A = k[x_1,\dots,x_n]$.

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 $\bar{\Sigma}^G = \Sigma[\xi_1,\dots,\xi_r]$. Existe $m >> 0$ de modo que $\xi_i^{p^m} \in \Sigma = k(x_1,\dots,x_n)$, para todo i. Escribamos $\xi_i^{p^m} = p_i/q_i$, con $p_i = \sum_j \lambda_{ij} x^j \in k[x_1,\dots,x_n]$ y $q_i = \sum_j \mu_{ij} x^j \in k[x_1,\dots,x_n]$. Sea $k' := k(\sqrt[p^m]{\lambda_{ij}}, \sqrt[p^m]{\mu_{ij}})_{ij}$ y $\Sigma' := k'(\sqrt[p^m]{x_1},\dots,\sqrt[p^m]{x_n})$. 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 $k[x_1,\dots,x_n]$ en Σ' es $k'[\sqrt[p^m]{x_1},\dots,\sqrt[p^m]{x_n}]$, pues $k'[\sqrt[p^m]{x_1},\dots,\sqrt[p^m]{x_n}]$ es un $k[x_1,\dots,x_n]$-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.

□

7. Definición: Diremos que $\operatorname{Spec} A$ es una curva íntegra afín si A es una k-álgebra de tipo finito íntegra y de dimensión 1.

8. Ejemplos: La recta afín $\mathbb{A}^1 = \operatorname{Spec} k[x]$, la circunferencia $S^1 = \operatorname{Spec} k[x,y]/(x^2+y^2-1)$, el nodo $\operatorname{Spec} k[x,y]/(y^2-x^2+x^3)$, la cúspide $\operatorname{Spec} k[x,y]/(y^2-x^3)$ son curvas íntegras afines.

9. Teorema: *Sea A el anillo de una curva afín íntegra (resp. un anillo de números 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 números 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 sólo 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 5.4.4 y 5.4.6.

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 5.3.5).

□

5.4.2. Cierre entero y anillos de valoración

10. 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 $\mathcal{O}$.

11. Lema: *Sea A un anillo íntegro incluido en un cuerpo Σ. Se cumple que $\xi \in \Sigma$ es entero sobre A si y sólo si $\xi \in A[\xi^{-1}]$.*

Demostración. Si ξ es entero sobre A, entonces existe una relación entera

$$\xi^n + \cdots + a_1\xi + a_0 = 0, \qquad \text{con } a_i \in A$$

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. □

12. Lema: *Sea $\mathcal{O}$ un anillo local íntegro incluido en un cuerpo Σ y sea $\xi \in \Sigma$. Entonces, un localizado (en 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 (3.3.14). 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. □

13. Proposición: *Sea $\mathcal{O}$ un anillo local íntegro incluido en el cuerpo Σ. $\mathcal{O}$ es un anillo de valoración de Σ si y sólo 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 5.4.12, ξ o ξ^{-1} pertenecen a $\mathcal{O}$, luego es de valoración.

□

14. 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 maximalidad $\mathcal{O}'$ no es dominado por ningún subanillo local de Σ, luego es un anillo de valoración de Σ por la proposición 5.4.13.

□

15. 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 5.4.11. 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 $\xi \notin \mathcal{O}_v$.

□

16. 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 $l_A(A/aA) = l_A(B/aB)$.

□

17. 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 para algún i, $l_A(A_i/aA_i) > l_A(A/aA)$. 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 5.4.16, $l_A(A_i/aA_i) = l_A(A/aA)$. En conclusión, $l_A(\bar{A}/a\bar{A}) \leq l_A(A/aA)$.

□

18. 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 obtenemos el siguiente teorema.

19. 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.*

20. 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".

21. Definición: Diremos que un ideal primo $\mathfrak{p}_x \subset A$ es de altura r si $\dim A_x = r$.

22. 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 $\frac{b}{a}\cdot\mathfrak{m}\subset A$. 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. Si $\frac{b}{a}\cdot\mathfrak{m}=A$, entonces $\mathfrak{m}$ 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 sólo si si $m_i\geq n_i$, para todo i, que equivale a $\frac{b}{a}\in\bigcap_{\text{alt.}\mathfrak{p}_x=1}A_x$. □

23. Corolario : *Sea A un anillo noetheriano íntegro. A es un anillo normal si y sólo 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 sólo 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 $f\in A$. □

24. 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

$$\begin{array}{ccccc} A' & \longrightarrow & A'[\xi] & \longrightarrow & A'[\xi]/\xi A'[\xi] & = & A'/(\xi A'[\xi]\cap A') \\ & \searrow^{f'} & & & & & \downarrow \\ & & & & & & \bar{k} \end{array}$$

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.

5.4.3. 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 $\mathfrak{p}_y=A\cap\mathfrak{p}_yA_y=A\cap\mathfrak{p}_{y'}A_{y'}=\mathfrak{p}_{y'}$. 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.

25. Definición: Se dice que C es la variedad de Riemann asociada a K.

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 $\mathcal{O}_{v'} \mapsto \mathcal{O}_v \cap K$. 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.

Sea $C' = \operatorname{Proj} k[\xi_0,\dots,\xi_n]$, $\operatorname{gr}\xi_i = 1$, 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 $\mathcal{O}_{C',x} := k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]_x \subseteq \Sigma$ (que no depende del abierto $U^h_{\xi_i}$ que contiene a x, considerado).

Dado un anillo de valoración $\mathcal{O}_v$ de Σ, trivial sobre k, existe un único punto $x \in C'$, tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x}$: 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, $k[\xi_0/\xi_i,\dots,\xi_n/\xi_i] \subset \mathcal{O}_v$. Si $\mathfrak{p}_x := \mathfrak{p}_v \cap k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, tenemos que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x}$. Sea otro $x' \in C'$ tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x'}$. Sea k, tal que $x \in U^h_{\xi_k}$. Si $x' \notin U^h_{\xi_i}$, entonces $\xi_i/\xi_k \in \mathfrak{p}_{x'}\mathcal{O}_{C',x'}$, luego $v(\xi_i/\xi_k) > 0$ y $v(\xi_j/\xi_k) = v(\xi_i/\xi_k \cdot \xi_j/\xi_i) = v(\xi_i/\xi_k) + v(\xi_i/\xi_j) > v(\xi_i/\xi_j)$, lo cual es contradictorio. Si $x' \in U^h_{\xi_i}$, entonces $\mathfrak{p}_{x'} := \mathfrak{p}_v \cap k[\xi_0/\xi_i,\dots,\xi_n/\xi_i] = \mathfrak{p}_x$ 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 $\mathcal{O}_v$ domina a $\mathcal{O}_{C',\pi(v)}$. 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 $\mathbb{P}^1$.

Sea C la variedad de Riemann asociada a K y $f \in K$ trascendente. Tenemos $k(f) \hookrightarrow K$ y el morfismo inducido entre las variedades de Riemann $f\colon C \to \mathbb{P}^1$. 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 $\{x_1,\dots,x_n\}$ 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,

$$\text{Nº de puntos de la fibra del } 0 = \dim_k A/(f) = \sum_{x \in C, v_x(f) \geq 0} v_x(f) \operatorname{gr}_k x,$$

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

$$\text{Nº de puntos de la fibra del } \infty = \dim_k A'/(1/f) = \sum_{x \in C, v_x(1/f) \geq 0} v_x(1/f) \operatorname{gr}_k x$$

número que se denomina *número de polos de* f. Por tanto,

$$0 = \text{Nº de puntos de la fibra del } 0 \ - \ \text{nº de puntos de la fibra del } \infty = \sum_{x \in C} v_x(f) \operatorname{gr}_k x$$

26. 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,*

$$\boxed{\textstyle\sum_{x \in C} v_x(f) \operatorname{gr}_k x = 0},$$

es decir, el número de ceros de f es igual a su número de polos.

5.5. Teoremas fundamentales de la Teoría de Números

Juan A. Navarro

Para el estudio y clasificación de los anillos de números enteros, A, se introducen el discriminante de A, el grupo $\mathrm{Pic}(A)$ 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 $\mathrm{Spec}\, A$ 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 sólo existe un número finito de cuerpos de números de discriminante fijo dado. El grupo de los ideales de A módulo isomorfismos, $\mathrm{Pic}\, A$, 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 sólo módulo p admite soluciones enteras, para infinitos primos p.

5.5.1. 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 sólo si $a = 0$.
2. *Desigualdad triangular:* $|a+b| \leq |a| + |b|$.
3. $|ab| = |a||b|$.

Es inmediato comprobar que para todo valor absoluto se 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.

2. 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 $a \in K$.

3. Proposición: *Dos valores absolutos sobre un cuerpo K son equivalentes si y sólo si inducen la misma topología.*

Demostración. 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, $1/x \in B(0,1)$. Conocido el valor $|x|$, la topología determina el valor absoluto de los demás elementos: Dado y, tendremos que $|y| = |x|^\alpha$, para cierto número real. Tenemos que ver cómo la topología determina este número α. En efecto,

$$\frac{n}{m} < \alpha \iff \frac{|x|^{\frac{n}{m}}}{|y|} < 1 \iff \left|\frac{x^n}{y^m}\right| < 1 \iff \frac{x^n}{y^m} \in B(0,1)$$

Se termina fácilmente. □

4. Definición: Un valor absoluto $||: A \to \mathbb{R}$ se dice arquimediano si la imagen de la aplicación natural $\mathbb{N} \to \mathbb{R}$ no está acotada, es decir, para toda constante $C > 0$ existe un natural n tal que $|n| > C$.

Evidentemente, todo cuerpo dotado de un valor absoluto arquimediano debe ser de característica cero.

5. 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 natural n en base d,

$$n = a_0 + a_1 d + \ldots + a_k d^k, \qquad \text{con } 0 \leq a_i < d$$

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. □

6. Primer teorema de Ostrowski, 1917: *Todo valor absoluto arquimediano sobre* $\mathbb{Q}$ *es equivalente al valor absoluto usual.*

Demostración. Por el lema, $|2| > 1$. Sustituyendo $||$ por $||^r$, con $r > 0$ conveniente, podemos suponer que $|2| = 2$. Entonces, $|3| \leq |2| + |1| = 3$ y $4 = |2| \cdot |2| = |4| \leq |3| + 1$, luego $|3| = 3$. Entonces, $|5| \leq |4| + |1| = 5$ y $6 = |2 \cdot 3| = |6| \leq |5| + 1$, luego $|5| = 5$. Así sucesivamente, obtenemos que $||$ es el valor absoluto usual sobre $\mathbb{N}$, luego lo es sobre $\mathbb{Q}$. □

Vamos ahora a determinar los valores absolutos arquimedianos sobre un cuerpo de números K (extensión finita de $\mathbb{Q}$).

7. 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 sólo si $e = 0$.
2. $||e_1 + e_2|| \leq ||e_1|| + ||e_2||$ (desigualdad triangular).
3. $||\lambda e|| = |\lambda| \cdot ||e||$.

8. 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

$$||e||' = ||\sum_i \lambda_i e_i||' \leq \sum_i |\lambda_i| ||e_i||' \leq \sum_i |\lambda_i| C = C \cdot n \cdot ||e||.$$

9. Proposición: *Si F es un subespacio vectorial cerrado de un espacio vectorial normado $(E,||||)$, entonces*

$$||\bar{e}|| := \text{ínf}\{||e'||: e' \in e+F\}$$

es una norma sobre E/F, y la proyección natural $E \to E/F$ es continua.

10. 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 $||||'$. □

11. Teorema: *Sea K una extensión finita de $\mathbb{Q}$. 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,*

$$\left\{ \begin{array}{l} \textit{valores absolutos arquimedianos} \\ \textit{sobre } K\textit{, módulo equivalencia} \end{array} \right\} = \left\{ \begin{array}{l} \textit{morfismos } K \to \mathbb{C} \\ \textit{mód. conjugación} \end{array} \right\} = \text{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$

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.

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 usual (por 5.5.6), 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 5.5.10, 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 $\hat{K} = \mathbb{C}$ (este último isomorfismo está unívocamente determinado salvo conjugación). En el segundo caso, el valor absoluto $||$ sobre $\hat{K} = \mathbb{C}$ es equivalente al usual porque es una norma sobre el cuerpo $(\mathbb{R},||)$, y tales normas son todas equivalentes a la norma infinita, la cual define la topología producto usual en $\mathbb{R}^2 = \mathbb{C}$. □

5.5.2. Valores absolutos no arquimedianos y valoraciones

12. Proposición: *Un valor absoluto $|| : A \to \mathbb{R}$ es no arquimediano si y sólo si verifica la desigualdad ultramétrica: $|a+b| \leq \text{máx}\{|a|,|b|\}$.*

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

$$|a+b| = (1+n)^{1/n}|b|,$$

y tomando límite para $n \to \infty$ se concluye que

$$|a+b| \leq 1 \cdot |b| = \text{máx}\{|a|,|b|\}.$$

$\Leftarrow$) De la desigualdad ultramétrica, resulta por inducción que $|n| \leq 1$ para todo $n \in \mathbb{N}$. □

13. Proposición : *Dada una valoración $v: K\backslash\{0\} \to \mathbb{R}$, la aplicación $||_v : K \to \mathbb{R}$, $|a|_v := e^{-v(f)}$ es un valor absoluto no arquimediano. Recíprocamente, dado un valor absoluto no arquimediano $||: K \to \mathbb{R}$, la aplicación $v_{||}: K\backslash\{0\} \to \mathbb{R}$, $v_{||}(a) := -\ln|a|$ es una valoración.*

14. 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 $a \in K\backslash\{0\}$.*

15. 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 $\lambda \in k\backslash\{0\}$), 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 $a \in K\backslash\{0\}$.*

16. Corolario: *Sea K un cuerpo de números y A el anillo de enteros de K. Entonces,*

$$\{\textit{Conjunto de valores absolutos no arquimedianos de } K\}/\sim = \operatorname{Spec} A$$

17. Corolario: *Sea $||_\infty$ el valor absoluto usual de $\mathbb{Q}$. Entonces,*

$$\left\{ \begin{array}{l} \textit{valores absolutos sobre } \mathbb{Q}, \\ \textit{módulo equivalencia} \end{array} \right\} = \operatorname{Spec}\mathbb{Z} \coprod \{||_\infty\}$$

18. Corolario: *Sea K un un cuerpo de números y A el anillo de enteros de K. Entonces,*

$$\left\{ \begin{array}{l} \textit{valores absolutos sobre } K, \\ \textit{módulo equivalencia} \end{array} \right\} = \operatorname{Spec} A \coprod \operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$

19. Corolario: *Sea K una $k(x)$-extensión finita de cuerpos y C la variedad de Riemann de K. Entonces,*

$$\{\textit{Conjunto de valores absolutos de } K, \textit{ triviales sobre } k\}/\sim = C$$

5.5.3. Producto de valores absolutos de una función

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

$$\boxed{\textstyle\prod_{x\in C} |f|_x^{\operatorname{gr}_k x} = e^{-\sum_{x\in C} \operatorname{gr}_k x \cdot v_x(f)} \overset{5.4.26}{=} e^0 = 1}$$

20. Definición: Dado un anillo A y un ideal maximal $\mathfrak{m}_x \subset A$, tal que $A/\mathfrak{m}_x$ sea un cuerpo finito, notaremos $\operatorname{gr} x := \ln|A/\mathfrak{m}_x|$.

Asociemos a cada número primo $p \in \mathbb{Z}$ el valor absoluto p-ádico $||_p$ definido por $|a|_p = e^{-v_p(a)}$. Observemos que $|a|_p^{\operatorname{gr} p} = p^{-v_p(a)}$.

21. Proposición: *Digamos que $\operatorname{gr}\infty = 1$. Entonces, dada $0 \neq f \in \mathbb{Q}$*

$$\prod_{x \in \operatorname{Spec}\mathbb{Z} \coprod \{\infty\}} |f|_x^{\operatorname{gr} x} = 1$$

22. Definición: Sea A una k-álgebra finita separable. Dada $a \in A$ consideremos el k-endomorfismo lineal $a\cdot: A \to A$, $b \mapsto ab$. Se define $N(a) = \det(a\cdot)$.

Obviamente, $N(1) = 1$ y $N(aa') = N(a)\cdot N(a')$. Sea K una k-extensión que trivialice a A y $\{\sigma_1, \ldots, \sigma_n\} = \operatorname{Hom}_{k-alg}(A, K)$. Por la proposición 2.3.27,

$$\boxed{N(a) = \textstyle\prod_i \sigma_i(a)}$$

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), $X_\infty := \operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$ 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).

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 $\operatorname{gr} y := \dim_{\mathbb{R}}(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{m}_y$.

23. Proposición: *Dada $a \in A$, se cumple que*

$$|N(a)| = \prod_{y \in X_\infty} |a|_y^{\operatorname{gr} y}$$

Demostración. $|N(a)| = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})} |\sigma(a)| = \prod_{y \in X_\infty} |a|_y^{\operatorname{gr} y}$. □

Dado $x \in X = \operatorname{Spec} A$, sea $|\,|_x$ el valor absoluto no arquimediano asociado a x definido por $|a|_x := e^{-v_x(a)}$. Recordemos que $\operatorname{gr} x := \ln |A/\mathfrak{m}_x|$. Observemos que $|a|_x^{-\operatorname{gr} x} = |A/\mathfrak{m}_x|^{v_x(a)}$.

24. Proposición: *Sea K un cuerpo de números y A el anillo de enteros de K. Dada $a \in A$, se cumple que*

1. $|N(a)| = |A/aA|$.
2. $|N(a)| = \prod_{x \in X} |a|_x^{-\operatorname{gr} x}$.

Demostración. 1. Existen sendas bases de los $\mathbb{Z}$-módulos A y A en las que el endomorfismo $a\cdot\colon A \to A$ diagonaliza. El determinante de la matriz de $a\cdot$ en estas bases es igual salvo signos a $|A/aA|$, y es igual, salvo signos al determinante del endomorfismo $a\cdot$, con lo que concluimos.

2. $|A/aA| = \prod_{x \in X} |(A/aA)_x| = \prod_{x \in X} |A/\mathfrak{m}_x|^{v_x(a)} = \prod_{x \in X} |a|_x^{-\operatorname{gr} x}$.

□

25. Teorema: *Sea K un cuerpo de números. Para toda $f \in K$, se cumple que*

$$\boxed{\prod_{x \in \bar{X}} |f|_x^{\operatorname{gr} x} = 1}$$

26. Ejercicio: Comprobar la fórmula del teorema 5.5.25, para $K = \mathbb{Q}[i]$ y $f = i + 1$.

Denotemos los invertibles (o unidades) de A, A^*.

27. Proposición: $A^* = \{a \in A : N(a) = \pm 1\}$.

Demostración. Sea $a \in A$. $|N(a)| = |A/(a)| = 1$ si y sólo si $a \in A^*$. □

28. Observación: Dado $a \in A$ sea $p_c(x) = \sum_{i=0}^n a_i x^{n-i}$ el polinomio característico de la homotecia $a\cdot\colon A \to A$. Sabemos que $N(a) = (-1)^n a_n$ y por otra parte $0 = p(a) = b \cdot a + a_n$, con $b \in A$. En conclusión, $N(a) = a \cdot c$, con $c \in A$.

29. Proposición: *Sea $c \in \mathbb{N}$. Consideremos la acción natural por multiplicación de A^* en $\{f \in A : |N(f)| = c\}$, entonces*

$$|\{f \in A : |N(f)| = c\}/A^*| \leq c^d$$

"El número de $f \in A$, salvo multiplicación por unidades, 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, $c \in fA$. Además, si $|N(f')| = c$ y $\overline{f'} = \bar{f}$ en A/cA, entonces $f'A = f'A + cA = fA + cA = fA$, es decir, $f' \in f \cdot A^*$. Por tanto, tenemos que

$$\{f \in A : |N(f)| = c\}/A^* \subseteq (A/cA)/A^*,\ \bar{f} \mapsto \overline{\bar{f}}$$

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 $|A/cA| = c^d$.

□

5.5.4. Divisores afines

30. Notación: En las siguientes subsecciones 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 sólo si $i\leq r$ y $\bar{\sigma}_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación).

31. Definición: Llamaremos grupo de divisores afines de K, que denotaremos $\mathrm{Div}(A)$, al grupo abeliano libre de base los puntos cerrados de $\mathrm{Spec}\,A$,

$$\mathrm{Div}(A)=\oplus_{x\in\mathrm{Spec}_{max}A}\mathbb{Z}\cdot x$$

Cada $D=\sum_i n_i\cdot x_i\in\mathrm{Div}(A)$ 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 $\mathrm{Sop}(D)=\{x\in\mathrm{Spec}\,A, n_x\neq 0\}$ es el soporte de D.

32. 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.

33. Ejercicio: Probar que $\mathrm{Pic}\,\mathbb{Z}=\{0\}$.

34. Ejercicio: Probar que $\mathrm{Pic}\,A=\{0\}$ si y sólo 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 $\mathfrak{a}'=f\cdot\mathfrak{a}$.

35. Proposición: *Se cumplen las igualdades*

$$\textit{Conj. de ideales no nulos de } A=\textit{Conj. de divisores afines efectivos},\ \mathfrak{a}=\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_r}^{n_r}\mapsto D(\mathfrak{a}):=\sum_i n_i x_i$$

$$\textit{Conjunto de ideales no nulos de } A,\textit{ módulo isomorfismos }=\mathrm{Pic}\,A,\ [\mathfrak{a}]\mapsto[D(\mathfrak{a})]$$

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 $\mathfrak{a}'$. □

36. Definición: Llamemos ideal fraccionario de K a los A-submódulos no nulos finito generados de K.

Los ideales fraccionarios son A-módulos localmente principales, porque son A-módulos finito generados de rango 1 sin torsión y A es localmente un dominio de ideales principales.

En el conjunto de ideales fraccionarios tenemos la operación multiplicación de ideales.

37. Notación: Sea $x\in\mathrm{Spec}\,A$ un punto cerrado. Denotemos $\mathfrak{m}_x^{-1}:=\{h\in K\colon D(h)\geq -x\}$, y dado $n\in\mathbb{N}$ denotemos $\mathfrak{m}_x^{-n}:=(\mathfrak{m}_x^{-1})^n$.

38. Proposición: *Sea $x\in\mathrm{Spec}\,A$ un punto cerrado. Entonces,*

1. *$\mathfrak{m}_x^{-1}$ es un ideal fraccionario.*
2. *Para todo ideal fraccionarios I de K,*
$$I=\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_m}^{n_m}$$
para ciertos $x_1,\dots,x_m\in\mathrm{Spec}\,A$ distintos (y únicos) y ciertos $n_1,\dots,n_m\in\mathbb{Z}$ (únicos).
3. *$\mathfrak{m}_x^{-1}\cdot\mathfrak{m}_x=A$.*

Demostración. Dado un ideal fraccionario I, denotemos $D(I) := \sum_{x\in \operatorname{Spec} A} \text{ínf}\{v_x(f), f \in I\}\cdot x$. Dados los divisores afines $D_i = \sum_x n_{ix}x$, con $1 \le i \le r$, denotemos

$$D_1 \cap \cdots \cap D_r := \sum_x \text{ínf}\{n_{1x},\ldots,n_{rx}\}\cdot x.$$

Si $I_1,\ldots,I_r \subset K$ son ideales fraccionarios, entonces $D(I_1+\ldots+I_r) = D(I_1)\cap\cdots\cap D(I_r)$ y $D(I_1\cdots I_r) = D(I_1)+\cdots+D(I_n)$.

Dado un punto cerrado $x \in \operatorname{Spec} A$, sea $f \in K$ tal que $v_x(f) = -1$. Existe $g \in A$ tal que $v_x(g) = 0$ (luego $v_x(fg) = -1$) y tal que $D(fg) = D(f)+D(g) \ge -x$. Sea $x' \notin \operatorname{Sop}(D(fg))$ y sea el ideal fraccionario $J = \mathfrak{m}_{x'} + A\cdot fg$. Tenemos que $D(J) = D(\mathfrak{m}_{x'})\cap D(fg) = -x$. Observemos que $J_y = A_y$, para $y \ne x$ y que $J_x = fgA_x$. Observemos que $J = \mathfrak{m}_x^{-1}$, porque $J \subseteq \mathfrak{m}_x^{-1}$ y son iguales localmente.

Dado un ideal fraccionario I y un punto cerrado $x \in \operatorname{Spec} A$, sea $t \in K$ tal que $v_x(t) = 1$ y $n = \text{ínf}\{v_x(f), f \in I\}$. Entonces, $I_x = t^n\cdot A_x$ y $I_x = \mathfrak{m}_x^n\cdot A_x$. Si $D(I) = \sum_{n_x} n_x\cdot x$, entonces

$$I = \prod_{n_x} \mathfrak{m}_x^{n_x}$$

porque localmente coinciden.

Por último, $D(\mathfrak{m}_x^{-1}\cdot\mathfrak{m}_x) = 0$, luego $\mathfrak{m}_x^{-1}\cdot\mathfrak{m}_x$ es un ideal de A que ha de coincidir con A. □

Si dos ideales fraccionarios no nulos $I, I' \subset K$ son isomorfos, localizando en el punto genérico obtenemos un isomorfismo de K-módulos de K, que es multiplicar por una $f \in K$, luego $I' = f\cdot I$.

39. Proposición: *Las asignaciones*

$$\begin{array}{rcl} \operatorname{Div} A & \longrightarrow & \{\textit{Ideales fraccionarios de } K\} \\ D = \sum_i n_i x_i & \longmapsto & \{f \in K : D(f) \ge D\} = \prod_i \mathfrak{m}_{x_i}^{n_i} \\ D(I) := \sum_x \text{ínf}\{v_x(f), f \in I\}\cdot x & \longleftarrow\!\shortmid & I \end{array}$$

son inversas entre sí. Por tanto,

$$\operatorname{Pic} A = \textit{Conjunto de ideales fraccionarios de } K\textit{, módulo isomorfismos}$$

Demostración. Si $I = \prod_{n_x} \mathfrak{m}_x^{n_x}$ entonces $D(I) = \sum_x n_x x$, y

$$I = \prod_{n_x} \mathfrak{m}_x^{n_x} = (\cap_{n_x} \mathfrak{m}_x^{n_x}) = \{f \in K : D(f) \ge D(I)\}$$

□

5.5.5. Divisores completos

40. Notación: Sea $X = \operatorname{Spec}_{max} A$, $X_\infty = \operatorname{Spec} K \otimes_{\mathbb{Q}} \mathbb{R}$ y $\bar{X} = X \coprod X_\infty$.

41. Definición: Llamaremos grupo de los divisores completos de $\bar{X}$, que denotaremos $\operatorname{Div}(\bar{X})$, al grupo

$$\operatorname{Div}(\bar{X}) = (\oplus_{x\in X}\mathbb{Z}\cdot x)\oplus(\oplus_{y\in X_\infty}\mathbb{R}\cdot y)$$

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 $\bar{D} \ge 0$ si $n_x, \lambda_y \ge 0$, para todo x e y.

42. 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 $\operatorname{Div}(\bar{X})$. El cociente de $\operatorname{Div}(\bar{X})$ por el subgrupo de los divisores principales completos se denota $\operatorname{Pic}(\bar{X})$ y se denomina grupo de Picard completo.

43. 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

$$\mathrm{gr}(\bar{D}) := \sum_{x\in X} n_x \cdot \mathrm{gr}\, x + \sum_{y\in X_\infty} \lambda_y \cdot \mathrm{gr}\, y$$

44. 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, $N\colon \{\text{Ideales fraccionarios de } K\} \to \mathbb{Q}^*$ es un morfismo de grupos.

45. 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,

$$|I/I'| = |A/\mathfrak{a}| = N(\mathfrak{a}) = N(I')/N(I)$$

□

46. Ejercicio: Sea $0 \neq f \in A$. Probar que $|N(f)| = N((f))$.

47. Proposición: *Dado un ideal fraccionario $I \subseteq K$ se cumple que*

$$\mathrm{gr}(D(I)) = \ln(N(I))$$

Demostración. Las aplicaciones $\mathrm{gr}\circ D, \ln\circ N\colon \{\text{Ideales fraccionarios de } K\} \to \mathbb{Q}$ son morfismos de grupos. Para ver que son iguales basta comprobar que coinciden sobre los ideales maximales $\mathfrak{m}_x$. Efectivamente, $\mathrm{gr}(D(\mathfrak{m}_x)) = \mathrm{gr}(x) = \ln|A/\mathfrak{m}_x| = \ln(N(\mathfrak{m}_x))$. □

Observemos que $\mathrm{gr}\colon \mathrm{Div}(\bar{X}) \to \mathbb{R}$ es un morfismo de grupos.

48. Teorema: *Para toda $f \in K$, se cumple que*

$$\mathrm{gr}(\bar{D}(f)) = 0$$

Demostración. Es consecuencia de la proposición 5.5.25 □

49. Ejercicio: Sea $\bar{X}$ el conjunto de valores absolutos de $\mathbb{Q}$, módulo equivalencia. Probar que $\mathrm{Pic}\,\bar{X} = \mathbb{R}$.

50. Proposición: *Sea $c \in \mathbb{Z}$. Salvo multiplicación por unidades existe un número finito de $a \in A$ tal que $N(a) = c$.*

Demostración. $|N(a)| = |A/aA| = |c|$ si y sólo si $\mathrm{gr}\,D(a) = \ln|c|$. Ahora bien, divisores afines efectivos de grado dado sólo 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 unidades a alguno de los a_i.

□

5.5.6. Volumen de un paralelepípedo. Discriminante

Sea $T_2 : L \times L \to \mathbb{R}$ una métrica simétrica no singular sobre un $\mathbb{Z}$-módulo libre L de rango n. T_2 extiende a $\Lambda^n_{\mathbb{Z}} L$:

$$T_2(e_1 \wedge \cdots \wedge e_n, e'_1 \wedge \cdots \wedge e'_n) := (i_{e_1} T_2 \wedge \cdots \wedge i_{e_n} T_2)(e'_1, \cdots, e'_n) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot T_2(e_1, e'_{\sigma(1)}) \cdots T_2(e_n, e'_{\sigma(n)})$$

Se cumple que

$$T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n) = \det((T_2(e_i, e_j)))$$

Si $e'_1, \ldots, e'_n$ es otra base y (λ_{ij}) es la matriz de cambio de base, entonces $e'_1 \wedge \cdots \wedge e'_n = \det(\lambda_{ij}) \cdot e_1 \wedge \cdots \wedge e_n$, y

$$T_2(e'_1 \wedge \cdots \wedge e'_n, e'_1 \wedge \cdots \wedge e'_n) = \det(\lambda_{ij})^2 T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n)$$

51. Definición: Sea $e_1, \ldots, e_n$ una base de L. Se define el discriminante de L, que denotamos Δ_L, por

$$\boxed{\Delta_L := \det(T_2) := \det(T_2(e_i, e_j))}$$

(Dadas dos bases del $\mathbb{Z}$-módulo libre L, el determinante de la matriz de cambio de bases ha ser ± 1. Por tanto, el determinante de la métrica T_2 en estas dos bases coincide).

Sea $E = L \otimes_{\mathbb{Z}} \mathbb{R}$, consideremos la inclusión $L \hookrightarrow E$ y el cociente E/L. Se define el volumen del paralelepípedo generado por $e_1, \ldots, e_n$ ("paralelepípedo fundamental"), que denotamos $Vol(e_1, \ldots, e_n)$, por

$$Vol(e_1, \ldots, e_n) := \sqrt{|\Delta_L|} =: Vol(E/L)$$

52. Definición: Diremos que un subgrupo aditivo Γ de un espacio vectorial real E de dimensión n, es una red si está generado por alguna base $\{e_1, \ldots, e_n\}$ del espacio vectorial, es decir, $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ y $E = \Gamma \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}e_1 \oplus \cdots \oplus \mathbb{R}e_n$.

53. Sea $\Gamma \subset K$ un $\mathbb{Z}$-módulo libre de rango d. Consideremos la inclusión canónica

$$\Gamma \hookrightarrow \Gamma \otimes_{\mathbb{Z}} \mathbb{R} = K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \oplus \mathbb{C}^s =: \mathcal{O}_\infty,\ a \mapsto (\sigma_1(a), \ldots, \sigma_r(a), \sigma_{r+1}(a), \ldots, \sigma_{r+s}(a))$$

Γ es una red de $\mathcal{O}_\infty$. **Todo anillo de enteros, como todo ideal fraccionario no nulo son redes de $\mathcal{O}_\infty$.**

En $\mathcal{O}_\infty$ tenemos la métrica T_2 de la traza. El volumen de los paralelepípedos con esta métrica es 2^s-veces el volumen de los paralelepípedos con la métrica euclídea estándar.

54. Notación: Sea A el anillo de enteros del cuerpo de números K. Por abuso de notación, escribiremos $\Delta_K := \Delta_A$.

Denotaremos una base de $\Gamma \subset K$, $\{a_1, \ldots, a_d\}$.

55. Observación: 1. $|\Delta_\Gamma| = Vol(\mathcal{O}_\infty/\Gamma)^2$. Si consideramos la matriz de números reales cuyas filas son los vectores $(\sigma_1(a_j), \ldots, \sigma_{r+s}(a_j)) \in \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$, entonces $Vol(\mathcal{O}_\infty/\Gamma) = 2^s |\det(\sigma_i(a_j))|$.

2. Si $\Gamma \cdot \Gamma \subseteq \Gamma$, entonces $T_2(a_i \cdot a_j)$ es la traza del endomorfismo de $\mathbb{Z}$-módulos $(a_i a_j)\cdot : \Gamma \to \Gamma$, luego es un número entero y Δ_Γ es un número entero.

56. Ejercicio: Sea A un anillo de enteros y supongamos que $i \notin A$. Demostrar que $\Delta_{A[i]} = (-4)^d \cdot \Delta_A^2$.

Como,

$$(T_2(a_i, a_j)) = (\operatorname{tr}(a_i a_j)) = (\sum_{k=1}^{d} \sigma_k(a_i a_j)) = (\sigma_i(a_j))^t \cdot (\sigma_i(a_j)),$$

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

$$\boxed{Vol(\mathcal{O}_\infty/\Gamma) = \sqrt{|\Delta_\Gamma|} = |\det((\sigma_i(a_j)))|}$$

57. Ejercicio: Probar que si K es una $\mathbb{Q}$-extensión de Galois, entonces $\sqrt{\Delta_K} \in K$.

Si tenemos dos redes $\Gamma' \subseteq \Gamma$, entonces existen bases en Γ' y Γ donde la matriz de la inclusión es diagonal y es claro que

$$\Delta_{\Gamma'} = |\Gamma/\Gamma'|^2 \cdot \Delta_\Gamma$$
$$Vol(\mathcal{O}_\infty/\Gamma') = |\Gamma/\Gamma'| \cdot Vol(\mathcal{O}_\infty/\Gamma)$$

Recordemos que si $I' \subset I$ son ideales fraccionarios, $|I/I'| = N(I')/N(I)$.

58. Proposición: *Si I es un ideal fraccionario, entonces*

$$\boxed{Vol(\mathcal{O}_\infty/I) = N(I) \cdot \sqrt{|\Delta_A|}}$$

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,

$$Vol(\mathcal{O}_\infty/I) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot Vol(\mathcal{O}_\infty/\mathfrak{b}^{-1}) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot N(\mathfrak{b}^{-1}) \cdot Vol(\mathcal{O}_\infty/A) = N(I) \cdot \sqrt{|\Delta_A|}$$

□

59. Ejemplo: Sea α raíz de un polinomio irreducible $p(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ y sea $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(p(x))$. Sea $\{\sigma_i\} = \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$, entonces las raíces de $p(x)$ son $\{\sigma_i(\alpha)\}_i$.

Una base de $\mathbb{Z}[\alpha]$ es $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Por tanto,

$$\Delta_{\mathbb{Z}[\alpha]} = \det((\sigma_i(\alpha^j)))^2 = \det((\alpha_i^j))^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta(p(x))$$

Sea A el anillo de enteros de K. Entonces,

$$\Delta(p(x)) = \Delta_{\mathbb{Z}[\alpha]} = |A/\mathbb{Z}[\alpha]|^2 \cdot \Delta_A$$

Por ejemplo, el discriminante de $x^2 - n$ es $4n$. Si n no tiene factores cuadráticos y $\mathbb{Z}[\sqrt{n}]$ no es normal, entonces $|A/\mathbb{Z}[\alpha]| = 2$. Como $\frac{\sqrt{n}+1}{2}$ es entero, $A = \mathbb{Z}[\frac{\sqrt{n}+1}{2}]$ (y $\Delta_A = n$).

60. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0, 1$ y sin factores cuadráticos. Demostrar que el discriminante de $K = \mathbb{Q}[\sqrt{n}]$ es n si $n \equiv 1 \mod 4$, y es $4n$ si $n \equiv 2, 3 \mod 4$.

61. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0, 1$ y sin factores cuadráticos. Sea Δ el discriminante de $\mathbb{Q}[\sqrt{n}]$. Probar que el anillo de enteros de $\mathbb{Q}[\sqrt{n}]$ es igual a $\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$.

5.5.7. Teorema de Riemann-Roch débil

62. Definición: Sea $\bar{D}$ un divisor completo, definimos $H^0(L_{\bar{D}}) := \{f \in K : \bar{D} + \bar{D}(f) \geq 0\}$.

Si $\bar{D} = n_1 x_1 + \cdots + n_m x_m + \lambda_1 y_1 + \cdots + \lambda_{r+s} y_{r+s}$, entonces

$$H^0(L_{\bar{D}}) = \left\{ \begin{array}{r} f \in K : v_{x_i}(f) \geq -n_i, \forall i \\ v_x(f) \geq 0, \forall x \neq x_i \end{array} \right\} \cap \{f \in K^* : v_{y_i}(f) \geq -\lambda_i, \forall y_i\}$$
$$= \mathfrak{m}_{x_1}^{-n_1} \cdots \mathfrak{m}_{x_m}^{-n_m} \bigcap \{(\mu_i) \in \mathbb{R}^r \times \mathbb{C}^s = \mathcal{O}_\infty : |\mu_i| \leq e^{\lambda_i}, \forall i\}$$

63. Propiedades:

1. *Si $D' = \bar{D} + \bar{D}(f)$, entonces tenemos una biyección $f\cdot : H^0(L_{D'}) \simeq H^0(L_{\bar{D}})$.*
2. *El conjunto $H^0(L_{\bar{D}})$ 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 $\{(\mu_j) \in \mathbb{R}^r \times \mathbb{C}^s = \mathcal{O}_\infty : |\mu_j| \leq e^{\lambda_j}, \forall j\}$, que es finito.*
3. *En el caso $\bar{D} = 0$, denotamos $L_{\bar{D}} = \mathcal{O}_{\bar{X}}$. Entonces, $H^0(\mathcal{O}_{\bar{X}}) \backslash \{0\} = \{f \in K^* : \bar{D}(f) = 0\}$ 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. *Si $\mathrm{gr}(\bar{D}) < 0$ entonces $H^0(L_{\bar{D}}) = \{0\}$.*
5. *Si $\mathrm{gr}(\bar{D}) = 0$ y $H^0(L_{\bar{D}}) \neq \{0\}$, entonces existe f tal que $\bar{D} + \bar{D}(f) \geq 0$, luego $\bar{D} + \bar{D}(f) = 0$ y $\bar{D} = \bar{D}(f^{-1})$.*

64. Teorema del punto de la red de Minkowski: *Sea E un espacio vectorial real de dimensión d, con una métrica T_2 no singular. Sea Γ una red de E y C un compacto de E, convexo y simétrico respecto del origen. Si $Vol(C) \geq 2^d Vol(E/\Gamma)$, 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 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 $\frac{y-x}{2} \in C$. □

65. Teorema de Riemann-Roch débil: *Sea $\bar{D}$ un divisor completo. Entonces, $H^0(L_{\bar{D}}) \neq \{0\}$ cuando*

$$\operatorname{gr}\bar{D} \geq \ln \sqrt{|\Delta_K|} - s \cdot \ln(\pi/2)$$

Demostración. Podemos suponer que $\bar{D} = -D(I) + D_\infty$, con $D_\infty = \sum_i \lambda_i y_i$. Por tanto, $H^0(L_{\bar{D}})$ es la intersección del ideal fraccionario I con el compacto

$$C = \{(\mu_1, \ldots, \mu_{r+s}) \in \mathcal{O}_\infty : |\mu_i| \leq e^{\lambda_i}, \forall i\}$$

que es un compacto de volumen $Vol(C) = 2^r e^{\lambda_1+\cdots+\lambda_r} \cdot 2^s \pi^s e^{2(\lambda_{r+1}+\cdots+\lambda_{r+s})} = 2^d (\frac{\pi}{2})^s e^{\operatorname{gr}(D_\infty)}$. El teorema del punto de la red de Minkowski asegura que $H^0(L_{\bar{D}}) \neq \{0\}$ cuando

$$2^d (\frac{\pi}{2})^s e^{\operatorname{gr}(D_\infty)} = Vol(C) \geq 2^d Vol(\mathcal{O}_\infty/I) = 2^d N(I) \sqrt{|\Delta_K|} = 2^d e^{\operatorname{gr} D(I)} \sqrt{|\Delta_K|}$$

es decir, cuando $(\frac{\pi}{2})^s e^{\operatorname{gr}\bar{D}} \geq \sqrt{|\Delta_K|}$.

□

66. Corolario: *Si $\bar{D}$ es un divisor completo y $\operatorname{gr}\bar{D} \geq \ln \sqrt{|\Delta_K|}$, entonces $\bar{D}$ es linealmente equivalente a un divisor completo efectivo.*

5.5.8. Finitud de la clase de ideales

67. 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 $\operatorname{gr}(D + D_\infty) = \ln \sqrt{|\Delta_K|}$. Por el teorema de Riemann-Roch débil, existe $f \in K$ tal que $D + D_\infty$ es linealmente equivalente a un divisor efectivo de grado $\ln \sqrt{|\Delta_K|}$. Por tanto, D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln \sqrt{|\Delta_K|}$. □

68. Teorema: $\operatorname{Pic} A$ *es un grupo finito.*

Demostración. El número de divisores afines efectivos de grado menor o igual que cierto número es finito. Dado $[D] \in \operatorname{Pic} A$, D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln \sqrt{|\Delta_K|}$ (o equivalentemente, todo ideal es isomorfo a un ideal de norma menor o igual a $\sqrt{|\Delta_K|}$). □

69. Ejercicio: Sea K un cuerpo de números y A el anillo de enteros de K. Probar que si todo ideal primo $\mathfrak{p}_x \subset A$ es principal si $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|}$, entonces A es un dominio de ideales principales.

Es conocido que $\mathbb{Q}[\sqrt{-r}]$, con $r > 0$ y no divisible por ningún primo al cuadrado, es de ideales principales si si sólo si $r = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

70. 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 $n = |\operatorname{Pic} A|$. Entonces, $n \cdot [\mathfrak{a}] = 0$, para todo $[\mathfrak{a}] \in \operatorname{Pic} A$, es decir, $\mathfrak{a}^n$ es un ideal principal, para todo ideal $\mathfrak{a} \subseteq A$. □

71. 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 $\mathfrak{a}^n = (a)$ es principal. Si B es el anillo de enteros de $K[\sqrt[n]{a}]$, entonces $\mathfrak{a} \cdot B = (\sqrt[n]{a})$. En efecto, $(\mathfrak{a} \cdot B)^n = a \cdot B = (\sqrt[n]{a})^n$, luego las descomposiciones en producto de ideales primos de $\mathfrak{a} \cdot B$ y la $(\sqrt[n]{a})$ han de ser la misma, luego son iguales. Si $\mathrm{Pic} A = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_n]\}$ y $(\mathfrak{a}_i)^n = (a_i)$, entonces $L = K[\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_n}]$.

□

72. Teorema de Minkowski: $\Delta_K \neq \pm 1$ *para toda extensión finita K de $\mathbb{Q}$, no trivial.*

Demostración. Si $\Delta_K = \pm 1$, por el corolario 5.5.66, todo divisor completo de grado cero es principal, lo cual es imposible porque hay un número no numerable de divisores completos de grado cero.

□

73. Teorema de Hermite: *Sólo 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.

Podemos suponer que $i \in K$: si $i \notin K$, entonces $|\Delta_{K[i]}| \leq |\Delta_{A[i]}| = 4^d |\Delta_A|^2 = 4^d |\Delta_K|^2$, y como probaremos, 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 y cada uno de éstos contiene un número finito de subextensiones. En conclusión, el número de cuerpos de discriminante Δ y grado d es finito.

Suponemos, pues, que $i \in K$ (luego $r = 0$). Consideremos en el infinito el divisor

$$(d + \ln \sqrt{|\Delta_K|}) \cdot y_1 - y_2 - \ldots - y_s$$

El teorema de Riemann-Roch débil afirma la existencia de una $f \in A$ tal que $|\sigma_i(f)| \leq e^{-1} < 1$, para todo $i > 1$. Como $N(f)$ es un número entero, se sigue $|\sigma_1(f)| = |f| > 1$. Sea $H = \{\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) \colon \sigma(f) = f\}$, tendremos que $|\sigma(f)| > 1$, para todo $\sigma \in H$. Por tanto, $H = \{\sigma_1\}$ y $K = \mathbb{Q}[f]$ (o bien, $H = \{\sigma_1, \bar{\sigma}_1\}$, en este caso $K = \mathbb{Q}[if]$ y tomaríamos if en vez de f). Observemos, además, que $|\sigma_1(f)| \leq e^d \cdot \sqrt{|\Delta_K|}$. Por tanto, los coeficientes del polinomio anulador de f están acotados, pues sus raíces $\sigma_i(f)$ lo están, y como son números enteros sólo hay un número finito de tales polinomios.

□

74. Proposición: *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*

$$|N(f)| \leq c|N(I)|, \text{ con } c = d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|}$$

Fijado el discriminante del cuerpo de números, el grado está acotado.

Demostración. Consideremos el compacto

$$C = \{(\lambda_1, \ldots, \lambda_r, \ldots, \lambda_{r+s}) \in \mathcal{O}_\infty = \mathbb{R}^r \times \mathbb{C}^s \colon \sum_{i \leq r} |\lambda_i| + \sum_{j > r} 2|\lambda_j| \leq t\}$$

que tiene volumen $2^r \pi^s t^d / d!$. Sea t, de modo que $Vol(C) = 2^d Vol(\mathcal{O}_\infty / I)$. 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,

$$|N(f)| = \prod_i |\sigma_i(f)| \leq (\sum_i |\sigma_i(f)|/d)^d \leq t^d / d^d = d! d^{-d} (4/\pi)^s \cdot Vol(\mathcal{O}_\infty / I) = d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot |N(I)|$$

Como $c \geq 1$, se sigue que fijado el discriminante el grado está acotado.

□

75. Ejercicio: Sea K un cuerpo de números de discriminante -4. Probar que $\dim_{\mathbb{Q}} K = 2$. Probar que $K = \mathbb{Q}[i]$.

5.5.9. Unidades de un anillo de enteros

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.

76. Lema: *Sea Γ un subgrupo discreto de $\mathbb{R}^d$. Entonces, existen $r \leq d$ vectores linealmente independientes $e_1,\dots,e_r \in \mathbb{R}^d$ de modo que $\Gamma = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_r$.*

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 $\mathbb{R}^d$, y que $\mathbb{Z}^d \subseteq \Gamma$. Consideremos la proyección $\pi\colon \mathbb{R}^d \to \mathbb{R}^d/\mathbb{Z}^d = S_1^d$. Observemos que 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. 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, $e_1,\dots,e_d \in \Gamma$ tales que $\Gamma = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_r$ y como $e_1,\dots,e_d$ generan $\mathbb{R}^d$, han de ser linealmente independientes en $\mathbb{R}^d$. □

Sea $\mathrm{Div}^0(\bar{X})$ el conjunto de los divisores completos de grado cero. Sea $\mathrm{Div}_\infty = \oplus_{y\in X_\infty}\mathbb{R}\cdot y = \mathbb{R}^{r+s}$ el grupo de los divisores completos de soporte en el infinito y Div^0_∞ el grupo de los divisores completos de soporte en el infinito de grado 0. Consideremos el morfismo natural $\mathrm{Div}(\bar{X}) \to \mathrm{Div}(X)$, $\bar{D} \mapsto \bar{D}_{|X}$ y la sucesión exacta,

$$0 \to \mathrm{Div}^0_\infty \to \mathrm{Div}^0(\bar{X}) \to \mathrm{Div}(X)$$

Sea $\mathrm{Pic}^0(\bar{X})$ el grupo de las clases de equivalencia de los divisores completos de grado 0. Sea A^* el conjunto de todas las unidades (o invertibles) de A y $\mathrm{Pic}^0_\infty := \mathrm{Div}^0_\infty/\bar{D}(A^*)$. Las sucesiones

$$0 \to \mathrm{Pic}^0_\infty \to \mathrm{Pic}^0(\bar{X}) \to \mathrm{Pic}(X)$$
$$1 \to \mu_K \to A^* \xrightarrow{\bar{D}} \mathrm{Div}^0_\infty \to \mathrm{Pic}^0_\infty \to 0$$

son exactas. Sabemos que $\mathrm{Pic}(X)$ es un grupo finito.

77. 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

$$\bar{D} + \bar{D}(f) \geq 0$$

Como $D(f) \geq 0$, entonces $f \in A$ y $c' := \mathrm{gr}D(f) \geq 0$. $\bar{D} + \bar{D}_\infty(f)$ está en el compacto

$$C := \{D'' \in \mathrm{Div}^{c-c'}_\infty : D'' \geq 0\}$$

Es decir, $\bar{D}$ pertenece al compacto $C_f := C - \bar{D}_\infty(f) \subset \mathrm{Div}^c_\infty$. Observemos que $c - c' \geq 0$, luego $c' \leq c$. Ahora bien, el número de $f \in A$, salvo multiplicación por unidades, tales que $\mathrm{gr}D(f) \leq c$ es finito. Por tanto, existe un número finito de funciones $f_i \in A$ de modo que para cada $\bar{D} \in \mathrm{Div}^c_\infty$, existe i tal que $\bar{D} \in C_{f_i} \bmod \bar{D}(A^*)$. Por tanto,

$$\mathrm{Pic}^c_\infty = \cup_i \overline{C_{f_i}},$$

que es unión de un número finito de compactos, luego compacto.

□

78. Teorema de Dirichlet: Pic^0_∞ *es un toro de dimensión $r+s-1$ y las unidades A^* es un grupo finito generado de rango $r+s-1$ y de torsión las raíces de la unidad contenidas en K.*

Demostración. A es un subconjunto discreto de $\mathscr{O}_\infty$, luego A^* es un subgrupo discreto de $\mathscr{O}_\infty^*$. Consideremos la aplicación

$$\bar{D}_\infty\colon \mathscr{O}_\infty^* = (\mathbb{R}^r \oplus \mathbb{C}^s)^* \to \mathrm{Div}_\infty,\ (\lambda_i) \mapsto \sum_i -(\ln|\lambda_i|)\cdot y_i$$

La imagen de A^* es $\bar{D}(A^*)$, luego $\bar{D}(A^*)$ es discreto en $\mathrm{Div}_\infty^0 = \mathbb{R}^{r+s-1}$. Por el lema anterior $\bar{D}(A^*)$ 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 $r+s-1$. El núcleo del epimorfismo $A^* \to \bar{D}(A^*)$, $f \mapsto \bar{D}(f)$ es $H^0(\mathscr{O}_{\bar{X}}) =: \mu_K$, que son las raíces de la unidad contenidas en K. Por tanto,

$$A^* \simeq \mu_K \oplus \mathbb{Z}^{r+s-1}$$

□

79. Ejercicio: Probar que existen $\xi_1,\dots,\xi_{r+s-1} \in A^*$, de modo que $a \in A^*$ si y sólo 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).

80. 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 $\dim_k K$ es impar, y es un grupo abeliano finito generado de rango $r+s-1$ y torsión μ_K si $\dim_k K$ es par.*

Demostración. Si $\dim_k K$ es impar, entonces $r > 0$, luego $K \subset \mathbb{R}$ y $\mu_K = \{\pm 1\}$. Además, $N(-1) = -1$, luego $\{a \in A : N(a) = 1\}$ es un subgrupo de índice dos de A^* y $\mu_K \cap \{a \in A : N(a) = 1\} = \{1\}$. Por tanto, $\{a \in A : N(a) = 1\}$ es un grupo de rango $r+s-1$ sin torsión, luego libre.

Si $\dim_k K$ es par, entonces $N(\xi) = 1$ para todo $\xi \in \mu_K$: Obviamente $N(\pm 1) = 1$. 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 $a \in A\setminus\{0\}$. Como $\{a \in A : N(a) = 1\}$ es un subgrupo de índice finito de A^* (1 ó 2) y $\mu_K \subset \{a \in A : N(a) = 1\}$, concluimos que es un grupo abeliano finito generado de rango $r+s-1$ y torsión μ_K.

□

81. Ejercicio: Probar 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 sólo

$$a = \begin{cases} \xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.} \\ \mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu \in \mu_K, \text{ si } \dim_k K \text{ es par.} \end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1} \in \mathbb{Z}$ (únicos). Probar 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 sólo

$$a = \begin{cases} \mu_i\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.} \\ \mu_i\cdot\mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu \in \mu_K, \text{ si } \dim_k K \text{ es par.} \end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1} \in \mathbb{Z}$ (únicos), para un i (único) (recordar la proposición 5.5.50).

82. Ejemplo: Sea $n > 1$ un entero sin factores cuadráticos y $K = \mathbb{Q}[\sqrt{n}]$ y $A = \mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$ el anillo de enteros de K. A^* es un grupo abeliano de rango 1 y parte de torsión ± 1. Sabemos que $x + y\cdot\frac{\Delta+\sqrt{\Delta}}{2} \in A^*$ si y sólo si $N(x + y\cdot\frac{\Delta+\sqrt{\Delta}}{2}) = \pm 1$, es decir, como $x + y\cdot\frac{\Delta+\sqrt{\Delta}}{2} = \frac{2x+y\Delta}{2} + \frac{y}{2}\cdot\sqrt{\Delta}$,

$$(2x + y\Delta)^2 - y^2\Delta = \pm 4$$

Por tanto,

$$A^* = \{\frac{a + b\sqrt{\Delta}}{2}, a, b \in \mathbb{Z} : a^2 - b^2\Delta = \pm 4\}$$

Para calcular el generador de A^*, que es único salvo toma de inverso y multiplicación por -1, observemos podemos suponer que $a, b > 0$ y ha de ser aquel que cumpla además que a y b son mínimos.

83. Ejercicio: Calcular las unidades de los anillos de enteros de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ y $\mathbb{Q}[\sqrt{6}]$.

5.5.10. Número de ideales de norma acotada

84. Teorema: *Sea $S(n)$ el número de ideales de A de norma $\le n$. Existe una constante no nula v tal que $S(n) = vn + O(n^{1-1/d})$.*

Demostración. En virtud de la finitud de $\operatorname{Pic} A$, basta probar el teorema para el número $S(n)$ 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, $S(n)$ es el número de divisores afines efectivos, D', de grado $\le \ln n$, afínmente equivalentes a un divisor afín dado $-D$ (podemos suponer $D = D(\mathfrak{a})$ efectivo y escribamos $m = \operatorname{gr} D$). La condición $D' = D(f) - D \ge 0$ significa que $f \in \mathfrak{a}$, y la condición $\operatorname{gr}(D(f) - D) = \operatorname{gr}(D(f)) - \operatorname{gr} D \le \ln n$ significa $\operatorname{gr}(D(f)) \le \ln n + m$. Es decir, $S(n)$ es el número de conjuntos fA^* tales que $f \in \mathfrak{a}$ y tales que $\operatorname{gr}(D(f)) \le \ln n + m$.

Consideremos los morfismos

$$\begin{array}{lcll} (\mathbb{R}^r \oplus \mathbb{C}^s)^* = \mathscr{O}_\infty^* & \overset{\bar{D}_\infty}{\to} & \operatorname{Div}_\infty & \overset{-\operatorname{gr}}{\to} \quad \mathbb{R} \\ (\lambda_1, \dots, \lambda_{r+s}) & \mapsto & -\sum_i (\ln|\lambda_i|) \cdot y_i & \end{array}$$

Observemos que $-\operatorname{gr}(\bar{D}_\infty(f)) = \operatorname{gr}(D(f))$, ya que $\operatorname{gr}\bar{D}(f) = 0$. Sea G el núcleo del morfismo de grupos $\bar{D}_\infty$ y $\operatorname{Div}_\infty \to \mathscr{O}_\infty^*$, $\sum_i \mu_i y_i \mapsto (e^{-\mu_1}, \dots, e^{-\mu_{r+s}})$ una sección de $\bar{D}_\infty$, luego $\mathscr{O}_\infty^* = G \times \operatorname{Div}_\infty$. Sea $\mathbb{R} \to \operatorname{Div}_\infty$, $t \mapsto \frac{-t}{d} \cdot (y_1 + \cdots + y_{r+s})$ una sección de $-\operatorname{gr}$. Luego $\operatorname{Div}_\infty = \operatorname{Div}_\infty^0 \times \mathbb{R}$ y

$$\mathscr{O}_\infty^* = G \times \operatorname{Div}_\infty^0 \times \mathbb{R}$$

y la homotecia por $\lambda \in \mathbb{R}$ en $\mathscr{O}_\infty^*$ se corresponde con la traslación por $\ln \lambda^d$ en el tercer factor de $G \times \operatorname{Div}_\infty^0 \times \mathbb{R}$. Sea $P \subset \operatorname{Div}_\infty^0$ el paralelepípedo fundamental de la red $\bar{D}(A^*)$ en $\operatorname{Div}_\infty^0$. Para cada conjunto fA^*, existe $u \in A^*$ tal que $\bar{D}_\infty(fu) \in P \times \mathbb{R} \subset \operatorname{Div}_\infty$ y todos los que cumplen esta condición son $f \cdot u \cdot \mu_K$ (observemos además que $\operatorname{gr}(D(fv)) = \operatorname{gr} D(f)$, para todo $v \in A^*$). Luego, si $w = |\mu_K|$, entonces $w \cdot S(n)$ es el número de elementos de la red $\mathfrak{a}$ en el conjunto

$$U_n := G \times P \times (-\infty, \ln n + m] = n^{1/d} U_1$$

Es decir, $w \cdot S(n)$ es el número de elementos de la red $n^{-1/d} \cdot \mathfrak{a}$ en U_1. Por el lema[1] 5.5.85, $w \cdot S(n) = v \cdot n + O(n^{\frac{d-1}{d}})$.

□

85. 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 $U \cap \lambda^{-1}\Gamma$, 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 $\Gamma = \mathbb{Z}^d$. Sea $C = \{x \in \mathbb{R}^d : 0 \le x_i \le \lambda^{-1}, \forall i\}$. Considerando la unión $\coprod_{p \in U \cap \lambda^{-1}\Gamma} p + C$, 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 a una distancia $\le \epsilon = \sqrt{d}/\lambda$ del borde C de U. Luego,

$$Vol(U) - Vol(C_\epsilon) \le P(\lambda)\lambda^{-d} \le Vol(U) + Vol(C_\epsilon)$$

y se concluye al observar que $Vol(C_\epsilon) = O(\epsilon)$.

□

[1] Donde $E = \mathscr{O}_\infty$, $\Gamma = \mathfrak{a}$ y $U = U_1 \coprod \{0\}$. $U_1 = G \times P \times (\infty, m]$ es acotado porque si denotamos por ϕ la igualdad $G \times \operatorname{Div}_\infty^0 \times \mathbb{R} = \mathscr{O}_\infty^*$, entonces $\phi(G \times P \times (-\infty, m]) = (0, e^{m/d}] \cdot \phi(G \times P \times \{0\})$. Observemos además que el cierre de $G \times P \times (-\infty, m]$ en $\mathscr{O}_\infty$ es igual a este conjunto unión $0 \in \mathscr{O}_\infty$

5.5.11. La función zeta

86. Teorema: *La serie* $\zeta(x)=\sum_{n=1}^{\infty} n^{-x}$ *es una función continua en* $(1,\infty)$ *tal que*

$$\lim_{x\to 1}(x-1)\cdot\zeta(x)=1 \quad y \quad \zeta(x)=\prod_p(1-\frac{1}{p^x})^{-1}$$

Demostración. La serie $\sum_{n=1}^{\infty} n^{-x}$ una serie de términos positivos y tenemos

$$\frac{1}{x-1}=\int_1^{\infty} t^{-x}dt<\sum_{n\geq 1} n^{-x}<1+\int_1^{\infty} t^{-x}dt=1+\frac{1}{x-1}$$

luego es convergente. Además, los sumandos n^{-x} son funciones continuas en x decrecientes, por lo que la serie $\zeta(x)$ es continua. Por último, la igualdad $\sum_{n=1}^{\infty} n^{-x}=\prod_p(1+p^{-x}+p^{-2x}+\cdots)=\prod(1-p^{-x})^{-1}$ expresa la unicidad de la descomposición de n en producto de números primos. □

87. Corolario: *Sea* $m\geq 2$ *un número natural y* P *cualquier conjunto de números primos. El producto* $\prod_{p\in P}(1-(p^m)^{-x})^{-1}$ *define una función continua en la semirrecta* $x>1/2$.

Demostración. La serie $\zeta(mx)=\sum_n(n^m)^{-x}$ define una función continua en la semirrecta $x>1/m\geq 2$ y la subserie formada por los términos correspondientes a los números n con todos sus factores primos en P coincide con el producto considerado. □

88. Definición: Sea K un cuerpo de números y A el anillo de enteros de K. Se dice que

$$\zeta_K(x):=\sum_{0\neq\mathfrak{a}\subset A} N(\mathfrak{a})^{-x}$$

es la función zeta de K.

89. 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 5.5.84 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 $h(x):=\sum_n a_n n^{-x}$ 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. □

90. 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. Por hipótesis existe una constante $c>0$ tal que $|b_n|<cn^{\epsilon}$. Ahora, para cada pareja de números naturales $m<r$,

$$\sum_{n=m}^{r} a_n\cdot n^{-x}=\sum_{n=m}^{r}(b_n-b_{n-1})\cdot n^{-x}=b_r r^{-x}-b_m m^{-x}+\sum_{n=m}^{r-1} b_n\cdot(n^{-x}-(n+1)^{-x})$$

Como $|b_n\cdot(n^{-x}-(n+1)^{-x})|\leq cn^{\epsilon}\cdot x\int_n^{n+1} t^{-x-1}dt\leq c\cdot x\int_n^{n+1} t^{-x-1+\epsilon}dt$,

$$|\sum_{n=m}^{r} a_n\cdot n^{-x}|\leq 2cm^{-x+\epsilon}+c\cdot x\int_m^{\infty} t^{-x-1+\epsilon}dt=(2c+\frac{cx}{-x+\epsilon})\cdot m^{-x+\epsilon},$$

que tiende a cero para $m>>0$ (fijado el compacto de la semirrecta (ϵ,∞)). □

91. Definición: Dado un anillo de enteros A y un ideal maximal $\mathfrak{p} \subset A$ y $(p) = \mathfrak{p} \cap \mathbb{Z}$, llamaremos grado sobre $\mathbb{Z}$ de $\mathfrak{p}$, que denotaremos $\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p}$, a

$$\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p} := \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{p}$$

Obviamente, $m = \mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p} \leq \dim_{\mathbb{Z}/p\mathbb{Z}} A/pA = d$ y el número de ideales primos en la fibra de p de grado m es menor o igual que d/m.

Por ejemplo, dado un polinomio mónico $q(x) \in \mathbb{Z}[x]$ sea $A = \mathbb{Z}[x]/(q(x))$. Los primos de de A de grado sobre $\mathbb{Z}$ igual a 1 se corresponden con las raíces racionales de $q(x)$ en $\mathbb{Z}/p\mathbb{Z}$ (variando p).

92. Notación: Dadas dos funciones continuas $f(x)$ y $g(x)$ en la semirrecta $x > 1$, escribiremos $f(x) \sim g(x)$ cuando $g(x) = u(x) \cdot f(x)$, en un entorno $(1, 1+\epsilon)$, para alguna función continua $u(x)$ definida en el entorno $(1-\epsilon, 1+\epsilon)$ y tal que $u(1) \neq 0$.

93. Teorema: *Se cumple que*

$$\zeta_K(x) \sim \prod_{\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p}=1} (1 - \frac{1}{N(\mathfrak{p})^x})^{-1}$$

Demostración. Sea $P_{m,r} := \{\text{primos } p \in \mathbb{Z}, \text{ tales que el número de ideales primos de grado } m \text{ sobre } \mathbb{Z} \text{ en la fibra de } p \text{ es } r\}$. Observemos que si $P_{m,r} \neq \emptyset$ entonces $m \cdot r \leq d$. Como

$$\zeta(x) = \prod_{\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p}=1} (1 - \frac{1}{N(\mathfrak{p})^x})^{-1} \cdot \prod_{m>1, mr \leq d} \prod_{p \in P_{m,r}} (1 - \frac{1}{(p^m)^x})^{-r}$$

y $\prod_{p \in P_{m,r}} (1 - \frac{1}{(p^m)^x})^{-r}$ definen funciones continuas en la semirrecta $x > 1/2$ según 5.5.87, hemos concluido.

□

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.

94. Corolario: *Todo cuerpo de números tiene infinitos primos de grado* 1 *sobre* $\mathbb{Z}$.

Demostración. Si K sólo tuviera un número finito de primos de grado 1, entonces existe $c \neq 0$ tal que

$$\lim_{x \to 1} \zeta(x) = c \cdot \lim_{x \to 1} \prod_{\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p}=1} (1 - \frac{1}{N(\mathfrak{p})^x})^{-1} < \infty$$

y $\lim_{x \to 1} (x-1) \cdot \zeta(x) = 0$ y llegamos a contradicción.

□

95. Corolario: *Todo polinomio no constante con coeficientes enteros $q(x)$ tiene infinitas raíces modulares. Más aún, hay infinitos números primos p en los que $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{Z}/p\mathbb{Z}$. □

96. Corolario: *Dado $0 \neq n \in \mathbb{N}$, en la lista $\{1 + mn, m \in \mathbb{N}\}$ existen infinitos números primos.*

Demostración. Existen infinitos primos p de modo que $\overline{x^n - 1} \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene todas sus raíces en p, es decir, en los que el morfismo de Fröbenius $F_p = \mathrm{Id}$, es decir, $p = 1 \in (\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$. □

97. 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 $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ con $\mathrm{gr}_{\mathbb{Z}}\,\mathfrak{p}_i = 1$, para todo i.

98. Corolario: *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 $d = \dim_k K$. Por hipótesis, la fibra de casi todos los primos de grado 1 sobre $\mathbb{Z}$ está formada por d primos de L, que necesariamente han de tener 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,

$$\zeta_L(x) \sim \xi_K(x)^d$$

Si $d > 1$ se obtiene la contradicción

$$\lim_{x\to 1}(x-1)\cdot\zeta_L(x) = \lim_{x\to 1}\zeta_K(x)^d = \infty$$

□

99. 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 $\mathbb{Q}$.*

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 sólo 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 corolario anterior, $\mathbb{Q} = K$ y $q(x) = \lambda\cdot(x-\alpha)$ descompone totalmente en $\mathbb{Q}$. □

100. Corolario: *Si un número entero es resto cuadrático módulo casi todo primo, entonces es un cuadrado perfecto.*

Demostración. Considérese en el corolario anterior $q(x) = x^2 - n$. □

101. 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 $L' \subseteq L$. Si $q(x), q'(x) \in \mathbb{Z}[x]$, la condición necesaria y suficiente para que todas las raíces de $q'(x)$ sean expresiones racionales de las raíces de $q(x)$ es que en casi todos los primos p en los que el automorfismo de Frobënius de $q(x)$ sea trivial lo sea el automorfismo de Frobënius de $q'(x)$.*

Demostración. Dado un cuerpo de números F denotemos A_F el anillo de enteros de F.

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 es 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, $L' \subseteq L$.

□

102. Teorema: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q(x_1,\dots,x_n)\\ &\cdots\cdots\\ 0 &= q_r(x_1,\dots,x_n)\end{aligned}$$

tenga alguna solución compleja es que admita soluciones modulares en infinitos primos

Demostración. Si el sistema no tiene soluciones complejas, el teorema de los ceros de Hilbert afirma que $0 = \mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r) = \mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)\otimes_{\mathbb{Q}}\mathbb{C}$, y por tanto

$$\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r) = 0$$

Luego existen polinomios $h_1,\dots,h_r \in \mathbb{Q}[x_1,\dots,x_n]$ tales que $\sum_i h_i q_i = 1$. Ahora es evidente que, salvo en los primos que dividan a algún denominador de los coeficientes de h_i, la reducción $\bar{q}_1 = 0,\dots,\bar{q}_r = 0$ módulo p del sistema dado carece de soluciones en $\mathbb{Z}/p\mathbb{Z}$.

Recíprocamente, si el sistema considerado tiene alguna raíz compleja, entonces

$$\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r) \neq 0$$

y el teorema de los ceros de Hilbert afirma que 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

$$x_1 = \frac{a_1}{m_1},\dots,x_n = \frac{a_n}{m_n}$$

con $a_i \in A$ y $m_i \in \mathbb{Z}$. Como el corolario 5.5.94 afirma la existencia de infinitos primos $\mathfrak{p}$ de grado 1 de en A, se concluye la existencia de infinitos primos p, tales que el sistema considerado tiene solución en $\mathbb{Z}/p\mathbb{Z} = A/\mathfrak{p}$.

□

5.6. Explosión a lo largo de un cerrado. Desingularización

1. Definición: 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 $\widetilde{X} \to X$. 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 verifica*

1. $\pi^{-1}(X\backslash x) \overset{\pi}{=} X\backslash x$.
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 $X\backslash x$ 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. $\pi^{-1}(Y)=\operatorname{Proj}G_IA$. *"La fibra de Y es igual al espacio normal a Y en X".*

Sea $I=(\xi_1,\dots,\xi_n)$. Dado $\xi\in I$ denotemoslo $\tilde{\xi}$ cuando lo pensemos como el elemento de grado 1 de D_IA. D_IA es un álgebra graduada generada por sus elementos de grado uno, pues se tiene un epimorfismo graduado

$$\begin{aligned}A[x_1,\dots,x_n]&\to D_IA\\ x_i&\mapsto\tilde{\xi}_i\end{aligned}$$

Entonces, $D_IA=A[\tilde{\xi}_1,\dots,\tilde{\xi}_n]$. Sabemos que $\operatorname{Proj}D_IA\setminus(\tilde{\xi})_0^h=\operatorname{Spec}A[\frac{\tilde{\xi}_1}{\tilde{\xi}},\dots,\frac{\tilde{\xi}_n}{\tilde{\xi}}]$. Además $A[\frac{\tilde{\xi}_1}{\tilde{\xi}},\dots,\frac{\tilde{\xi}_n}{\tilde{\xi}}]$ es isomorfo, con el isomorfismo obvio, al subanillo $A[\frac{\xi_1}{\xi},\dots,\frac{\xi_n}{\xi}]$ de A_ξ.

5. Ejercicio: Probar que $\operatorname{Proj}D_IA=\operatorname{Proj}D_{I^n}A$ para todo $n\in\mathbb{N}$ (Pista: Consideremos la inclusión natural $D_{I^n}A\subset D_IA$ que multiplica los grados por n. Dado $\xi\in I$, pruébese las igualdades

$$\operatorname{Proj}D_IA\setminus(\tilde{\xi})_0^h=\operatorname{Spec}[(D_IA)_{\tilde{\xi}}]_0=\operatorname{Spec}[(D_IA)_{\tilde{\xi}^n}]_0=\operatorname{Spec}[(D_{I^n}A)_{\tilde{\xi}^n}]_0=\operatorname{Proj}D_{I^n}A\setminus(\tilde{\xi}^n)_0^h.$$

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. Probar

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

$$\begin{array}{ccc}\widetilde{C}&\overset{\tilde{i}}{\hookrightarrow}&\widetilde{\mathbb{A}}^n\\ \downarrow\pi&&\downarrow\pi\\ C&\overset{i}{\hookrightarrow}&\mathbb{A}^n\end{array}$$

Probar que si C es una recta, que pasa por el origen, entonces $\widetilde{C}\overset{\pi}{=}C$. Diremos que $\tilde{i}(\pi^{-1}(x))$ es la dirección definida por la recta C en x. Probar que si $n=2$ y C es la curva nodal $y^2-x^2+x^3=0$, entonces $\tilde{i}(\pi^{-1}(x))$ 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 $\mathfrak{m}=(\xi_1,\dots,\xi_n)$. Consideremos el isomorfismo graduado

$$D_{\mathfrak{m}}A=A[\tilde{\xi}_1,\dots,\tilde{\xi}_n]$$

Sabemos que dado $\xi\in\mathfrak{m}$, $\operatorname{Proj}D_{\mathfrak{m}}A\setminus(\tilde{\xi})_0^h=U_{\tilde{\xi}}^h=\operatorname{Spec}A[\tilde{\xi}_1/\tilde{\xi},\dots,\tilde{\xi}_n/\tilde{\xi}]=\operatorname{Spec}A[\xi_1/\xi,\dots,\xi_n/\xi]$. 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 anterior (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 $y_1,\dots,y_r$ 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 $\bar{\xi} \notin \mathfrak{p}_{i,1} \subsetneq \mathfrak{m}/\mathfrak{m}^2$. 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 $(A_1)_{\frac{\xi_i^m}{\xi}} = A[\xi_1/\xi_i, \ldots, \xi_n/\xi_i]$. *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 verifica 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 $\operatorname{Proj} D_{\mathfrak{m}_x}A = U_{\tilde{\xi}}^h = \operatorname{Spec} A[\xi/\xi] = \operatorname{Spec} A$, 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 5.6.11, A está incluido estrictamente en A_1= anillo de explosión en x. Por el lema 5.6.12, A_1 está incluido en el cierre entero $\bar{A}$ de A en su cuerpo de fracciones. Así pues, tenemos $A \subsetneq A_1 \subseteq \bar{A}$.

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

$$\operatorname{Spec}\bar{A} = \operatorname{Spec}A_n \underset{\pi_n}{\to} \operatorname{Spec}A_{n-1} \underset{\pi_{n-1}}{\to} \cdots \to \operatorname{Spec}A_1 \underset{\pi_1}{\to} \operatorname{Spec}A,$$

la cadena correspondiente de fibras excepcionales es un orden finito arbolado que se conoce como árbol de explosión de A.

5.7. 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 de $\mathbb{A}^m$ definida por los ceros del polinomio, 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 $\{H_1,\dots,H_r\}$ 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 5.6.7, y $A \to A_1$ el morfismo de explosión. Para todo $s >> 0$ se cumple que $\mathfrak{m}^s = \mathfrak{m}^s \cdot A_1$.*[2]

Demostración. Sea $\mathfrak{m} = (\xi_1,\dots,\xi_n)$ y $\xi \in \mathfrak{m}$ tal que $A_1 = A[\xi_1/\xi,\dots,\xi_n/\xi]$. Un sistema generador de A_1 como A-módulo lo forman los elementos de la forma $\frac{\xi_1^{\alpha_1}\cdots\xi_n^{\alpha_n}}{\xi^{\alpha_1+\cdots+\alpha_n}}$. Cada uno de ellos satisface que $\xi^s \cdot \frac{\xi_1^{\alpha_1}\cdots\xi_n^{\alpha_n}}{\xi^{\alpha_1+\cdots+\alpha_n}} \in \mathfrak{m}^s$ 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 5.6.7. 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 $-l_A(A_1/A)$.*

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 tenemos $S_{A_x}(n) = l_A(A_1/\mathfrak{m}_x^n A_1) - l_A(A_1/A) = l_A(A_1/\mathfrak{m}_x A_1)n - l_A(A_1/A)$, porque $\mathfrak{m}_x A_1$ es principal. Por tanto, $m(A_x) = l_A(A_1/\mathfrak{m}_x A_1) = \dim_{A/\mathfrak{m}_x A}(A_1/\mathfrak{m}_x A_1)$ y $S_{A_x}(0) = -l_A(A_1/A)$. □

8. Corolario: *Sea A como en el teorema 5.6.7. 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. □

9. 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.

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.

□

[2] **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.

5.8. 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 $\xi \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$ un parámetro transversal a C en x. Sabemos que $\tilde{C}$ está contenido en el abierto afín $U^h_{\tilde{\xi}}$ de $\widetilde{\mathbb{A}}^n$ cuyo anillo es $A[x_1/\xi,\dots,x_n/\xi]$. Si $H = (p)_0$, la ecuación de $\tilde{H}$ en el abierto $U^h_{\tilde{\xi}}$ es $p' = p/\xi^r$, 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

$$\begin{aligned}(C \cap H)_x = l(\mathcal{O}/(p)) \overset{5.4.16}{=} l(\mathcal{O}_1/(p)) = l(\mathcal{O}_1/(\xi^r \cdot p')) &= r \cdot l(\mathcal{O}_1/(\xi)) + l(\mathcal{O}_1/p') \\ &= m_x(H) \cdot m_x(C) + \sum_i (\tilde{C} \cap \tilde{H})_{y_i}\end{aligned}$$

□

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 sólo 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 sólo 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.

□

5.9. Ramas analíticas

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.

1. 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.

2. Teorema : *Sea $\bar{\mathcal{O}}$ el cierre entero de $\mathcal{O}$ en su cuerpo de fracciones Σ. Denotemos $y_1,\dots,y_s$ los puntos cerrados de* $\operatorname{Spec}\bar{\mathcal{O}}$*. 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 sólo ideal primo maximal y un sólo ideal primo minimal.

□

Considérese la sucesión exacta $0 \to \mathcal{O} \to \bar{\mathcal{O}} \to \mathcal{C} \to 0$. Completando se obtiene $0 \to \widehat{\mathcal{O}} \to \widehat{\bar{\mathcal{O}}} \to \widehat{\mathcal{C}} \to 0$. Se verifica que $\widehat{\mathcal{C}} = \mathcal{C}$ ya que $\mathcal{C}$ es un $\mathcal{O}$-módulo finito generado de soporte x. En particular, si $\mathfrak{p}_y$ es un ideal primo mínimo de $\widehat{\mathcal{O}}$, entonces $(\widehat{\mathcal{C}})_y = 0$, luego $(\widehat{\mathcal{O}})_y = (\widehat{\bar{\mathcal{O}}})_y$.

3. Teorema: *Hay una correspondencia biunívoca entre las ramas analíticas de $\mathcal{O}$ en x y las valoraciones de Σ que dominan a $\mathcal{O}$, esto es, entre el espectro minimal de $\widehat{\mathcal{O}}$ y el espectro maximal de $\bar{\mathcal{O}}$.*

Demostración. Si $\mathfrak{p}_y$ es un ideal primo minimal de $\widehat{\mathscr{O}}$, la fibra de y por el morfismo $\mathrm{Spec}\widehat{\tilde{\mathscr{O}}} \to \mathrm{Spec}\widehat{\mathscr{O}}$ es el espectro de $\widehat{\tilde{\mathscr{O}}}_y/\mathfrak{p}_y\widehat{\tilde{\mathscr{O}}}_y = \widehat{\mathscr{O}}_y/\mathfrak{p}_y\widehat{\mathscr{O}}_y$ por el comentario anterior. Por tanto, la fibra de y es un sólo punto que habrá de ser minimal, luego el espectro minimal de $\widehat{\mathscr{O}}$ está en correspondencia biunívoca con el espectro minimal de $\widehat{\tilde{\mathscr{O}}}$. Por el teorema anterior se concluye. □

4. Ejemplo: Sea $C \equiv p(x,y) = 0$ una curva plana íntegra que pasa por el origen, or. Sea $\mathscr{O} = (\mathbb{C}[x,y]_{or}/(p))$ es el anillo local de C en or y $\widehat{\mathscr{O}} = \mathbb{C}[[x,y]]/(p)$.

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 $p = f_1 \cdots f_r$, diferentes entre sí porque $\widehat{\mathscr{O}}$ no tiene nilpotentes (ya que $\widehat{\tilde{\mathscr{O}}}$, 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 $\mathbb{C}[[x,y]]/(f_i) \hookrightarrow \widehat{\tilde{\mathscr{O}}_{y_i}} = \mathbb{C}[[t]]$. 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.

5.9.1. 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 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, $ncx + mcy = rc$, 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.

5.10. Puntos cuspidales y contacto maximal

1. Definición: Sea $x \in C$ un punto de una curva íntegra y $\mathscr{O}$ su anillo local. Diremos que x es un punto cuspidal si el cierre entero de $\mathscr{O}$ 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 sólo 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 sólo 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 $\mathrm{Spec}\mathcal{O}$, entonces $m = l(\mathcal{O}/(f)) = l(\bar{\mathcal{O}}/(f)) = l(\hat{\bar{\mathcal{O}}}/(f))$. Por tanto, $f = \lambda \cdot t^m$, siendo λ una serie formal invertible. Como k es algebraicamente cerrado, λ tiene raíz n-ésima en $\hat{\bar{\mathcal{O}}} = k[[t]]$. Si definimos $u = \sqrt[n]{\lambda} \cdot t$, entonces $\hat{\bar{\mathcal{O}}} = k[[u]]$ y $f = u^n$. Así pues, toda función de $\hat{\bar{\mathcal{O}}}$ (y por tanto de $\mathcal{O}$) admite un desarrollo en serie formal en $u = \sqrt[n]{f}$. 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 $\mathrm{Spec}\mathcal{O}$, cada $\bar{x}_i$ admite un desarrollo de Puiseux $\bar{x}_i = \sum_{j \geq 0} a_j (\sqrt[n]{\bar{x}_1})^j$, con $a_j \in k$.

5.10.1. 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 sólo 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 $C_r \to .\overset{\pi}{.}. \to C$ de transformaciones cuadráticas X_r (transformada propia 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 $\mathbb{A}^2 = \operatorname{Spec} A$ en el origen está recubierto por dos abiertos afines $\operatorname{Spec} A[\frac{x}{t},\frac{y}{t}]$, 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 verifica*

$$\frac{DP}{t^{m-1}} = \tilde{D}\left(\frac{P}{t^m}\right)$$

"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
$$\frac{DP}{t^{m-1}} = (tD)\left(\frac{P}{t^m}\right) + (mDt)\left(\frac{P}{t^m}\right)$$
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. Se concluye por el teorema anterior. □

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 5.10.3 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 5.8.3), lo cual no es posible. Por tanto, después de un número finito de explosiones la multiplicidad debe bajar estrictamente, y se concluye por inducción.

□

5.11. 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, $C \cap H$ es un número finito de puntos cerrados. Existe, por tanto, un hiperplano H' que no pasa por ninguno de esos puntos, luego $C \cap H$ está incluido en el espacio afín complementario $\mathbb{A}^n = \mathbb{P}^n - H'$. Deshomogeneizando tenemos que $C \cap H = \operatorname{Spec} A$. El número de puntos de corte (contando multiplicidades y grados) de C con H, que denotaremos $(C \cap H)$, es $\dim_k A$. Este número no depende de la elección de 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 mínimo $r < n$ 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 sólo 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.

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 localmente $(\frac{p_3}{x_0^{n_3}}) \subseteq (\frac{p_1}{x_0^{n_1}}) + (\frac{p_2}{x_0^{n_2}})$. 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 simples en x, se cortan transversalmente en x y $x \in C_3$.*
2. *x es un punto simple 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 simple 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 $(p_3)_x \subset (p_1,p_2)_x \in k[x,y]$.

□

5.12. Apéndice: Revestimientos

5.12.1. 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 $p(x) \in \mathbb{Z}[x]$ y sea $\mathbb{Q}[\alpha_1,\dots,\alpha_n]$ el cuerpo de descomposición de $p(x)$. Consideremos el revestimiento $\operatorname{Spec} \mathbb{Z}[\alpha_1,\dots,\alpha_n] \to \operatorname{Spec} \mathbb{Z}$. 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 Frobënius.

5.12.2. Teoría de Galois de revestimientos

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 sólo si en espectros es epiyectivo.

2. Notación: Siempre que escribamos $\operatorname{Spec} B \to \operatorname{Spec} A$, será la aplicación inducida por un morfismo de anillos $A \to B$. Diremos que $\operatorname{Spec} B \to \operatorname{Spec} A$ es un revestimiento (resp. morfismo finito, plano), si el morfismo $A \to B$ es un revestimiento (resp. finito, plano). Dado otro morfismo $\operatorname{Spec} B' \to \operatorname{Spec} A$, denotaremos

$$\operatorname{Spec} B \underset{\operatorname{Spec} A}{\times} \operatorname{Spec} B' := \operatorname{Spec}(B \otimes_A B')$$

Denotaremos $\operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} B, \operatorname{Spec} B') := \operatorname{Hom}_{A-alg}(B', B)$. Si $Y \to X$ e $Y' \to X$ son revestimientos, diremos que $f \in \operatorname{Hom}_X(Y, Y')$ es un morfismo de revestimientos.

Observemos que si $\pi\colon Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ es epiyectivo entonces por cambio de base también lo es: Dado un cambio de base $f\colon X' \to X$, el morfismo inducido $\pi'\colon Y \times_X X' \to X'$ 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, $y \times_x x' = \operatorname{Spec}(k(y) \otimes_{k(x)} k(y') \neq \emptyset$. Como tenemos un morfismo obvio $y \times_x x' \to Y \times_X x'$, $\pi'^{-1}(x')$ es no vacío.

3. Ejemplos: 1. Los revestimientos de un cuerpo k son las k-álgebras finitas. En particular, las extensiones finitas de cuerpos son revestimientos.

2. Sea $B = A \times \overset{n}{\cdots} \times A$. El morfismo de anillos obvio $A \to B$ es un revestimiento. Observemos que

$$\operatorname{Spec} B = \operatorname{Spec} A \coprod \overset{n}{\cdots} \coprod \operatorname{Spec} A$$

Se dice que $\operatorname{Spec} B$ es un revestimiento trivial de $\operatorname{Spec} A$.

3. Todo morfismo finito $\varphi\colon A \to B$ entre dominios de Dedekind es inyectivo y es un revestimiento:

En efecto, $\operatorname{Ker}\varphi = 0$, porque si no $A/\operatorname{Ker}\varphi$ sería un cuerpo y B una $A/\operatorname{Ker}\varphi$-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.

4. Proposición: *La noción de revestimiento es estable por cambio de base.*

Demostración. En efecto, pues lo son la finitud y la fiel platitud. □

5. 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 $(- \otimes_A B) \otimes_B C = - \otimes_A C$. □

6. Definición: Diremos que un revestimiento $\operatorname{Spec} B \to \operatorname{Spec} A$ es de grado n, si B_x es un A_x-módulo libre de rango n, para todo punto cerrado $x \in \operatorname{Spec} A$.

Sabemos que todo A-módulo finito generado y plano es localmente libre. Si M es un A-módulo finito generado plano, entonces $\operatorname{Spec} A$ 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 $\operatorname{Spec} A_i = \{x \in \operatorname{Spec} A$ tales que M_x es un A_x-módulo libre de rango $i\}$.

Sea $A \to B$ es un morfismo finito plano, y denotemos $f\colon Y := \operatorname{Spec} B \to \operatorname{Spec} A =: X$ el morfismo inducido en los espectros. Entonces, $\operatorname{Spec} A = \coprod_{i=0}^{n} \operatorname{Spec} A_i$ e $Y = \coprod_{i=1}^{n} f^{-1}(\operatorname{Spec} A_i)$ y cada $f^{-1}(\operatorname{Spec} A_i)$ es un revestimiento de grado i de $\operatorname{Spec} A_i$. Además, $f(Y) = \coprod_{i=1}^{n} \operatorname{Spec} A_i$.

7. Proposición: *Si $f\colon Y \to X$ es un morfismo finito plano, entonces $f(Y)$ es un abierto y cerrado de X.*

Si X es conexo, $Y \to X$ es un revestimiento e $Y = Y_1 \coprod Y_2$ 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.

8. Proposición: *Sea $f\colon Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ 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 $\dim_{A_x/\mathfrak{p}_x A_x} B_x/\mathfrak{p}_x B_x = n$. □

9. Proposición: *Sea $f\colon Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ 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 sólo 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 0.6.9. □

10. 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.

11. Ejemplo: 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.

12. Ejemplo: Las k-álgebras finitas separables son revestimientos puros.

13. Ejercicio: Probar que un revestimiento $\pi\colon Y \to X$ es puro si y sólo si para cada punto cerrado $x \in X$, $\pi^{-1}(x) \to x$ es un revestimiento puro.

14. 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. □

15. 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 $0 = \Omega_{B/A} = \Omega_{B'/A} \oplus \Omega_{B''/A}$. □

16. Teorema: *Sea $\pi\colon Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ 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 $\sigma\colon B \to A$ la sección. Escribamos $I = \operatorname{Ker}\sigma$. Por 3.7.5, $I/I^2 = \Omega_{B/A} \otimes_B A = 0$. 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 $Y = \operatorname{Spec} B$. □

17. 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 sólo si $Y \times_X X' \to X'$ es un revestimiento trivial.

Demostración. Para la primera igualdad, véase 0.5.13. 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 $X' \coprod \overset{r}{\cdots} \coprod X' \hookrightarrow Y \times_X X'$ de revestimientos sobre X' y por grados, $r \leq n$. Además es una igualdad si y sólo si $r = n$. □

18. 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.

19. 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. Vamos a proceder 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

$$\begin{aligned} Y \times_X X' &= (Y \times_X Y) \times_Y X' = (Y \coprod Y_2 \coprod \cdots \coprod Y_r) \times_Y X' \\ &= X' \coprod \cdots \coprod X' \end{aligned}$$

□

Dejamos que el lector pruebe la siguiente proposición.

20. Proposición: *Sea X conexo. Si un revestimiento $Y \to X$ es un cerrado de un revestimiento trivial de X, o un revestimiento trivial de X se epiyecta sobre él, entonces $Y \to X$ es trivial.*

En consecuencia, si un revestimiento es un cerrado de un revestimiento puro, o un revestimiento puro se epiyecta sobre él, entonces el revestimiento es puro.

21. Proposición: *Sea X conexo. Si $\pi\colon Y' \to Y$ es un epimorfismo de revestimientos sobre X y $Y' \to X$ es un revestimiento puro, entonces π es un revestimiento puro.*

Demostración. Basta demostrar el teorema por cambio de base fielmente plano. Podemos suponer, pues, que Y' es trivial, luego Y también es trivial. Como todo morfismo entre revestimientos triviales aplica cada componente isomorfa a la base en otra componente, es fácil concluir la proposición. □

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, $\mathrm{Hom}_X(X'', Y) = \{\phi_1, \ldots, \phi_n\}$. 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 $Y \times \overset{n}{\cdots} \times Y$, luego es un revestimiento de X; además, como $Y \times \overset{n}{\cdots} \times Y$ es un revestimiento puro, X' es puro. Por la proposición anterior, X'' es un revestimiento puro epiyectivo 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 5.12.17, 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.

Para concluir, X' trivializa a Y, luego se trivializa a sí mismo, esto es, es un revestimiento principal de X. □

25. Proposición: *Sea $\pi\colon Y' \to Y$ 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 sólo 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*

$$P : C_G \rightsquigarrow C_{X'/X} \quad P(Z) = (X' \times Z)/G$$
$$P' : C_{X'/X} \rightsquigarrow C_G \quad P'(Y) = \mathrm{Hom}_X(X', Y)$$

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 $C_{Tru/X'}$ de X'. Los funtores que dan la equivalencia son $F : C_{Conj} \rightsquigarrow C_{Tru/X}$, $F(Z) := X' \times Z$ y $F' : C_{Tru/X} \rightsquigarrow C_{Conj}$, $F'(Y) = \mathrm{Hom}_{X'}(X', Y)$: $F \circ F' = \mathrm{Id}$, 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 $Z = \{z\}$.

2. Diremos que un revestimiento $\pi : Y' \to X'$ es un G-revestimiento si G opera en Y' por isomorfismos (de revestimientos sobre X) y π es un morfismo de G-conjuntos (es decir, $g \cdot \circ \pi = \pi \circ g \cdot$, para todo $g \in G$). La categoría de G-conjuntos finitos C_G es equivalente a la categoría de G-revestimientos triviales de X' $C_{Tru/X'}$: Por 1., los funtores $F : C_G \rightsquigarrow C_{Tru/X}$, $F(Z) := X' \times Z$ (G opera sobre los dos factores) y $F' : C_{Tru/X'} \rightsquigarrow C_G$, $F'(Y') := \mathrm{Hom}_{X'}(X', Y')$ (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 $C_{Tru/X'}$ de X' es equivalente a la categoría $C_{X'/X}$ de revestimientos de X trivializados por X'. Los funtores que dan la equivalencia son $S : C_{Tru/X'} \rightsquigarrow C_{X'/X}$, $S(Y') := Y'/G$ y $S' : C_{X'/X} \rightsquigarrow C_{Tru/X'}$, $S'(Y) := X' \times_X Y$. 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 5.12.25, $X' \to Y$ 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 conexo de grupo G y $H \subseteq G$ un subgrupo. Entonces, $X'/H \to X$ es un revestimiento principal si y sólo si H es un subgrupo normal de G.*

Demostración. $X'/H \to X$ es de Galois si y sólo 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,

$$X'/H \text{ es de Galois} \iff |N(H)/H| = |G/H| \iff |N(H)| = |G|$$
$$\iff H \text{ es normal en } G$$

□

5.12.3. El maravilloso automorfismo de Frobënius

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 $p \in \mathbb{Z}$.

30. 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*

$$\pi\colon \operatorname{Spec} B \to \operatorname{Spec} B^G \overset{3.4.4}{=} (\operatorname{Spec} B)/G.$$

Sea $x \in \operatorname{Spec} B$, $y := \pi(x)$, $D := \{g \in G : g(x) = x\}$ 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 de 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 de 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 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

$$\boxed{|D| = e_x \cdot \operatorname{gr}_y x}$$

31. 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 Frobënius, 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 Frobënius de Σ_A en el primo p.*

Demostración. Observemos que $A^G = \mathbb{Z}$ porque está incluido en $\mathbb{Q}$ y es finito sobre $\mathbb{Z}$. Además, 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 5.12.30, 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. □

32. 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 Frobënius 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 Frobënius, 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 Frobënius. Por tanto, el automorfismo de Frobënius 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 $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Dado un ideal $\mathfrak{m} \subset A$ en la fibra de p, $A/\mathfrak{m} = \mathbb{Z}/p\mathbb{Z}[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]$ es el cuerpo de descomposición de $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$. 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 sólo si lo es $\mathbb{Z}/p\mathbb{Z}[x]/(\overline{q(x)})$ (es decir, $q(x)$ es separable módulo p). Al automorfismo de Frobënius F_p asociado a $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ en p se le denomina también el automorfismo de Frobënius de $q(x)$ en p.

33. El polinomio $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es separable precisamente en los primos que no dividan al discriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$.

34. Cualquier cuártica cuyo grupo de Galois sea el grupo de Klein es irreducible, aunque no lo sea módulo cualquier primo p.

35. 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.

36. 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 $((\mathbb{Z}/n\mathbb{Z})^*, \cdot) = \langle p \rangle_{\{p<n, \text{ primo y no divide a } n\}}$.

37. 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 $\langle F_2, F_3, F_5 \rangle = S_n$.

38. *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 rápido de cálculo de $(\frac{n}{q})$, cuando n es primo.

Por una parte, el automorfismo de Frobënius 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 Frobënius 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 Frobënius F_2 de K en 2 es la identidad cuando $\frac{\tilde{q}-1}{4}$ sea múltiplo de 2. Por tanto,

$$(\frac{2}{q}) = (-1)^{\frac{\tilde{q}-1}{4}} = (-1)^{\frac{\tilde{q}+1}{2} \cdot \frac{\tilde{q}-1}{4}} = (-1)^{\frac{\tilde{q}^2-1}{8}} = (-1)^{\frac{q^2-1}{8}}$$

5.12.4. Revestimientos ramificados de curvas

En esta sección 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 base, también lo es la métrica de la traza. Es decir, dado un morfismo de anillos $A \to C$, se verifica el diagrama 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 en B de modo 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.

39. Definición: Sea $\varphi : A \to B$ un revestimiento. Llamaremos diferente de B sobre A, $\mathrm{dif}_{B/A}$, al módulo definido por la sucesión exacta

$$B \xrightarrow{T_A} B^* \to \mathrm{dif}_{B/A} \to 0$$

40. Definición: Sea $\varphi : A \to B$ 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.

41. 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 base $A \to k(x)$ (donde $k(x)$ es el cuerpo residual de x). Pero en este caso la equivalencia $(\mathrm{dif}_{B/A})_x = 0 \Leftrightarrow (\mathrm{Disc}_{B/A})_x = 0$ es inmediata y la equivalencia $(\mathrm{dif}_{B/A})_x = 0 \Leftrightarrow (\Omega_{B/A})_x = 0$ es la proposición 2.3.28. □

42. 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.

43. 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).*

[3] Es consecuencia de que el núcleo del morfismo $f : \prod_i B_{a_i} \to \prod_{ij} B_{a_i a_j}$, $f((b_i)) = (c_{ij})_{ij}$ con $c_{ij} := b_i - b_j$, es la imagen del morfismo inyectivo $B \to \prod_i B$, $b \mapsto (b,\ldots,b)$, como puede probarse localizando en cada a_i (véase [23]). En el caso A íntegro, pruébelo el lector usando que $\bigcap_i A_{a_i} = A$.

Demostración. Escribamos $X = \operatorname{Spec} B$ e $Y = \operatorname{Spec} A$. 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, $\Lambda_A^r B \simeq A$ 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). □

5.12.5. Cálculos locales

A partir de ahora supondremos que $A \to B$ es un revestimiento entre dominios de Dedekind tal que el morfismo entre los cuerpos de fracciones, $\Sigma_A \hookrightarrow \Sigma_B$, es separable.

Consideremos el diagrama conmutativo definido por las polaridades de las métricas de la traza

$$\begin{array}{ccc} B & \xrightarrow{T_A} & B^* = \operatorname{Hom}_A(B,A) \\ \downarrow & & \downarrow \\ \Sigma_B & \xrightarrow{T_{\Sigma_A}} & \Sigma_B^* = \operatorname{Hom}_{\Sigma_A}(\Sigma_B, \Sigma_A) \end{array}$$

B^* se identifica, vía T_{Σ_A}, con el A-submódulo de Σ_B formado por las $f \in \Sigma_B$ tales que $T_{\Sigma_A}(f,B) = \operatorname{tr}(fB) \subseteq A$.

44. Teorema: *Si $B = A[\xi]$, entonces $A[\xi] = A[x]/(p(x))$, donde $p(x)$ es mónico (de grado $n = \dim_{\Sigma_A} \Sigma_B$), y B^* se identifica, vía la métrica de la traza, con el A-submódulo libre de Σ_B de base*

$$\frac{1}{p'(\xi)}, \frac{\xi}{p'(\xi)}, \ldots, \frac{\xi^{n-1}}{p'(\xi)}$$

siendo $p'(x)$ es la derivada de $p(x)$ respecto de x.

Demostración. Sabemos que B es un A-módulo localmente libre de rango n. Por Nakayama, $1, \xi, \ldots, \xi^{n-1}$ es una base, luego $A[\xi] = A[x]/(p(x))$, con $p(x)$ mónico de grado n (y como $\Sigma_B = \Sigma_A[x]/(p(x))$, $p(x) \in \Sigma_A[x]$ es un polinomio separable).

Sea $w_1, \ldots, w_n \in B^*$ la base dual de $1, \xi, \ldots, \xi^{n-1}$, que es base también de Σ_B^*. Escribamos

$$T_{\Sigma_A}\left(\frac{\xi^j}{p'(\xi)}\right) = \sum_i a_{ji} w_i = \sum_i \operatorname{tr}\left(\frac{\xi^j \xi^i}{p'(\xi)}\right) w_i, \text{ con } a_{ji} \in \Sigma_A$$

Para probar que $\frac{1}{p'(\xi)}, \frac{\xi}{p'(\xi)}, \ldots, \frac{\xi^{n-1}}{p'(\xi)}$ es base de 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 $\operatorname{tr}\left(\frac{\xi^j \xi^i}{p'(\xi)}\right) = \sum_s \frac{\alpha_s^{i+j}}{p'(\alpha_s)}$. 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

$$\operatorname{tr}\left(\frac{\xi^i \xi^j}{p'(\xi)}\right) = \sum_s \frac{\alpha_s^{i+j}}{p'(\alpha_s)} = \begin{cases} 1 & \text{si } i+j = n-1 \\ 0 & \text{si } i+j \le n-1 \end{cases}$$

Por tanto, $\det(a_{ji}) = \pm 1$ y hemos concluido.

□

45. Teorema: *Si A y B son locales (de ideales maximales $\mathfrak{m}'$ y $\mathfrak{m}$ respectivamente) y $A/\mathfrak{m}'$ es un cuerpo perfecto, entonces $B = A[\xi]$.*

Demostración. Denotemos $k = B/\mathfrak{m}$, $k' = A/\mathfrak{m}'$. Por ser B de Dedekind $\mathfrak{m}/\mathfrak{m}^2 = (\bar{f})$. Por otra parte, $B/\mathfrak{m}'B = B/\mathfrak{m}^r$ es una k'-álgebra completa, luego por el teorema de Cohen 4.4.22, podemos suponer que es una k-álgebra. Ahora es sencillo demostrar que el morfismo $k[x]/(x^r) \to B/\mathfrak{m}'B, x \mapsto f$ 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 $B = A[\xi]$. □

46. 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 es un anillo local de ideal maximal $\mathfrak{m}$ y que $A/\mathfrak{m}$ es un cuerpo perfecto. Entonces,* $\operatorname{dif}_{B/A}$ *es isomorfo a* $\Omega_{B/A}$.

Demostración. 1) Supongamos que $B = A[\xi] = A[x]/(p(x))$.

En este caso $\Omega_{B/A} = B/p'(\xi)B$ como B-módulos. Por otra parte, por el teorema 5.12.44, B^* es un A-módulo libre de base $\frac{1}{p'(\xi)}, \dots, \frac{\xi^{n-1}}{p'(\xi)}$, luego se tiene un diagrama conmutativo de filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & B^* & \longrightarrow & \operatorname{dif}_{B/A} & \longrightarrow & 0 \\ & & \wr\downarrow{\scriptstyle \cdot p'(\xi)} & & \wr\downarrow{\scriptstyle \cdot p'(\xi)} & & & & \\ 0 & \longrightarrow & p'(\xi)B & \longrightarrow & B & \longrightarrow & B/p'(\xi)B & \longrightarrow & 0 \end{array}$$

de donde se concluye.

2) Caso general.

Si A y B fuesen locales entonces por el teorema 5.12.45 estaríamos en el caso 1) y habríamos concluido. Veamos que completando ésta es la situación.

Tanto $\Omega_{B/A}$ como $\operatorname{dif}_{B/A}$ son A-módulos finito generados concentrados en el punto cerrado de A, luego son completos para la topología $\mathfrak{m}$-ádica. Por tanto, y por la estabilidad por cambio de base,

$$\Omega_{B/A} = \widehat{\Omega}_{B/A} = \Omega_{B/A} \otimes_A \widehat{A} = \Omega_{\widehat{B}/\widehat{A}}$$

y

$$\operatorname{dif}_{B/A} = \widehat{\operatorname{dif}}_{B/A} = \operatorname{dif}_{B/A} \otimes_A \widehat{A} = \operatorname{dif}_{\widehat{B}/\widehat{A}}$$

$\widehat{A} \to \widehat{B}$ 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 $\mathfrak{m}B = \mathfrak{m}_{x_1}^{n_1} \cdot \dots \cdot \mathfrak{m}_{x_r}^{n_r}$, donde $x_1, \dots, x_r$ son puntos cerrados de B. Por tanto,

$$\begin{aligned} \widehat{B} &= \varprojlim_n B/\mathfrak{m}^n B = \varprojlim_n \prod_{i=1}^r (B/\mathfrak{m}^n B)_{x_i} = \prod_{i=1}^r \varprojlim_n (B/\mathfrak{m}^n B)_{x_i} = \prod_{i=1}^r \varprojlim_n B/\mathfrak{m}_{x_i}^n \\ &= \prod_{i=1}^r \widehat{B}_{x_i} \end{aligned}$$

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 $\operatorname{dif}_{\widehat{B}/\widehat{A}} = \prod \operatorname{dif}_{\widehat{B}_{x_i}/\widehat{A}}$ y por tanto

$$\operatorname{dif}_{B/A} = \operatorname{dif}_{\widehat{B}/\widehat{A}} = \prod \operatorname{dif}_{\widehat{B}_{x_i}/\widehat{A}} \overset{1)}{=} \prod \Omega_{\widehat{B}_{x_i}/\widehat{A}} = \Omega_{\widehat{B}/\widehat{A}} = \Omega_{B/A}$$

□

5.13. Problemas

1. Pruébese que el anillo local de $k[x,y]$ en el origen es íntegramente cerrado pero no es un anillo de valoración.

2. 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 del anillo de valoración B, entonces $B/\mathfrak{p}_x$ 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 subanillos de valoración contenidos en $\mathcal{O}_v$ y los subanillos de valoración de $\mathcal{O}_v/\mathfrak{p}_v$.

3. Consideremos el morfismo $\mathbb{C}[x,y] \to \mathbb{C}[[\theta]]$, $x \mapsto \theta, y \mapsto sen\theta$. Demostrar que $\mathcal{O}_v = \mathbb{C}(x,y) \cap \mathbb{C}[[\theta]]$ es un anillo de valoración discreta, tal que $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{C}$. Explicar la frase "$v(p(x,y))$ es igual a la multiplicidad de intersección de $p(x,y) = 0$ con $y = senx$, en el origen".

4. Sea $\mathcal{O}_v$ un anillo de valoración discreta de $\mathbb{C}(x,y)$ trivial sobre $\mathbb{C}$.

   a) Demostrar 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, demostrar 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 $\mathfrak{m}_x = (x,y)$, demostrar 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 $n \in \mathbb{N}$. Demostrar 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 $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{C}$.

5. 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 $p(x,y)$. Demostrar que v extiende a una valoración de $\mathbb{C}(x,y)$.

6. Sea α un número irracional positivo. Demostrar que la aplicación $v : \mathbb{C}[x,y] \to \mathbb{Z} + \mathbb{Z}\alpha$, definida por $v(\sum c_{n,m} x^n y^m) = \min\{n + m\alpha | c_{n,m} \neq 0\}$ extiende a una valoración de $\mathbb{C}(x,y)$.

7. 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 sólo si $x = 0$.

   b) $f(xy) = f(x)f(y)$, para todo $x, y \in \Sigma$.

   c) $f(x+y) \leq C \max\{f(x), f(y)\}$ 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.)

[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.

8. 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]Demostrar que los $x \in K$ tales que $f(x) \neq \infty$ (es decir, valor finito) forman un subanillo de valoración de K.

9. Probar que $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ es un dominio de Dedekind.

10. Sea A un dominio de Dedekind, $x_1, \ldots, x_r \in \operatorname{Spec} A$ puntos cerrados y $n_1, \ldots, n_r \in \mathbb{N}$. Probar que existe $f \in A$, de modo que $v_{x_i}(f) = n_i$, para $1 \leq i \leq r$.

11. 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 0.3.69)

    b) Probar que M es isomorfo a la suma directa de su parte de torsión, un A-módulo libre y un ideal.

12. Demostrar 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).

13. Sea $\mathcal{O}$ un anillo local íntegro. Probar 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 $\mathcal{O}$.

14. Sea $\mathfrak{m}_{or} = (x) \subseteq k[x]$ y $\mathcal{O} := k[x]_{or}$. Sea $\Sigma := k(x^{1/n})_{n \in \mathbb{N}}$. Probar que no existe ningún anillo de valoración discreta de Σ que domine a $\mathcal{O}$.

15. 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, $A \hookrightarrow \operatorname{Hom}_A(I, I) \hookrightarrow \bar{A}$.

    b) Si $0 \neq I \subset A$ es un ideal radical, probar que $\operatorname{Hom}_A(I, A) \cap \bar{A} = \operatorname{Hom}_A(I, I)$.

16. Sea A un anillo noetheriano íntegro y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. Sea $Y \subset \operatorname{Spec} A$ 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 $h = \frac{f}{g} \in \bar{A}$, probar que $(\operatorname{Anul}(hA/(hA \cap A)))_0 = \{x \in \operatorname{Spec} A : h \notin A_x\} \subset Y$.

    b) Probar que existe $n \in \mathbb{N}$ de modo que $I^n \subset \operatorname{Anul}(hA/(hA \cap A))$.

    c) Probar que si $A = \operatorname{Hom}_A(I, I)$ entonces A es íntegramente cerrado en su cuerpo de fracciones.

17. Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra sobre un cuerpo algebraicamente cerrado. Probar 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.

18. Probar 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.

19. Probar 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.

20. Calcular los anillos de valoración del cuerpo de fracciones de $\mathbb{C}[x, y]/(y^2 - x^2 + x^3)$, que contengan a $\mathbb{C}$.

21. Calcular el cierre entero de $\mathbb{Z}[\sqrt[2]{5}]$.

[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.

22. Probar que el discriminante de todo cuerpo de números es congruente con $0, 1 \mod 4$.

    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 $\Delta = (P-N)^2 = (P+N)^2 - 4PN$.

23. 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 $c_1 \cdots c_n > |\det((a_{ij}))|$. Probar que existe $(m_1 \ldots, m_n) \in \mathbb{Z}^n \setminus \{0\}$ tal que

$$|\sum_j a_{ij} m_j| < c_i, \ \forall i$$

24. Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Probar 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 $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$.

25. 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

$$\prod_{y \in X_\infty} c_y^{\mathrm{gr}\, y} > (\frac{2}{\pi})^s \cdot Vol(\mathcal{O}_\infty / I)$$

    Probar que existe $0 \neq f \in I$, tal que $|f|_y < c_y$ para todo $y \in X_\infty$.

26. Sea K un cuerpo de números de anillo de enteros A. Probar que existe un ideal $\mathfrak{a} \subseteq A$ tal que $N(\mathfrak{a}) \leq \frac{d!}{d^d} \cdot (\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

27. Probar que el anillo de enteros de $\mathbb{Q}[\sqrt{n}]$ es un anillo de ideales principales, para $n = 5, 8, 11, -3, -4, -7, -8, -11$.

28. Probar que si $\dim_{\mathbb{Q}} K >> 0$ entonces $|\Delta_K| >> 0$.

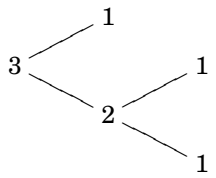
29. **La batalla de Hastings** (14 de octubre de 1066). "Los hombres de Harold permanecían bien juntos, como solían hacer, y formaban 13 escuadrones, con el mismo número de hombres en cada escuadrón, y hostigaban a los esforzados normandos que se aventuraban entrar en sus reductos; porque un único golpe 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?

30. 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 $c \circ \sigma \in P$. Probar 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 $\sigma \notin P$.

31. Desingularizar la curva $y^2 - x^7 = 0$. ¿Es esta curva birracional a la recta afín?

32. Calcular la multiplicidad de intersección de $y^2 - x^3 + y^4 = 0$ con $yx + x^3 + y^3 = 0$ en el origen.

33. Definir una curva plana que pase por el origen y cuyo árbol de explosión en el origen sea



34. Probar 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.

35. Calcular el grado del revestimiento $k[x] \to k[x,y]/(x^2 + y^2 - 1)$. Calcular los puntos en que ramifica.

36. Sean X e Y dos k-variedades algebraicas y $x \in X$ e $y \in Y$ dos puntos racionales. Probar que

$$m_{(x,y)}(X \times_k Y) = m_x(X) \cdot m_y(Y)$$

37. Probar 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.

38. Parametrizar la curva $x^6 - x^2y^3 - y^5 = 0$. Calcular sus soluciones racionales.

39. Probar el Teorema de Pascal: Si un hexágono está inscrito en una cónica irreducible, entonces los lados opuestos se cortan en puntos alineados.

40. Probar 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. Probar que los puntos $p_{ij} = R_{ij} \cap R_{ji}$ $(i < j)$ están alineados.

41. 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.

42. 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.

43. Demostrar que las tangentes a una cúbica irreducible plana en 3 puntos alineados cortan a la cúbica en otros 3 puntos alineados.

44. Demostrar 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.

45. Probar que una recta que pase por dos puntos de inflexión de una cúbica plana irreducible pasa por un tercer punto de inflexión.

46. Probar que si una cúbica pasa por ocho de los nueve puntos distintos de corte de otras dos cúbicas, entonces también pasa por el noveno.

47. 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.

48. 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. Probar que C_{n+m-3} pasa por el punto restante.

49. 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 $\gamma - 3$.

50. *a*) Sea C la cúbica plana $y^2 = x^2 + x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}_1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcular 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 $\mathbb{A}_1 \to C$, $x = t^2$, $y = t^3$.

51. Probar que si una cónica tiene un punto singular entonces no es irreducible.

52. Probar que si una cúbica plana tiene dos puntos singulares entonces no es irreducible.

53. Probar que si una cuártica plana tiene cuatro puntos singulares entonces no es irreducible.

54. Probar 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).

55. 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.

56. Calcular 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.

57. Sean $X=\mathrm{Spec}A$ e $Y=\mathrm{Spec}B$ variedades sobre un cuerpo algebraicamente cerrado. Sean $x\in X$, $y\in Y$ dos puntos cerrados. Probar que las multiplicidades cumplen

$$m_{(x,y)}(X\times Y)=m_x(X)\cdot m_y(Y)$$

58. Sea $X=\mathrm{Spec}\mathcal{O}_X$, supongamos que $\mathcal{O}_X$ es un anillo noetheriano e $I\subset\mathcal{O}_X$ 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, $B=\mathcal{O}_X\oplus I^m\oplus I^{2m}\oplus\ldots\subset B'=\mathcal{O}_X\oplus I\oplus I^2\oplus\ldots$, 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.

MANUALES UEX

Capítulo 6

Álgebra Conmutativa Homológica

6.1. 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 $k[x_1,\dots,x_n]$-módulos libres

$$0 \to k[x_1,\dots,x_n]\cdot \mathbf{x_1}\wedge\dots\wedge\mathbf{x_n} \xrightarrow{d_n} \cdots \to \bigoplus_{i_1<\cdots<i_r} k[x_1,\dots,x_n]\cdot \mathbf{x_{i_1}}\wedge\dots\wedge\mathbf{x_{i_r}} \xrightarrow{d_r}\cdots$$
$$\to k[x_1,\dots,x_n]\cdot \mathbf{x_1}\oplus\cdots\oplus k[x_1,\dots,x_n]\cdot \mathbf{x_n} \xrightarrow{d_1} k[x_1,\dots,x_n]\to k[x_1,\dots,x_n]/(x_1,\dots,x_n)\to 0$$

con $d_r(\mathbf{x_{i_1}}\wedge\dots\wedge\mathbf{x_{i_r}}) = \sum(-1)^{j-1}x_{i_j}\cdot\mathbf{x_{i_1}}\wedge\dots\wedge\widehat{\mathbf{x_{i_j}}}\wedge\dots\wedge\mathbf{x_{i_r}}$. No es difícil comprobar que esta sucesión de morfismos es exacta. Si $\mathcal{O}$ es un anillo local de ideal maximal $\mathfrak{m}$, $f_1,\dots,f_n$ es un sistema mínimo generador de $\mathfrak{m}$ y en la sucesión anterior sustituimos $k[x_1,\dots,x_n]$ 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 sólo 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 $\{f_1,\dots,f_n\}$ un sistema mínimo de parámetros (es decir, $(f_1,\dots,f_n)_0 = \{\mathfrak{m}\}$ 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 $\mathcal{O}/(f_1,\dots,f_n)$ es un $\mathcal{O}/(f_1,\dots,f_n)$-módulo inyectivo se dice que $\mathcal{O}$ es un anillo de Gorenstein. Probamos que dados $f_1,\dots,f_n\in\mathfrak{m}$, 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 $\mathcal{O}/(f_1,\dots,f_{i-1})$, 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.

6.2. 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*

$$\begin{array}{ccc} H(M') & \xrightarrow{\quad H(i)\quad} & H(M) \\ & {\scriptstyle\delta}\nwarrow \quad \nearrow{\scriptstyle H(p)} & \\ & H(M'') & \end{array}$$

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 $i(c') = \mathrm{d}\,c$. 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

$$\begin{array}{ccccc} c & & \xmapsto{\quad p\quad} & & c'' \\ \top & & & & \top \\ \downarrow{\scriptstyle \mathrm{d}} & & & & \downarrow{\scriptstyle \mathrm{d}} \\ c' & \xmapsto{\quad i\quad} & \mathrm{d}\,c & \xmapsto{\quad p\quad} & 0 \\ \top & & \top & & \\ \downarrow{\scriptstyle \mathrm{d}} & & \downarrow{\scriptstyle \mathrm{d}} & & \\ 0 & \xmapsto{\quad i\quad} & 0 & & \end{array}$$

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 $\operatorname{Im}\delta = \operatorname{Ker} H(i)$.

Dejamos como ejercicio probar el resto de la exactitud del triángulo.

□

4. Diagrama 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 $L = M \oplus N$ y $\mathrm{d}\colon L \to L$, $(m,n) \mapsto (0, f(m))$. Es inmediato ver que (L,d) es un módulo 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 módulos diferenciales y morfismos diferenciales. El triángulo exacto de cohomología dado en la proposición anterior, es justamente la sucesión exacta requerida. □

5. Definición: Un *complejo* de A-módulos K es un A-módulo diferencial y graduado $K = \bigoplus_{i\in\mathbb{Z}} K^i$, tal 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 verifica 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.

6. Ejemplo: Consideremos un poliedro r-dimensional de n vértices $\{a_1,\ldots,a_n\}$. 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 $S_p^\alpha = \{a_{i_0},\ldots,a_{i_p}\}$, con $\alpha = \{i_0,\ldots,i_p\}$. Denotemos por $M_p = \sum_\alpha \mathbb{Q}\cdot S_p^\alpha$ 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

$$\mathrm{d}_p\{a_{i_0},\ldots,a_{i_p}\} = \sum_{j=0}^{p} (-1)^j \{a_{i_0},\ldots,\widehat{a_{i_j}},\ldots,a_{i_p}\}$$

Se cumple que $\mathrm{d}_p \circ \mathrm{d}_{p+1} = 0$. La homología del complejo de cadenas sobre el poliedro es por definición, $H(M) = \bigoplus_{p=0}^{p} \mathrm{Ker}\,\mathrm{d}_p/\mathrm{Im}\,\mathrm{d}_{p+1}$.

La dimensión de los grupos de homología de M son invariantes topológicos esenciales del poliedro. Se llama característica del poliedro a $\chi(M) := \sum_{i=0}^{r} (-1)^i \dim_{\mathbb{Q}} H_i(M)$ y se verifica

$$\chi(M) = n^0 \text{ vértices } - n^0 \text{ aristas } + n^0 \text{ caras } + \ldots + (-1)^r n^0 \text{ r-símplices}$$

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 $\chi(M) = 2 - 2g$.

7. Definición: Un morfismo de complejos $f\colon K \to L$ 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.

Si $0 \to K' \to K \to K'' \to 0$ es una sucesión exacta de complejos, el triángulo de cohomología define la siguiente sucesión exacta larga de cohomología:

$$\cdots \to H^i(K'') \xrightarrow{\delta} H^{i+1}(K'') \to H^{i+1}(K) \to H^{i+1}(K'') \xrightarrow{\delta} H^{i+2}(K') \to \cdots$$

Dado un complejo K denotaremos por $K[n]$ el complejo definido por: $K[n]^p := K^{n+p}$ y $d_{K[n]} := (-1)^n d_K$.

8. Definición: Si $\{M_i, \mathrm{d}_i\}_{i\in I}$ son complejos, podemos definir la suma directa $\bigoplus_{i\in I} M_i$, que es un complejo con la graduación

$$(\bigoplus_i M_i)^n = \bigoplus_i M_i^n$$

y con la diferencial $\mathrm{d} = \oplus\, \mathrm{d}_i$.

Bicomplejos

9. Definición: Un bicomplejo es un objeto bigraduado

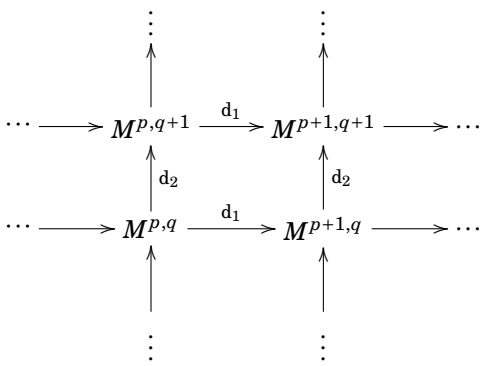
$$M = \underset{p,q\in\mathbb{Z}}{\oplus} M^{p,q}$$

dotado de dos diferenciales: una "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 $M^{p,\cdot} = \underset{q}{\oplus} M^{p,q}$, entonces M es un complejo con la graduación $M = \underset{p}{\oplus} M^{p,\cdot}$ y la diferencial d_1. Análogamente, si denotamos $M^{\cdot,q} = \underset{p}{\oplus} M^{p,q}$, entonces M es un complejo con la graduación $M = \underset{q}{\oplus} M^{\cdot,q}$ y la diferencial d_2. Denotaremos (M,d_1) y (M,d_2) estas dos estructuras de complejo de M, y $H^n_{\mathrm{d}_1}(M)$, $H^n_{\mathrm{d}_2}(M)$ 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 $M^{\cdot,q}$. Entonces $H^n_{d_1}(M)$ es un complejo con la graduación

$$H^n_{\mathrm{d}_1}(M) = \underset{q}{\oplus} H^n_{\mathrm{d}_1}(M^{\cdot,q})$$

y la diferencial d_2. Análogamente, $H^n_{\mathrm{d}_2}(M)$ es un complejo con la graduación

$$H^n_{\mathrm{d}_2}(M) = \underset{p}{\oplus} H^n_{\mathrm{d}_2}(M^{p,\cdot})$$

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

$$M^n = \underset{p+q=n}{\oplus} M^{p,q}$$

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 $\underset{p,q}{\oplus} (M^p \otimes N^q)$ 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

$$\mathrm{d}_1 \colon \mathrm{Hom}(M^{-q}, N^p) \to \mathrm{Hom}(M^{-q}, N^{p+1}), \quad f \mapsto \mathrm{d}_N \circ f$$
$$\mathrm{d}_2 \colon \mathrm{Hom}(M^{-q}, N^p) \to \mathrm{Hom}(M^{-q-1}, N^p), \quad f \mapsto (-1)^{q+1} f \circ \mathrm{d}_M$$

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 6.2.14).

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 $f \colon K \to L$ es cuasi-isomorfismo si y sólo 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 $\delta \colon H^n(\mathrm{Im}\,\mathrm{d}_1) \to H^n(\mathrm{Ker}\,\mathrm{d}_1)$ es isomorfismo. Dicho morfismo es: $\delta(\overline{\mathrm{d}_1 m_{p,q}}) = \overline{\mathrm{d}_1 m_{p,q} + (-1)^p \mathrm{d}_2 m_{p,q}}$. Vamos a ver que δ es un isomorfismo porque coincide "módulo graduados" con el morfismo $H^n(\mathrm{Im}\,\mathrm{d}_1) \to H^n(\mathrm{Ker}\,\mathrm{d}_1)$, $d_1 m \mapsto d_1 m$, (inducido por la inclusión natural $\mathrm{Im}\,\mathrm{d}_1 \to \mathrm{Ker}\,\mathrm{d}_1$), que es isomorfismo porque $H(H_{\mathrm{d}_1}(M)) = 0$ por hipótesis.

Como $\operatorname{Im} d_1$ y $\operatorname{Ker} d_1$ tienen diferencial horizontal nula, se verifica que

$$H^n(\operatorname{Im} d_1) = \oplus_p H^{n-p}_{d_2}((\operatorname{Im} d_1)^{p,\cdot}), \qquad H^n(\operatorname{Ker} d_1) = \oplus_p H^{n-p}_{d_2}((\operatorname{Ker} d_1)^{p,\cdot})$$

Consideremos en ambos las filtraciones

$$F_r := \oplus_{p\le r} H^{n-p}_{d_2}((\operatorname{Im} d_1)^{p,\cdot}), \qquad F'_r := \oplus_{p\ge r} H^{n-p}_{d_2}((\operatorname{Ker} d_1)^{p,\cdot})$$

Por ser M de diagonales acotadas por la izquierda, se obtiene que $F_r = F'_r = 0$ para $r << 0$. Tenemos que $H^n(\operatorname{Im} d_1) = \bigcup_{s=r}^{\infty} F_s$ y $H^n(\operatorname{Ker} d_1) = \bigcup_{s=r}^{\infty} F'_s$. F_s y F'_s son completos y separados, para todo $s \ge r$. El morfismo δ es compatible con las filtraciones, luego para que sea isomorfismo basta que lo sea el morfismo inducido en los graduados,

$$G(H^n(\operatorname{Im} d_1)) \xrightarrow{G(\delta)} G(H^n(\operatorname{Ker} d_1))$$

que viene dado por $G(\delta)(\overline{d_1 m}) = \overline{d_1 m}$, luego coincide con el morfismo inducido en los graduados por el morfismo $H(i)\colon H^n(\operatorname{Im} d_1) \to H^n(\operatorname{Ker} d_1)$ asociado a la inclusión $i\colon \operatorname{Im} d_1 \to \operatorname{Ker} d_1$. Este último es isomorfismo, como se deduce de la sucesión exacta

$$0 \to \operatorname{Im} d_1 \xrightarrow{i} \operatorname{Ker} d_1 \to H_{d_1}(M) \to 0$$

ya que $H_{d_1}(M)$ es acíclico por hipótesis. □

16. Teorema: *Sea $f : M \to N$ un morfismo entre bicomplejos. Supongamos que M y N son de diagonales acotadas por la izquierda. Si el morfismo inducido*

$$H_{d_2}(H_{d_1}(M)) \to H_{d_2}(H_{d_1}(N))$$

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

$$H_{d_1}(H_{d_2}(M)) \to H_{d_1}(H_{d_2}(N))$$

es isomorfismo entonces el morfismo $M^\cdot \to N^\cdot$ entre los complejos simples asociados es un cuasi-isomorfismo.

Demostración. Podemos considerar $f : M^{\cdot,\cdot} \to N^{\cdot,\cdot}$ como un tricomplejo de diferenciales, con las notaciones obvias, $d_1, d_2, d_3 = f$. Cuando consideremos la diferencial simple asociada a dos diferenciales la denotaremos como la suma de las dos diferenciales. Ahora ya, $H_{d_1}(f)\colon H_{d_1}(M) \to H_{d_1}(N)$ es un cuasi-isomorfismo $\iff 0 = H_{d_3+d_2}(\operatorname{Cono}(H_{d_1}(f))) = H_{d_3+d_2}(H_{d_1}(\operatorname{Cono}(f))) \Rightarrow 0 = H_{(d_3+d_2)+d_1}(\operatorname{Cono}(f)) = H_{d_3+(d_2+d_1)}(\operatorname{Cono}(f)) \iff f : M \to N$ 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 $H^i_{d_1}(M) = 0$ para todo $i \ne n$ (respectivamente, $H^i_{d_2}(M) = 0$ para todo $i \ne n$), entonces $H^{i+n}(M^\cdot) = H^i_{d_2}(H^n_{d_1}(M))$ (respectivamente, $H^{i+n}(M^\cdot) = H^i_{d_1}(H^n_{d_2}(M))$).*

Demostración. Dado un bicomplejo B, sea $B^{\le n,\cdot}$ el bicomplejo

$$B^{\le n,\cdot} = \cdots \to B^{n-2,\cdot} \to B^{n-1,\cdot} \to \operatorname{Ker} d_1^n \to 0 \cdots$$

Es inmediato que

$$H^i_{d_1}(B^{\le n,\cdot}) = \begin{cases} H^i_{d_1}(B^\cdot) \text{ para } i \le n \\ 0 \quad \text{para } i > n \end{cases}$$

Por las hipótesis y el teorema anterior los morfismos

$$H^n_{d_1}(M)[-n] \leftarrow M^{\le n,\cdot} \to M^\cdot$$

son cuasi-isomorfismos, luego $H^i(M^\cdot) = H^i(H^n_{d_1}(M)[-n]) = H^{i-n}_{d_2}(H^n_{d_1}(M))$. □

6.3. 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 $\mathrm{Tor}_i(N,M) = H_i(L_\cdot \otimes M)$, y se denomina i-ésimo módulo de torsión de N y M. Cuando queramos explicitar el anillo, escribiremos $\mathrm{Tor}_i = \mathrm{Tor}_i^A$.

3. Proposición: $\mathrm{Tor}_i(N,M)$ *no depende de la resolución de* N *escogida y* $\mathrm{Tor}_i(N,M) = \mathrm{Tor}_i(M,N)$.

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 $i \neq 0$ 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 6.2.17, tenemos que

$$H_i(L_\cdot \otimes M) = H_i(L_\cdot \otimes L'_\cdot) = H_i(N \otimes L'_\cdot)$$

□

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 $0 \to N_1 \to N_2 \to N_3 \to 0$, 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

$$\cdots \to \mathrm{Tor}_i(N_1,M) \to \mathrm{Tor}_i(N_2,M) \to \mathrm{Tor}_i(N_3,M) \to \mathrm{Tor}_{i-1}(N_1,M) \to \cdots$$
$$\cdots \to \mathrm{Tor}_1(N_1,M) \to \mathrm{Tor}_1(N_2,M) \to \mathrm{Tor}_1(N_3,M) \to N_1 \otimes M \to N_2 \otimes M \to N_3 \otimes M \to 0$$

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 sólo si $\mathrm{Tor}_1(M,A/I) = 0$ para todo ideal I. Por último, $\mathrm{Tor}_1(M,A/I) = 0$ si y sólo 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 sólo 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

$$\mathrm{Tor}_i^A(M,N) \otimes_A B = H_i(L_\cdot \otimes_A N) \otimes_A B = H_i(L_\cdot \otimes_A N \otimes_A B) = H_i((L_\cdot \otimes_A B) \otimes_B (N \otimes_A B)) = \mathrm{Tor}_i^B(M \otimes_A B, N \otimes_A B)$$

□

8. 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 epiyecciones.

Se verifican trivialmente las siguientes propiedades:

a) El producto directo de módulos inyectivos es inyectivo.

b) Un sumando directo de un módulo inyectivo es también inyectivo.

9. Criterio del ideal para módulos inyectivos: *Un A-módulo M es inyectivo si y sólo si para todo ideal $I \subset A$ el morfismo inducido* $\mathrm{Hom}_A(A,M) \to \mathrm{Hom}_A(I,M)$ *es epiyectivo.*

Demostración. El directo es obvio. Probemos el recíproco. Dada una inyección $N_1 \hookrightarrow N_2$ (que pensamos como inclusión) y un morfismo $f: N_1 \to M$, tenemos que probar que f extiende a N_2. Consideremos el conjunto, X, de parejas (N', f'), donde N' es un submódulo de N_2 que contiene a N_1 y $f' \in \mathrm{Hom}_A(N', M)$ es una extensión de f. Consideremos en X la relación de orden: $(N', f') \leq (N'', f'')$ si $N' \subseteq N''$ y $f''_{|N'} = f'$. Por el lema de Zorn existen en X elementos maximales. Sea (N', f') un elemento maximal. Si $N' \neq N_2$, sea $n \in N_2 \backslash N'$. Sea $I := \{a \in A : a \cdot n \in N'\}$ y $g: I \to M$ el morfismo de A-módulos definido por $g(i) := f'(i \cdot n)$, para todo $i \in I$. Sea $g': A \to M$ tal que $g'_{|I} = g$. Por último, el morfismo $f'': N' + \langle n \rangle \to M$, definido por $f''(n' + an) = f'(n') + g'(a)$, está bien definido y $f''_{|N'} = f'$. Luego, $(N' + \langle n \rangle, f'') > (N', f')$ y hemos llegado a contradicción. Por tanto, $N' = N_2$ y f extiende a N_2. □

10. Definición: Sea A un anillo íntegro. Un A-módulo M se dice de división si para todo $a \in A$ no nulo, el morfismo $M \xrightarrow{\cdot a} M$ es epiyectivo.

11. Teorema: *Si A es íntegro, todo A-módulo inyectivo es de división. Si A es un dominio de ideales principales, entonces un módulo es inyectivo si y sólo si es de división.*

Demostración. Dado el morfismo inyectivo $A \xrightarrow{a\cdot} A$, si tomamos $\mathrm{Hom}_A(\ ,M)$ obtenemos el morfismo $M \xrightarrow{a\cdot} M$. Por tanto, si M es un A-módulo inyectivo, entonces los morfismos $M \xrightarrow{a\cdot} M$ son epiyectivos, luego M es de división. Dado un ideal de $I = aA$ de un anillo de ideales principales, la inclusión $I \subseteq A$ equivale al morfismo $A \xrightarrow{a\cdot} A$, por tanto, si M es división al tomar $\mathrm{Hom}_A(\ ,M)$ obtenemos un epimorfismo, luego por el criterio del ideal para módulos inyectivos, M es un módulo inyectivo.

□

Así, por ejemplo, $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son $\mathbb{Z}$-módulos inyectivos, y por tanto $R = \mathbb{Q} \oplus \mathbb{Q}/\mathbb{Z}$ es inyectivo.

Denotemos por $M^* = \mathrm{Hom}_{\mathbb{Z}}(M,R)$, para cada A-módulo M. Observemos que todo $\mathbb{Z}$-módulo cíclico se inyecta en R: $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$, $\bar{1} \mapsto \overline{1/n}$.

12. Lema: *El morfismo natural $M \to M^{**}$ es inyectivo.*

Demostración. Tenemos que ver que dado $m \in M$ existe $w \in M^*$ tal que $w(m) \neq 0$. Consideremos una inmersión $\mathbb{Z} \cdot m \hookrightarrow R$. Por ser R inyectivo, extiende a un morfismo de $\mathbb{Z}$-módulos $w: M \to R$, que no es nulo sobre m. □

El funtor $\mathrm{Hom}_{\mathbb{Z}}(-,R)$ es exacto y transforma límites inductivos en límites proyectivos, luego por el teorema de representabilidad es representable. Aplicando el funtor a A, se obtiene que el representante es

$$A^* = \mathrm{Hom}_{\mathbb{Z}}(A,R)$$

que ha de ser un A-módulo inyectivo. Explícitamente,

$$\begin{array}{rcl} \mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbb{Z}}(A,R)) & = & \mathrm{Hom}_{\mathbb{Z}}(M,R) \\ \phi & \longmapsto & \tilde{\phi}: m \mapsto \phi(m)(1) \\ \tilde{f}: \tilde{f}(m)(a) = f(am) & \longmapsto & f \end{array}$$

13. Teorema: *Todo módulo es submódulo de un inyectivo. En lenguaje categorial: la categoría de módulos sobre un anillo tiene suficientes inyectivos.*

Demostración. Sea M un A-módulo. Consideremos una epiyección $\oplus A \to M^* \to 0$. 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, la composición de los morfismos $M \hookrightarrow M^{**} \hookrightarrow \prod A^*$ es inyectiva. □

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

$$H^i(\mathrm{Hom}(P_\cdot, M)) \overset{6.2.17}{=} H^i(\mathrm{Hom}^\cdot(P_\cdot, I^\cdot)) \overset{6.2.17}{=} H^i(\mathrm{Hom}(N, I^\cdot))$$

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

$$\cdots \to \mathrm{Ext}^i(N_3,M) \to \mathrm{Ext}^i(N_2,M) \to \mathrm{Ext}^i(N_1,M) \to \mathrm{Ext}^{i+1}(N_3,M) \to \cdots$$

14. 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 A.*
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 y de la sucesión exacta larga de extens. Si A 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 □

15. 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,

$$\begin{aligned}\mathrm{Ext}^i_A(M,N)\otimes_A B &= H^i(\mathrm{Hom}_A(L_\cdot,N))\otimes_A B = H^i(\mathrm{Hom}_A(L_\cdot,N)\otimes_A B) = H^i(\mathrm{Hom}_B(L_\cdot\otimes_A B, N\otimes_A B))\\ &= \mathrm{Ext}^i_B(M\otimes_A B, N\otimes_A B)\end{aligned}$$

□

16. 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. □

6.4. Complejo de Koszul

Sea $\mathscr{O}$ un anillo local y $a_1,\dots,a_r$ elementos no invertibles de $\mathscr{O}$. Sea L un $\mathscr{O}$-módulo libre de base $e_1,\dots,e_r$, y $w: L\to\mathscr{O}$ el morfismo $w(e_i)=a_i$.

1. Definición: Llamaremos complejo de Koszul respecto de $a_1,\dots,a_r$ al complejo de $\mathscr{O}$-módulos

$$K_\cdot(a_1,\dots,a_r,\mathscr{O}) := \bigoplus_{i=0}^{r}\Lambda^i L,$$

cuya diferencial $d:\Lambda^j L\to\Lambda^{j-1}L$, de grado -1, es la contracción interior con w, es decir,

$$d(e_{i_1}\wedge\cdots\wedge e_{i_p}) := \sum_{j=1}^{p}(-1)^{j-1}a_{i_j}e_{i_1}\wedge\cdots\wedge\widehat{e_{i_j}}\wedge\cdots\wedge e_{i_p}$$

Para cada complejo $M_\cdot$ de $\mathscr{O}$-módulos, denotaremos $M_\cdot(a_1,\dots,a_r)$ al complejo $M_\cdot\otimes_{\mathscr{O}}K_\cdot(a_1,\dots,a_r,\mathscr{O})$. Obsérvese que $K_\cdot(a_1,\dots,a_r,\mathscr{O}) = K_\cdot(a_1,\mathscr{O})\otimes_{\mathscr{O}}\cdots\otimes_{\mathscr{O}}K_\cdot(a_r,\mathscr{O})$. Observemos también que

$$\begin{aligned}H_0(K_\cdot(a_1,\dots,a_r,\mathscr{O})) &= \mathscr{O}/(a_1\dots,a_r)\\ H_r(K_\cdot(a_1,\dots,a_r,\mathscr{O})) &= \{a\in\mathscr{O} : a\cdot a_i = 0 \text{ para todo } i\}\end{aligned}$$

2. Teorema: *Sea $M_\cdot$ un complejo de $\mathscr{O}$-módulos y $x\in\mathscr{O}$. Escribamos $M_\cdot(x) = M\otimes_{\mathscr{O}}\mathscr{O}(x) = M\oplus M\cdot\mathbf{x}$. Entonces, la sucesión de complejos:*

$$0\to M_\cdot \xrightarrow{i} M_\cdot(x)\xrightarrow{\pi} M_\cdot[-1]\to 0,\quad i(a)=a,\ \pi(a+b\mathbf{x})=b,$$

es exacta. 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 $\delta: H_p(M_\cdot)\to H_p(M_\cdot)$ es multiplicar por $(-1)^p x$.

Demostración. Veamos que δ es multiplicar por $(-1)^p x$. Dado $b\in M_p$ tal que $db=0$, tenemos

$$\begin{array}{ccccc} a+b\mathbf{x} & & \xrightarrow[\pi]{} & & b \\ \downarrow & & & & \downarrow \\ da+(-1)^p xb & \longrightarrow & da+(-1)^p xb & \longrightarrow & 0 \end{array}$$

luego $\delta(\bar b) = (-1)^p x\bar b$. □

3. Definición: Sean $a_1,\dots,a_r$ elementos no invertibles de un anillo local $\mathscr{O}$. Diremos que $a_1,\dots,a_r$ es una sucesión regular si a_i no divide al cero en $\mathscr{O}/(a_1,\dots,a_{i-1})$, para todo i.

4. Teorema: *Sea $\mathcal{O}$ local y noetheriano y $a_1,\dots,a_r$ elementos no invertibles de $\mathcal{O}$. Las siguientes condiciones son equivalentes:*

1. *$a_1,\dots,a_r$ es una sucesión regular.*
2. *$H_i(K_\cdot(a_1,\dots,a_r))=0$, para todo $i>0$.*
3. *$H_1(K_\cdot(a_1,\dots,a_r))=0$.*

Demostración. 1. $\Rightarrow$ 2. Procedemos por inducción sobre r. Si $r=1$, entonces $H_1(K_\cdot(a_1,\mathcal{O}))=\{a\in\mathcal{O}: a\cdot a_1=0\}=0$ y concluimos. Sea $r>1$. Por el teorema anterior, y por inducción, tenemos

$$\begin{array}{ccccc} H_p(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) & \to & H_p(K_\cdot(a_1,\dots,a_r,\mathcal{O})) & \to & H_{p-1}(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) \\ \| & & & & \| \\ 0 & & & & 0 \end{array}$$

para $p>1$, luego $H_p(K_\cdot(a_1,\dots,a_r,\mathcal{O})=0$ para $p>1$. Para $p=1$ tenemos

$$\begin{array}{ccccccc} & 0\to H_1(K_\cdot(a_1,\dots,a_r,\mathcal{O})) & \to & H_0(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) & \xrightarrow{\cdot a_r} & H_0(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) \\ (*) & & & \| & & \| \\ & & & \mathcal{O}/(a_1,\dots,a_{r-1}) & & \mathcal{O}/(a_1,\dots,a_{r-1}) \end{array}$$

luego $H_1(K_\cdot(a_1,\dots,a_r,\mathcal{O}))=0$, por la regularidad de la sucesión.

2. $\Rightarrow$ 3. Evidente

3. $\Rightarrow$ 1. Por el teorema anterior tenemos la sucesión

$$\begin{array}{ccccc} H_1(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) & \xrightarrow{\cdot -a_r} & H_1(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O})) & \to & H_1(K_\cdot(a_1,\dots,a_r,\mathcal{O})) \\ & & & & \| \\ & & & & 0 \end{array}$$

Por Nakayama, $H_1(K_\cdot(a_1,\dots,a_{r-1},\mathcal{O}))=0$. Por inducción sobre r, $a_1,\dots,a_{r-1}$ es una sucesión regular. Para concluir que $a_1,\dots,a_r$ es regular basta observar la sucesión $(*)$. □

Dado que $K_\cdot(a_1,\dots,a_r,\mathcal{O})=K_\cdot(a_1,\mathcal{O})\otimes\cdots\otimes K_\cdot(a_r,\mathcal{O})$, se obtiene como corolario de este teorema que el que $a_1,\dots,a_r$ sea una sucesión regular no depende del orden en que sean escritos $a_1,\dots,a_r$.

5. Proposición: *Si $\{a_1,\dots,a_r\}$ es una sucesión regular del anillo local noetheriano $\mathcal{O}$ e $I=(a_1,\dots,a_r)$, entonces I/I^2 es un $\mathcal{O}/I$-módulo libre de rango r.*

Demostración. El complejo de Koszul asociado a $\{a_1,\dots,a_r\}$ es acíclico en grado mayor que cero, luego tenemos la sucesión exacta

$$\Lambda^2 L\to L\to I\to 0$$

Tensando por $\otimes_{\mathcal{O}}\mathcal{O}/I$, obtenemos que $L\otimes_{\mathcal{O}}\mathcal{O}/I\simeq I/I^2$, pues el morfismo $(\Lambda^2 L)\otimes_{\mathcal{O}}\mathcal{O}/I\to L\otimes_{\mathcal{O}}\mathcal{O}/I$ es nulo. □

6. Observación: En las hipótesis de la proposición 6.4.5, 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 4.3.9 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 4.3.9, 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 $f:\operatorname{Spec}B\to\operatorname{Spec}A$ 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 6.4.7. □

Sabemos por 4.4.25 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. 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 6.4.5, $(\Delta/\Delta^2)_x = (\Omega_{A/k})_x$ 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. □

6.5. Teorema de Serre para los anillos regulares

En toda la sección, $\mathscr{O}$ denota un anillo local noetheriano de maximal $\mathfrak{m}$.

1. Proposición: *Sea M un $\mathscr{O}$-módulo finito generado. Entonces,*

$$\operatorname{Tor}_1(M, \mathscr{O}/\mathfrak{m}) = 0 \Leftrightarrow M \text{ es libre}$$

Demostración. Sean L un módulo libre y $\pi : L \to M$ un morfismo tal que $\bar{\pi} : L \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} \to M \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m}$ 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 $\mathscr{O}/\mathfrak{m}$ obtenemos una sucesión exacta

$$0 \to \operatorname{Tor}_1(M, \mathscr{O}/\mathfrak{m}) \to N \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} \to L \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} \xrightarrow{\sim} M \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} \to 0$$

Luego $N \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} = 0$, y por el lema de Nakayama $N = 0$ y $L \simeq M$. □

2. Corolario: *Sea M un $\mathscr{O}$-módulo finito generado. Si $\operatorname{Tor}_{n+1}(M, \mathscr{O}/\mathfrak{m}) = 0$, 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 $\operatorname{Tor}_i(\operatorname{Ker} d_j, \mathscr{O}/\mathfrak{m}) = \operatorname{Tor}_{i+1}(\operatorname{Ker} d_{j-1}, \mathscr{O}/\mathfrak{m})$, para $i > 0$. Por tanto,

$$\operatorname{Tor}_1(\operatorname{Ker} d_{n-1}, \mathscr{O}/\mathfrak{m}) = \operatorname{Tor}_2(\operatorname{Ker} d_{n-2}, \mathscr{O}/\mathfrak{m}) = \cdots = \operatorname{Tor}_n(\operatorname{Ker} d_0, \mathscr{O}/\mathfrak{m}) = \operatorname{Tor}_{n+1}(M, \mathscr{O}/\mathfrak{m}) = 0$$

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 $\mathscr{O}$-módulo finito generado. Se cumple que*

1. $\operatorname{dimpro} M = \sup \{i : \operatorname{Tor}_i(M, \mathscr{O}/\mathfrak{m}) \neq 0\}$.
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 6.5.2, 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 $\mathrm{dimpro}\,M=\sup\{i:\mathrm{Tor}_i(M,\mathscr{O}/\mathfrak{m})\neq 0\}\leq\mathrm{dimpro}\,\mathscr{O}/\mathfrak{m}$, se concluye que $\mathrm{dimglo}\,\mathscr{O}=\mathrm{dimpro}\,\mathscr{O}/\mathfrak{m}$.

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 verifica*

$$\mathrm{Tor}_n^A(M,N)=\mathrm{Tor}_n^{A/xA}(M/xM,N)$$

para todo $n\geq 0$.

Demostración. Sea $L_\cdot$ una resolución de M por módulos libres. Consideremos el bicomplejo B, $L_\cdot\overset{x\cdot}{\hookrightarrow}L_\cdot$, es decir, $B=\mathrm{Cono}(x\cdot)$. Como $H^n_{d_1}(B)=0$, para $n\neq 0$ y $H^0_{d_1}(B)=L_\cdot/x\cdot L_\cdot$ entonces $H(B)=H(L_\cdot/x\cdot L_\cdot)$, por 6.2.17. Como $H_{d_2}(B)=0$, para $n\neq 0$ y $H^0_{d_2}(B)=[M\overset{x\cdot}{\hookrightarrow}M]$, entonces $H(B)=H([M\overset{x\cdot}{\hookrightarrow}M])=M/xM$, por 6.2.17. Por tanto, $H(L_\cdot/x\cdot L_\cdot))=M/xM$ y $L_\cdot/xL_\cdot$ es una resolución de M/xM por A/xA-módulos libres. Como N es un A/xA-módulo, se verifica $L_\cdot\otimes_A N=L_\cdot/xL_\cdot\otimes_{A/xA}N$, luego

$$\mathrm{Tor}_n^A(M,N)=H_n(L_\cdot\otimes_A N)=H_n(L_\cdot/xL_\cdot\otimes_{A/xA}N)=\mathrm{Tor}_n^{A/xA}(M/xM,N)$$

□

8. Teorema de Serre: *Sea $\mathscr{O}$ un anillo local noetheriano. $\mathscr{O}$ es regular si y sólo si tiene dimensión global finita. Además, si $\mathscr{O}$ es regular, su dimensión global coincide con su dimensión de Krull.*

Demostración. Sea $\mathscr{O}$ regular de ideal maximal $\mathfrak{m}$, y $x_1,\ldots,x_n$ un sistema mínimo de parámetros que generen $\mathfrak{m}$. El complejo de Koszul asociado, $K_\cdot$, es una resolución de $\mathscr{O}/\mathfrak{m}$ por $n+1$ libres. Además, $\mathrm{Tor}_n(\mathscr{O}/\mathfrak{m},\mathscr{O}/\mathfrak{m})=H_n(K_\cdot\otimes\mathscr{O}/\mathfrak{m})$ y es fácil ver que éste último vale $\mathscr{O}/\mathfrak{m}$. En conclusión, $\mathrm{dimglo}\,\mathscr{O}=\mathrm{dimpro}\,\mathscr{O}/\mathfrak{m}=n=\dim\mathscr{O}$.

Veamos el recíproco. Lo vamos a demostrar por inducción sobre $\dim\mathscr{O}$.

Si $\mathrm{dimglo}\,\mathscr{O}=0$, entonces $\mathscr{O}=\mathscr{O}/\mathfrak{m}$ y es regular. Podemos suponer que $\mathrm{dimglo}\,\mathscr{O}>0$. 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 $0\neq a\in\mathscr{O}$ tal que $a\cdot\mathfrak{m}=0$. Sea $L_{n-2}\overset{d_{n-2}}{\to}L_{n-3}\cdots\to L_0\to\mathscr{O}/\mathfrak{m}\to 0$ una resolución de $\mathscr{O}/\mathfrak{m}$ por módulos libres finito generados. Sean L_{n-1} un libre finito generado y $L_{n-1}\overset{d_{n-1}}{\to}\mathrm{Ker}\,d_{n-2}$ una epiyección que sea isomorfismo al hacer módulo $\mathfrak{m}$. Entonces $0\to\mathrm{Ker}\,d_{n-1}\to L_{n-1}\to L_{n-2}\to\cdots\to L_0\to\mathscr{O}/\mathfrak{m}\to 0$ es una resolución por libres de $\mathscr{O}/\mathfrak{m}$ (por 6.5.2, ya que $\mathrm{Tor}_1(\mathrm{Ker}\,d_{n-1},\mathscr{O}/\mathfrak{m})=\mathrm{Tor}_{n+1}(\mathscr{O}/\mathfrak{m},\mathscr{O}/\mathfrak{m})=0$) 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.

Sea $x\in\mathfrak{m}\backslash\mathfrak{m}^2$ un no divisor de cero. Existe: Sean $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, 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 $\mathscr{O}/x\mathscr{O}$ es regular, porque como $x\in\mathfrak{m}\backslash\mathfrak{m}^2$, entonces $\mathscr{O}$ sería regular. Por la hipótesis de inducción sobre $\dim\mathscr{O}$, basta demostrar que $\mathscr{O}/x\mathscr{O}$ tiene dimensión global finita. Para ello

basta demostrar 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, por el lema, $\mathrm{Tor}_i^{\mathcal{O}}(\mathfrak{m}, \mathcal{O}/\mathfrak{m}) = \mathrm{Tor}_i^{\mathcal{O}/x\mathcal{O}}(\mathfrak{m}/x\mathfrak{m}, \mathcal{O}/\mathfrak{m})$.

□

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 6.3.7. □

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 sólo 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 sólo 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 6.5.14, 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, tenemos $0 \to L_{m,f} \to L_{m-1,f} \to \cdots \to L_{0,f} \to \mathfrak{p}\mathcal{O}_f \to 0$, resolución por libres de $\mathfrak{p}\mathcal{O}_f$. 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 $\mathcal{O}$ es DFU. En efecto, sea $\mathfrak{p}$ un ideal primo de altura 1 de $\mathcal{O}$. Si $f \in \mathfrak{p}$, entonces $\mathfrak{p} = (f)$. Si $f \notin \mathfrak{p}$, entonces $\mathfrak{p}\mathcal{O}_f$ es principal (pues $\mathcal{O}_f$ es DFU). Escribamos $\mathfrak{p}\mathcal{O}_f = a \cdot \mathcal{O}_f$, con $a \in \mathcal{O}$. Por noetherianidad podemos escoger a de modo que no sea divisible por f en $\mathcal{O}$. Si $b \in \mathfrak{p}$, entonces para cierto $n \in \mathbb{N}$ y $s \in \mathcal{O}$, $b \cdot f^n = a \cdot s$. Ahora bien, como a no es divisible por f, que es primo, se tendrá que $\frac{s}{f^n} \in \mathcal{O}$ y $b = a \cdot \frac{s}{f^n}$. En conclusión, $\mathfrak{p} = (a)$ es principal, luego $\mathcal{O}$ es DFU por 6.5.14.

□

6.6. 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 $a_1,\dots,a_n \in A$ es una sucesión M-regular si a_{i+1} no es divisor de cero en $M/(a_1,\dots,a_i)M$.

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. Escribamos $I \subseteq \bigcup_{i=1}^{r} \mathfrak{p}_{x_i}$. Si I está incluido en la unión de $r-1$ de los ideales primos $\mathfrak{p}_{x_i}$, quedémosnos con estos $r-1$ ideales primos. Reiteremos este proceso el número máximo de veces que podamos. Podemos suponer que $I \subseteq \bigcup_{i=1}^{r} \mathfrak{p}_{x_i}$ y que I no está incluido en alguna unión de $r-1$ de los ideales primos $\mathfrak{p}_{x_i}$. Tenemos que probar que $r=1$. Supongamos que $r>1$. Sea $f_j \in I$, tal que $f_j \notin \cup_{i\neq j}\mathfrak{p}_{x_i}$. Observemos que f_j se anula en x_j y no se anula en x_i, para $i \neq j$. Sea $g_j := \prod_{i\neq j} f_i \in I$, que se anula en todos los x_i, salvo en x_j. Entonces, $f = \sum_i g_i \in I$ y no se anula en ningún x_i, es decir, $f \notin \bigcup_{i=1}^{r} \mathfrak{p}_{x_i}$ y hemos llegado a contradicción. □

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 sólo si existe algún elemento M-regular en I.*

Demostración. $\mathrm{Hom}_A(A/I,M) = \{m \in M : I\cdot m = 0\}$, luego 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 $I \subseteq \cup_j \mathfrak{p}_j$, 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* $\mathrm{Ext}^i_A(A/I,M) = 0$*, para* $0 \leq i < r$.

Demostración. Supongamos que $\mathrm{Ext}^i_A(A/I,M) = 0$ para todo $0 \leq i < r$. Como $\mathrm{Hom}_A(A/I,M) = 0$, 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

$$0 = \mathrm{Ext}^i_A(A/I,M) \to \mathrm{Ext}^i_A(A/I,M/a_1M) \to \mathrm{Ext}^{i+1}_A(A/I,M/a_1M) = 0$$

para todo $i+1 < r$. Por lo tanto $\mathrm{Ext}^i_A(A/I,M/a_1M) = 0$ para $0 \leq i < r-1$. 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

$$0 = \mathrm{Ext}^j_A(A/I,M/a_1M) \to \mathrm{Ext}^{j+1}_A(A/I,M) \xrightarrow{a_1\cdot} \mathrm{Ext}^{j+1}_A(A/I,M)$$

para $-1 \leq j < r-1$. Por tanto, la aplicación $\mathrm{Ext}^{j+1}_A(A/I,M) \xrightarrow{a_1\cdot} \mathrm{Ext}^{j+1}_A(A/I,M)$ es inyectiva para $0 \leq j+1 < r$. Ahora bien, $\mathrm{Ext}^{j+1}_A(A/I,M)$ está anulado por I (como se observa al calcular los extens resolviendo M por inyectivos) y $a_1 \in I$, luego $\mathrm{Ext}^j_A(A/I,M) = 0$ para $0 \leq j < r$. □

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 $M/(a_1,\dots,a_n)M \neq 0$.

Sea $\mathcal{O}$ local de ideal maximal $\mathfrak{m}$ y M un $\mathcal{O}$-módulo finito generado. Entonces, $\mathrm{prof} M = n$ si y sólo si $\mathrm{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},M) = 0$ para $0 \leq i < n$ y $\mathrm{Ext}^n_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},M) \neq 0$.

6. Observación: En el 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 sólo 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

$$\underset{\|}{\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}, a), M)} \to \operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) \xrightarrow{a\cdot} \operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, M) \to \underset{\|}{\operatorname{Ext}^{i+1}_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p}, a), M)}$$
$$0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 0$$

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 sólo 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; es más, si $\mathfrak{p}$ es un ideal primo divisor de cero, 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 sólo 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 $\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}, \mathcal{O}) \neq 0$. Por el teorema anterior, $0 \geq \operatorname{prof} \mathcal{O} - \dim \mathcal{O}/\mathfrak{p} = \dim \mathcal{O} - \dim \mathcal{O}/\mathfrak{p}$ 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 sólo si $(a)_0 \subset \operatorname{Spec}\mathcal{O}$ no es un divisor topológico, es decir, no existe un cerrado propio $C \subset \operatorname{Spec} A$ tal que $(a)_0 \cup C = \operatorname{Spec}\mathcal{O}$.

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 sólo si todo sistema de parámetros $\{f_1,\dots,f_n\}$ ($(f_1,\dots,f_n)_0 = \{x\}$) es una sucesión regular.*

Demostración. Como $\mathcal{O}/(f_1,\dots,f_n)$ es de dimensión cero es de Cohen-Macaulay. Por tanto, si $\{f_1,\dots,f_n\}$ es una sucesión regular $\mathcal{O}$ es de Cohen-Macaulay.

Supongamos ahora que $\mathcal{O}$ es Cohen-Macaulay. Como $\dim \mathcal{O} = n$ y $\dim \mathcal{O}/(f_1,\dots,f_n) = 0$, entonces $\dim \mathcal{O}/(f_1,\dots,f_i) = \dim \mathcal{O} - i$. 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 $\operatorname{Spec} A$ es Cohen-Macaulay) si A es noetheriano y A_x es Cohen-Macaulay para todo $x \in \operatorname{Spec} A$.

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 sólo si B es de Cohen-Macaulay.*

Demostración. Observemos que A es noetheriano si y sólo 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 3.4.8).

Sea $x \in \operatorname{Spec} A$ y $f^{*-1}(x) = \{y_1,\dots,y_r\}$. Los extens son estables por cambio de base plano, luego

$$\operatorname{Ext}^i_{A_x}((A/\mathfrak{p}_x)_x, A_x) \otimes_{A_x} B_x = \operatorname{Ext}^i_{B_x}((B/\mathfrak{p}_x B)_x, B_x) = \prod_j \operatorname{Ext}^i_{B_{y_j}}((B/\mathfrak{p}_x B)_{y_j}, B_{y_j})$$

Ahora, por el teorema de Ischebeck, es fácil concluir que A_x es de Cohen-Macaulay si y sólo 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 $t_1,\dots,t_n$ un sistema mínimo de parámetros que generen $\mathfrak{m}$. Por ser $A \to B$ finito, $\dim B/(t_1,\dots,t_n) = 0$, y por tanto $t_1,\dots,t_n$ es una sucesión regular en B, por ser B Cohen-Macaulay. Entonces,

$$\operatorname{Tor}^A_1(A/\mathfrak{m}, B) = H_1(K_\cdot(t_1,\dots,t_n,A) \otimes_A B) = H_1(K_\cdot(t_1,\dots,t_n,B)) = 0$$

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 6.6.16 nos dice que X es Cohen-Macaulay si y sólo 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: Llamaremos dimensión inyectiva de M, y lo denotaremos $\operatorname{diminy} M$, 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.

20. Corolario: $\operatorname{diminy} M \leq n \Leftrightarrow \operatorname{Ext}_A^{n+1}(A/I, M) = 0$ *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 6.3.14 concluimos que C es un A-módulo inyectivo y $\operatorname{diminy} M \leq n$. □

21. 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]).

22. Proposición: *Sea* $\mathcal{O}$ *local noetheriano de ideal maximal* $\mathfrak{m}$. $\mathcal{O}$ *es inyectivo* $\Leftrightarrow$ $\mathcal{O}$ *es un anillo artiniano y* $\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = \mathcal{O}/\mathfrak{m}$.

Demostración. Sea N un $\mathcal{O}$-módulo finito generado. Denotemos $N^* = \operatorname{Hom}_{\mathcal{O}}(N, \mathcal{O})$ y $k = \mathcal{O}/\mathfrak{m}$. Veamos el recíproco:

1) $l(N^*) \leq l(N)$. En efecto, lo probamos por inducción sobre la longitud. Sea $0 \to k \to N \to N/k = N' \to 0$ una sucesión exacta. Entonces se tiene 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

$$0 \to k \to \mathcal{O} \to \mathfrak{m}^* \to \operatorname{Ext}_{\mathcal{O}}^1(\mathcal{O}/\mathfrak{m}, \mathcal{O}) \to 0$$

luego, $l(\operatorname{Ext}_{\mathcal{O}}^1(\mathcal{O}/\mathfrak{m}, \mathcal{O})) = l(\mathfrak{m}^*) - l(\mathcal{O}) + 1 \leq 0$, y $\operatorname{Ext}_{\mathcal{O}}^1(\mathcal{O}/\mathfrak{m}, \mathcal{O}) = 0$. Por el corolario anterior, $\mathcal{O}$ es inyectivo.

Probemos el directo. Dado un ideal primo $\mathfrak{p} \underset{\neq}{\subset} \mathfrak{m}$, sea $x \in \mathfrak{m} \setminus \mathfrak{p}$ y consideremos el morfismo $\mathcal{O}/\mathfrak{p} \overset{x\cdot}{\hookrightarrow} \mathcal{O}/\mathfrak{p}$. Entonces el morfismo $(\mathcal{O}/\mathfrak{p})^* \overset{x\cdot}{\to} (\mathcal{O}/\mathfrak{p})^*$ 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 $l(k^*) = n$. 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 $k^* \simeq k$. □

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 verifica*

$$\operatorname{Ext}_A^{n+1}(N, M) = \operatorname{Ext}_{A/xA}^n(N, M/xM)$$

Demostración. 1) La sucesión exacta $0 \to M \overset{x\cdot}{\to} M \to M/xM \to 0$ induce la sucesión exacta

$$0 = \operatorname{Hom}_A(N, M) \to \operatorname{Hom}_A(N, M/xM) \to \operatorname{Ext}_A^1(N, M) \overset{x\cdot=0}{\to} 0$$

Es decir, $\operatorname{Ext}_A^1(N, M) = \operatorname{Hom}_A(N, M/xM) = \operatorname{Hom}_{A/xA}(N, M/xM)$.

2) Como x es A-regular, tenemos que $\operatorname{dimpro} A/xA = 1$ y por tanto $\operatorname{Ext}_A^n(A/xA, M) = 0$, para $n \neq 1$. Por tanto, $\operatorname{Ext}_A^n(P, M) = 0$ para todo A/xA-módulo libre P, para $n \neq 1$.

3) Sea $P_\cdot \to N$ una resolución de N por A/xA-módulos libres y $M \to I^\cdot$ una resolución de M por A-módulos inyectivos. Entonces,

$$\operatorname{Ext}_A^{i+1}(N, M) \overset{6.2.17}{=} H^{i+1}(\operatorname{Hom}_A^\cdot(P_\cdot, I^\cdot)) \overset{2),6.2.17}{=} H^i(\operatorname{Ext}_A^1(P_\cdot, M))$$
$$\overset{1)}{=} H^i(\operatorname{Hom}_{A/xA}(P_\cdot, M/x \cdot M)) = \operatorname{Ext}_{A/xA}^i(N, M/xM)$$

□

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* $\operatorname{Ext}^n_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \mathcal{O}/\mathfrak{m}$.
4. $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = 0$ *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 6.6.22 y $\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \mathcal{O}/\mathfrak{m}$, por 6.6.22.

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 6.6.22. Sea $\dim\mathcal{O} = n > 0$. Probemos que $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\quad,\mathcal{O}) = 0$ para todo $i > 0$. Por el lema,

$$\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \operatorname{Ext}^{n+i-1}_{\mathcal{O}/x\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}/x\mathcal{O}) \overset{\text{Ind.}}{=} 0$$

si $x \in \mathfrak{m}$ es un elemento $\mathcal{O}$-regular. 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 $\operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^{n+i}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \to \operatorname{Ext}^{n+i+1}_{\mathcal{O}}(\mathcal{O}/(\mathfrak{p},x),\mathcal{O}) = 0$ (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 concentrado en $\mathfrak{m}$. Sea $\mathfrak{p}_y$ un ideal primo estrictamente contenido en $\mathfrak{m}$, máximo cumpliendo $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) = 0$. De la sucesión $0 \to \mathcal{O}/\mathfrak{p}_y \xrightarrow{x\cdot} \mathcal{O}/\mathfrak{p}_y \to \mathcal{O}/(\mathfrak{p}_y,x) \to 0$ ($x \in \mathfrak{m}\backslash\mathfrak{p}$), obtenemos $\operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) \to 0$, luego por Nakayama $\operatorname{Ext}^{r-1}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_y,\mathcal{O}) = 0$ y evidentemente $\operatorname{Ext}^{r-1}_{\mathcal{O}_y}((\mathcal{O}/\mathfrak{p}_y)_y,\mathcal{O}_y) = 0$. Por inducción sobre la dimensión del anillo obtenemos que $\operatorname{diminy}\mathcal{O}_y < r-1$. De aquí deducimos que $\operatorname{Ext}^r_{\mathcal{O}}(M,\mathcal{O})$ está concentrado en $\mathfrak{m}$ para todo módulo finito generado M. Sea $\mathfrak{p}$ un ideal primo máximo con la condición de que $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \neq 0$. Para $x \in \mathfrak{m}\backslash\mathfrak{p}$ consideremos la sucesión $0 \to \mathcal{O}/\mathfrak{p} \xrightarrow{x\cdot} \mathcal{O}/\mathfrak{p} \to \mathcal{O}/(\mathfrak{p},x) \to 0$ y de aquí la sucesión $0 \to \operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) \xrightarrow{x\cdot} \operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O})$. Ahora bien, como $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O})$ es de longitud finita, $x\cdot$ es isomorfismo, luego por Nakayama $\operatorname{Ext}^r_{\mathcal{O}}(\mathcal{O}/\mathfrak{p},\mathcal{O}) = 0$ y llegamos a contradicción. En conclusión, $\operatorname{Ext}^r_{\mathcal{O}}(-,\mathcal{O}) = 0$ y $\operatorname{diminy}\mathcal{O} < r$. □

25. Definición: Diremos que un anillo $\mathcal{O}$ local noetheriano es de Gorenstein si verifica cualquiera de las condiciones equivalentes del teorema anterior.

26. 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 sólo si $\mathcal{O}/x\mathcal{O}$ es de Gorenstein.*

Demostración. Es consecuencia inmediata de la igualdad $\operatorname{Ext}^i_{\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}) = \operatorname{Ext}^{i-1}_{\mathcal{O}/x\mathcal{O}}(\mathcal{O}/\mathfrak{m},\mathcal{O}/x\mathcal{O})$. □

27. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de ideal maximal $\mathfrak{m}$ y $x \in \operatorname{Spec}\mathcal{O}$. Se verifica:*

a) Si $\mathcal{O}$ es de Gorenstein, entonces $\mathcal{O}_x$ es de Gorenstein.

b) $\mathcal{O}$ es de Gorenstein si y sólo 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. □

28. 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 $d \iff \mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}},\mathcal{O}) = 0$ para $i \neq n-d$ y $\mathrm{Ext}^{n-d}_{\mathcal{O}}(\bar{\mathcal{O}},\mathcal{O}) \simeq \bar{\mathcal{O}}$.*

Demostración. Procedemos por inducción sobre $n = \dim \mathcal{O}$.

a) Si $\dim \mathcal{O} = 0$, entonces $\mathcal{O}$ es inyectivo. Por tanto, $\mathcal{O}$ 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 6.6.22, $\bar{\mathcal{O}}$ es inyectivo y por tanto Gorenstein. Recíprocamente, supongamos que $\bar{\mathcal{O}}$ es Gorenstein. Dado un $\bar{\mathcal{O}}$-módulo finito generado N, denotemos $N^* = \mathrm{Hom}_{\mathcal{O}}(N,\mathcal{O})$. $(\mathcal{O}/\mathfrak{m})^* = \mathcal{O}/\mathfrak{m}$. 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 6.6.23, $\mathrm{Ext}^i_{\mathcal{O}}(\bar{\mathcal{O}},\mathcal{O}) = \mathrm{Ext}^{i-1}_{\mathcal{O}/t\mathcal{O}}(\bar{\mathcal{O}},\mathcal{O}/t\mathcal{O})$ 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.

□

6.7. Criterios de platitud

6.7.1. 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 $\alpha \subseteq A$, finito generado, $\alpha \otimes_A M$ 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 plano sobre A.*
2. *M/I^nM es plano sobre A/I^n, para todo $n \geq 0$.*
3. *M/IM es plano sobre A/I y $(\overset{\infty}{\underset{n=0}{\oplus}} I^n/I^{n+1}) \underset{A}{\otimes} M \simeq \overset{\infty}{\underset{n=0}{\oplus}} (I^nM/I^{n+1}M)$.*
4. *M/IM es plano sobre A/I 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 $\alpha \subset A$ el morfismo $\alpha \underset{A}{\otimes} M \to M$, $a \otimes m \mapsto am$ es inyectivo. Basta probar que en el diagrama conmutativo

$$\begin{array}{ccc} \alpha \otimes M & \longrightarrow & M \\ \downarrow & & \downarrow \\ \widehat{\alpha \otimes M} & \longrightarrow & \widehat{M} \end{array}$$

el morfismo $\widehat{\alpha \otimes M} \to \widehat{M}$ es inyectivo. Por el lema de Artin-Rees, la topología I-ádica en α coincide con la topología definida por la filtración $\{I^k \cap \alpha\}$. Por lo tanto, la topología definida en $\alpha \otimes M$ por $\{I^k(\alpha \otimes M)\}$, coincide con la topología definida por $\{(I^k \cap \alpha) \otimes M\}$. En conclusión $\widehat{\alpha \otimes M} = \varprojlim (\bar{\alpha}_k \underset{A/I^k}{\otimes} M/I^kM)$, donde $\bar{\alpha}_k = \alpha/(I^k \cap \alpha) \subset A/I^k$. Como el límite proyectivo de inyecciones es una inyección, el morfismo $\widehat{\alpha \otimes M} \to \widehat{M}$ 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

$$\begin{array}{ccccccc} & & I^{k+1}/I^n \underset{A}{\otimes} M & \longrightarrow & I^k/I^n \underset{A}{\otimes} M & \longrightarrow & I^k/I^{k+1} \underset{A}{\otimes} M \longrightarrow 0 \\ & & \downarrow{\scriptstyle \phi_{k+1}} & & \downarrow{\scriptstyle \phi_k} & & \downarrow{\scriptstyle \wr} \\ 0 \longrightarrow & I^{k+1}M/I^nM & \longrightarrow & I^kM/I^nM & \longrightarrow & I^kM/I^{k+1}M & \longrightarrow 0 \end{array}$$

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 $\operatorname{Tor}_1^A(A/I, M) = 0$.

4. $\Rightarrow$ 2. Si $\operatorname{Tor}_1^A(A/I, M) = 0$, entonces $\operatorname{Tor}_1^A(N, M) = 0$ 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

$$\begin{array}{ccccccccc} \operatorname{Tor}_1^A(L,M) & \longrightarrow & \operatorname{Tor}_1^A(N,M) & \longrightarrow & K \otimes_A M & \longrightarrow & L \otimes_A M & \longrightarrow & N \otimes_A M \longrightarrow 0 \\ \| & & \| & & \| & & \| & & \| \\ 0 & \longrightarrow & \operatorname{Tor}_1^{A/I}(N, M/IM) & \to & K \otimes_{A/I} M/IM & \to & L \otimes_{A/I} M/IM & \to & N \otimes_{A/I} M/IM \to 0 \end{array}$$

Como M/IM es un A/I-módulo plano, concluimos que $\operatorname{Tor}_1^A(N, M) = 0$. Ahora, si N es un A/I^k-módulo, demostremos que $\operatorname{Tor}_1^A(N, M) = 0$. 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 $\operatorname{Tor}_1^A(N, M) = 0$.

Por tanto, dada una sucesión exacta $0 \to N_1 \to N_2 \to N_3 \to 0$ de A/I^k-módulos, la segunda fila del diagrama

$$\begin{array}{ccccccc} 0 \longrightarrow & N_1 \otimes_A M & \longrightarrow & N_2 \otimes_A M & \longrightarrow & N_3 \otimes_A M & \longrightarrow 0 \\ & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} & \\ & N_1 \otimes_{A/I^k} M/I^kM & \to & N_2 \otimes_{A/I^k} M/I^kM & \to & N_3 \otimes_{A/I^k} M/I^kM \to 0 & \end{array}$$

es exacta, es decir, M/I^kM es un A/I^k-módulo plano. □

3. Corolario: *Sean A y B k-álgebras de tipo finito y $f: A \to B$ un morfismos de k-álgebras. Entonces, f es un morfismo plano si y sólo 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 $f^*: Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$ es plano si y sólo si*

$$C_xX \times_x f^{*-1}(x) = C(X/f^{*-1}(x))$$

para todo punto cerrado $x \in X$.

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 sólo 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 $\bar{\mathcal{O}} = \mathcal{O}/a\mathcal{O}$, $\bar{\mathcal{O}}' = \mathcal{O}'/a\mathcal{O}'$.

Veamos el directo. 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 $f_1, \ldots, f_r$ un sistema mínimo de parámetros de $\bar{\mathcal{O}}'/\mathfrak{m}\bar{\mathcal{O}}'$ y $f_{r+1}, \ldots, f_n$ un sistema de parámetros mínimo de $\bar{\mathcal{O}}$. Entonces $f_1, \ldots, f_n$ 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 6.5.7, 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 $\mathcal{O}$.

Recíprocamente. 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 sólo si f es plano.*

8. Proposición: *Sean B y C A-álgebras noetherianas planas. Entonces, $f \in \operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} C, \operatorname{Spec} B)$ es plano si es plano en fibras sobre* $\operatorname{Spec} A$.

Demostración. Podemos suponer A,B,C locales y que los morfismos $A\to B$, $B\to C$ son locales. Sea I el ideal maximal de A. Por hipótesis, C/IC es una B/IB-álgebra plana. Además,

$$(I^nB/I^{n+1}B)\underset{B}{\otimes}C=\left(I^n/I^{n+1}\underset{A}{\otimes}B\right)\underset{B}{\otimes}C=I^n/I^{n+1}\underset{A}{\otimes}C=I^nC/I^{n+1}C,$$

donde la primera igualdad y la última se deben al criterio local de platitud 6.7.2; 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 $\mathcal{O}'$-módulos finito generados y supongamos que P es un $\mathcal{O}$-módulo plano. Un morfismo de $\mathcal{O}'$-módulos $i\colon M\to P$ 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

$$0=\operatorname{Tor}_{\mathcal{O}}^1(\mathcal{O}/\mathfrak{m},P/M)\to M\otimes_{\mathcal{O}}\mathcal{O}/\mathfrak{m}\to P\otimes_{\mathcal{O}}\mathcal{O}/\mathfrak{m}$$

$\Leftarrow$) 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 $\operatorname{Tor}_1^{\mathcal{O}}(\mathcal{O}/\mathfrak{m},P/M)=0$. 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, en la proposición anterior, el morfismo $M\xrightarrow{b\cdot}M, m\mapsto b\cdot m$.

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

$$0\to M/\mathfrak{m}^nM\xrightarrow{b\cdot}M/\mathfrak{m}^nM\to M/(\mathfrak{m}^nM+bM)\to 0$$

luego b no es divisor de cero en $M/\mathfrak{m}^nM$, para todo n, y por el lema de la serpiente tampoco es divisor de cero en $\mathfrak{m}^nM/\mathfrak{m}^{n+1}M$. Si consideramos el diagrama de filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_{\mathfrak{m}}M & \xrightarrow{b\cdot} & G_{\mathfrak{m}}M & \longrightarrow & G_{\mathfrak{m}}(M/bM) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle\pi} & & \uparrow{\scriptstyle\pi} & & \| & & \\ 0 & \longrightarrow & (G_{\mathfrak{m}}\mathcal{O})\otimes_{\mathcal{O}/\mathfrak{m}}M/\mathfrak{m}M & \xrightarrow{b\cdot} & (G_{\mathfrak{m}}\mathcal{O})\otimes_{\mathcal{O}/\mathfrak{m}}M/\mathfrak{m}M & \longrightarrow & (G_{\mathfrak{m}}\mathcal{O})\otimes_{\mathcal{O}/\mathfrak{m}}M/(\mathfrak{m}M+bM) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \operatorname{Ker}\pi & \xrightarrow{b\cdot} & \operatorname{Ker}\pi & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

obtenemos, por el lema de Nakayama (grado a grado), que $\operatorname{Ker}\pi=0$. Por tanto, M es un $\mathcal{O}$-módulo plano.

□

6.7.2. 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 $\frac{m_1}{s_1},\dots,\frac{m_n}{s_n}$ 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

$$M_0 = N_0, M_1 = M_0 \oplus M_1/M_0 = N_0 \oplus N_1, \dots, M_n = \oplus_{i=0}^{n} N_i \text{ y } M = \cup_{i=0}^{\infty} M_i = \oplus_{i=0}^{\infty} N_i.$$

□

13. Criterio topológico de Nagata: *Sea A un anillo noetheriano. Un subconjunto U de* $\operatorname{Spec}A$ *es abierto si y sólo si verifica:*

1) Si $\bar{x} \cap U \neq \emptyset$, entonces $x \in U$ ("estabilidad por generalizaciones").

2) Si $x \in U$, entonces $\bar{x} \cap U$ es un entorno de x en $\bar{x}$.

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, por 1) $x_i \in U$, y por 2) existe un abierto W tal que $x_i \in W \cap \bar{x}_i \subset U$; por lo tanto $C_1 \cup \cdots \cup C_r = \overline{\operatorname{Spec}A\setminus U} = C_1 \cup \cdots \cup (C_i \setminus (W \cap \bar{x}_i)) \cup \cdots \cup C_r$, 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 $U := \{x \in \operatorname{Spec}B : M_x$ es plano sobre $A\}$ es un abierto de* $\operatorname{Spec}B$.

Demostración. Tenemos que ver que U verifica las condiciones 1) y 2) del criterio topológico de Nagata 6.7.13. Evidentemente U es estable por generalizaciones. Probemos 2). Sea $x \in U$ e $y \in \bar{x}$. Sea $\mathfrak{p}_x$ el ideal definido por x y escribamos $\mathfrak{p} = A \cap \mathfrak{p}_x$, $\bar{A} = A/\mathfrak{p}$.

Por el criterio local de platitud M_y es un A-módulo plano si y sólo si $\operatorname{Tor}_1^A(M_y,\bar{A}) = 0$ y $(M/\mathfrak{p}M)_y$ es $\bar{A}$- plano. Ahora bien, $\operatorname{Tor}_1^A(M,\bar{A})_x = \operatorname{Tor}_1^A(M_x,\bar{A}) = 0$, 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. Lema: *Si B es una A-álgebra de tipo finito, el morfismo natural $f\colon \mathrm{Spec}B \to \mathrm{Spec}A$ transforma casi-cerrados en casi-cerrados.*

Demostración. Por ser B de tipo finito sobre A, podemos factorizar $\mathrm{Spec}B \xrightarrow{f} \mathrm{Spec}A$ 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 un morfismo $\pi\colon \mathbb{A}^1 \times \mathrm{Spec}A \to \mathrm{Spec}A$. Para probar que la imagen de un casi-cerrado Z es un casi-cerrado, podemos suponer que $\overline{\pi(Z)} = \mathrm{Spec}A$, sin más que considerar la proyección $\mathbb{A}^1 \times \overline{\pi(Z)} \to \overline{\pi(Z)}$. 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 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 $f(U_b) = \underset{i}{\cup} U_{a_i}$. 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 $U_a \subseteq f(U_b)$.

□

17. 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 sólo si se cumple para un cerrado $X_1 \underset{\neq}{\subseteq} X$ y podemos repetir este proceso sucesivamente, tendremos por la noetherienidad de X, que $X_n = \emptyset$, para $n >> 0$, y sólo hay que probar el teorema en este caso (que suele ser trivial). Este modo de proceder se denomina demostración por inducción noetheriana sobre X.*

18. 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.

□

6.8. 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 $\mathrm{Spec}A \to \mathrm{Spec}R$, 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 B es una A-álgebra plana, 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, porque lo es en fibras sobre S (por 6.4.9) y por 6.7.10.

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 $f\colon X = \operatorname{Spec}B \to S = \operatorname{Spec}A$ es un morfismo de tipo finito plano de dimensión n. Se verifica que f es liso si y sólo 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 6.4.5, y es de rango n porque en fibras es de rango n por 4.3.13. 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 4.3.13. □

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 sólo si el morfismo $E \to B$ admite sección (de A-álgebras). Además,*

$$\operatorname{Isom}_{B-ext}(B * L, B * L) = \operatorname{Der}_A(B,L)$$

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.

Si D es una A-derivación de B en L, 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 $\operatorname{Exalcom}_A(B,L)$ 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

$$\begin{aligned} f_*\colon \operatorname{Exalcom}_A(B,L) &\to \operatorname{Exalcom}_A(B,L') \\ E &\mapsto (E * L')/(l, -f(l))_{l \in L} \end{aligned}$$

El conjunto $\operatorname{Exalcom}_A(B,L)$ tiene estructura de grupo mediante el producto:

$$\begin{aligned} \operatorname{Exalcom}_A(B,L) \times \operatorname{Exalcom}_A(B,L) &\longrightarrow \operatorname{Exalcom}_A(B,L) \\ (E,E') &\longmapsto E \underset{B}{\times} E'/(l,-l)_{l \in L}, \end{aligned}$$

donde $E \times_B E' = \{(e,e') \in E \times E' : \pi(e) = \pi'(e')\}$. El paso al opuesto es el morfismo $(-1)_*$, siendo $-1 : L \to L$, $l \mapsto -l$. El elemento neutro es la extensión trivial. Con esta estructura, el morfismo f_* anteriormente definido es morfismo de grupos.

Un morfismo de A-álgebras $\phi : B \to B'$, induce un morfismo de grupos

$$\begin{aligned} \phi^* : \operatorname{Exalcom}_A(B',L) &\to \operatorname{Exalcom}_A(B,L) \\ E' &\mapsto E' \underset{B}{\times} B' \end{aligned}$$

Finalmente, un morfismo de anillos $\phi : A \to A'$ induce un morfismo de grupos

$$\begin{aligned} \phi' : \operatorname{Exalcom}_{A'}(B,L) &\to \operatorname{Exalcom}_A(B,L) \\ E &\mapsto E \end{aligned}$$

cuyo núcleo se denota $\operatorname{Exalcom}_{A'/A}(B,L)$ y representa las clases de A'-extensiones de B por L que son A-triviales.

8. Teorema: *Sean $A \xrightarrow{f} A' \xrightarrow{\phi} B$ morfismos de anillos y L un B-módulo. Se tienen las sucesiones exactas*

1. $0 \to \operatorname{Der}_{A'}(B,L) \to \operatorname{Der}_A(B,L) \to \operatorname{Der}_A(A',L) \xrightarrow{\delta} \operatorname{Exalcom}_{A'/A}(B,L) \to 0.$

2. $0 \to \operatorname{Exalcom}_{A'/A}(B,L) \to \operatorname{Exalcom}_{A'}(B,L) \xrightarrow{f'} \operatorname{Exalcom}_A(B,L) \xrightarrow{\phi^*} \operatorname{Exalcom}_A(A',L).$

Es decir, se tiene la sucesión exacta

$$\begin{aligned} 0 \to \operatorname{Der}_{A'}(B,L) \to \operatorname{Der}_A(B,L) \to \operatorname{Der}_A(A',L) \to \\ \to \operatorname{Exalcom}_{A'}(B,L) \xrightarrow{f'} \operatorname{Exalcom}_A(B,L) \xrightarrow{\phi^*} \operatorname{Exalcom}_A(A',L) \end{aligned}$$

Demostración. En primer lugar, definamos el morfismo $\delta : \operatorname{Der}_A(A',L) \to \operatorname{Exalcom}_{A'}(B,L)$. Dada una A-derivación $D : A' \to L$, consideramos la A-extensión trivial $B * L$ y la dotamos de estructura de A'-álgebra mediante el morfismo de anillos

$$\begin{aligned} A' &\longrightarrow B * L \\ a' &\mapsto (a', Da') \end{aligned}$$

que es morfismo de anillos por ser D derivación. Además el morfismo $B * L \to B$ es de A'-álgebras, luego $B * L$ es una A'-extensión de B por L. Veamos ahora la exactitud de la sucesión.

- La exactitud de $0 \to \operatorname{Der}_{A'}(B,L) \to \operatorname{Der}_A(B,L) \to \operatorname{Der}_A(A',L)$ es inmediata.

- Exactitud de $\operatorname{Der}_A(B,L) \to \operatorname{Der}_A(A',L) \xrightarrow{\delta} \operatorname{Exalcom}_{A'}(B,L)$. Sea D una A-derivación de A' en L. Si D proviene de una derivación de B (que seguimos denotando D), entonces la A'-extensión $B * L$ construida anteriormente admite la sección $B \to B * L$, $b \mapsto (b, Db)$, luego es trivial. Recíprocamente, si la A'-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 A' es D.

- Exactitud de $\operatorname{Der}_A(A',L) \xrightarrow{\delta} \operatorname{Exalcom}_{A'}(B,L) \xrightarrow{f'} \operatorname{Exalcom}_A(B,L)$. Por definición de δ, la A'-extensión $\delta(D)$ es A-trivial. Recíprocamente, si una A'-extensión E de B por L es A-trivial, entonces $E = B * L$, como A-álgebra, y el morfismo de anillos $A' \to B * L$, $a' \mapsto (a', Da')$ define una A-derivación D de A' en L, de modo que $E = \delta(D)$.

- Exactitud de $\operatorname{Exalcom}_{A'}(B,L) \xrightarrow{f'} \operatorname{Exalcom}_A(B,L) \xrightarrow{\phi^*} \operatorname{Exalcom}_A(A',L)$. Si E es una A-extensión de B por L que está en el núcleo de ϕ^*, entonces $E \underset{B}{\times} A'$ es A-extensión trivial de A' por L, luego admite sección $A' \to E \underset{B}{\times} A'$. Componiendo este sección con la proyección natural $E \underset{B}{\times} A' \to E$, se obtiene un morfismo de anillos $\alpha : A' \to E$ que dota a E de estructura de A'-álgebra, compatible con su estructura de A-álgebra. Por tanto, E está en la imagen de f'. Recíprocamente, si E es una A'-extensión de B por L, entonces $E \underset{B}{\times} A'$ es una A-extensión trivial de A' por L, porque el morfismo de proyección $E \underset{B}{\times} A' \to A'$ tiene sección $a' \mapsto (a', a')$ □

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 $A[x_1,\dots,x_n]$ 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. $\mathrm{Hom}_{A'-\text{álg}}(A' \otimes_A B, C) = \mathrm{Hom}_{A-\text{álg}}(B,C) \twoheadrightarrow \mathrm{Hom}_{A-\text{álg}}(B,C/I) = \mathrm{Hom}_{A'-\text{álg}}(A' \otimes_A B, C/I)$. □

12. Teorema: *Si $A \to B$ 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, el morfismo (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 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 de B-módulos $I/I^2 \to L$. 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 una asignación es la inversa de la otra.

□

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 6.8.12), la sucesión de diferenciales es exacta si y sólo si tomando homomorfismos en todo módulo es exacta. Por el apartado 1. de 6.8.8 y el lema anterior se concluye.

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 una sucesión exacta

$$0 \to \mathrm{Der}_A(B/I,L) \to \mathrm{Der}_A(B,L) \to \mathrm{Hom}_B(I/I^2,L) \to 0$$

Ahora bien, por el lema anterior $\mathrm{Hom}_B(I/I^2,L) \simeq \mathrm{Exalcom}_B(B/I,L)$. Por tanto, teniendo en cuenta la sucesión exacta del teorema 6.8.8, se concluye que $\mathrm{Exalcom}_{B/A}(B/I,L) = \mathrm{Exalcom}_B(B/I,L)$. Ahora, por hipótesis, $\mathrm{Exalcom}_A(B,L) = 0$, luego, de nuevo por la sucesión exacta 6.8.8, $\mathrm{Exalcom}_A(B/I,L) = 0$ 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 sólo 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 $C = B/I$. Por el criterio jacobiano de lisitud formal, la lisitud formal es una propiedad local en C. Además, dado un ideal maximal $\mathfrak{m}_x \subset C$, para demostrar que C_x es formalmente liso sobre A, localizando en y (donde $\mathfrak{p}_y := \mathfrak{m}_x \cap A$) podemos suponer que $\mathfrak{p}_y$ es un ideal maximal de A. Lo mismo decimos con la lisitud.

Observemos que $I/\mathfrak{m}_x I = \bar{I}/\bar{\mathfrak{m}}_x \bar{I}$, denotamos con las barras los ideales correspondientes en la fibra de y. En efecto, si $A \to C$ es plano, $\bar{I} = I \otimes_A A/\mathfrak{m}_y$ y $\bar{I}/\bar{\mathfrak{m}}_x\bar{I} = (I/\mathfrak{m}_x I) \otimes_A A/\mathfrak{m}_y = I/\mathfrak{m}_x I$. Si $A \to C$ es formalmente liso, 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 $A/\mathfrak{m}_y \to C/\mathfrak{m}_y C$ 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.

Si C es una A-álgebra lisa veamos que es formalmente lisa. $\Omega_{C/A}$ es un C-módulo localmente libre y la sucesión del criterio jacobiano de lisitud formal es exacta porque lo es en fibras sobre y, luego $A \to C$ es formalmente liso.

Recíprocamente, veamos que si C es una A-álgebra formalmente lisa entonces es 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. 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 6.7.10, C es A-plano.

□

6.9. Problemas

1. Sea $f: K \to L$ un morfismo de complejos y $\mathrm{Cono}(f)$ su cono. Probar

   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 $K^{\le m} = \cdots \to K^{i,\cdot} \to \cdots \to K^{m-1,\cdot} \to Z^m \to 0$ (donde $Z^m = \mathrm{Ker}\, \mathrm{d}_1^m$). Demostrar que el conúcleo de la inclusión $K^{\le n-1} \hookrightarrow K^{\le n}$ es cuasi-isomorfo a $H_{\mathrm{d}_1}(K)[-n]$

3. Dar una nueva demostración del teorema 6.2.16 usando el problema anterior.

4. Probar 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, $Z = \mathrm{Ker}\, d$ y $B = \mathrm{Im}\, d$.

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 $\mathrm{Ker}\, \pi = 0 \to B^n \to B^n \to 0$, o aplíquese el teorema 6.2.16). Como el teorema es cierto para $H^n(K)$, hemos terminado.

6. Probar que A es regular si y sólo si $A[x]$ lo es.

7. Sea M un A-módulo inyectivo y $\bar{A} = A/J$. Probar que $\mathrm{Hom}_A(\bar{A}, M)$ es un $\bar{A}$-módulo inyectivo. Probar 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. Probar que $\mathrm{Ext}^i_A(N, M) = \mathrm{Ext}^i_{A/xA}(N/xN, M)$.

9. Sea A un anillo noetheriano. Probar que A es un anillo de Cohen-Macaulay si y sólo si $A[x]$ lo es.

10. Sea A un anillo noetheriano. Probar que A es un anillo de Gorenstein si y sólo si $A[x]$ lo es.

Capítulo 7

Desingularización de superficies

Juan B. Sancho

7.1. 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 aumenta 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 sólo 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.

7.2. 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 0.7.10. 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 3.7.4). Así pues, el polinomio 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 5.7.4) el polinomio 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 4.3.9, $\mathfrak{p}_y = (t_1, \ldots, t_{n-r})$, donde los t_i son linealmente independientes en $\mathfrak{m}/\mathfrak{m}^2$. De nuevo por 4.3.9, 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 verifica*

$$G_{\mathfrak{p}_y} \mathcal{O} = \mathcal{O}/\mathfrak{p}_y[t_1, \ldots, t_{n-r}]$$

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 $\mathcal{O}/\mathfrak{p}_y[t_1,\dots,t_{n-r}]$ 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 de [23]. Si $A[\xi_1,\dots,\xi_n]$ es una A-álgebra graduada, entonces $\widetilde{X} = \operatorname{Proj} A[\xi_1,\dots,\xi_n]$ no es, en general, una variedad afín, es decir, no es isomorfo a $\operatorname{Spec} B$, 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

$$U^h_{\xi_i} = \operatorname{Spec} A[\xi_1/\xi_i,\dots,\xi_n/\xi_i]$$

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 $\mathfrak{p}_Y \subset \mathcal{O}_X$ el ideal primo de las funciones que se anulan en Y y

$$\pi\colon \widetilde{X} = \operatorname{Proj} D_{\mathfrak{p}_Y}\mathcal{O}_X \to X$$

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, $\pi^{-1}(Y) = \operatorname{Proj} G_{\mathfrak{p}_Y}\mathcal{O}_X$ que es localmente isomorfo (por el lema anterior) a

$$\operatorname{Proj}\mathcal{O}/\mathfrak{p}_Y[t_1,\dots,t_{n-r}] = \mathbb{P}^{n-r-1}\times Y$$

siendo r la dimensión de Y. Por tanto, $\mathcal{O}_{\widetilde{X}}/\mathfrak{p}_Y\mathcal{O}_{\widetilde{X}}$ es un anillo regular. Ahora bien, $\mathfrak{p}_Y\mathcal{O}_{\widetilde{X}}$ es un ideal localmente principal. Como la explosión de un anillo íntegro es íntegro, $\widetilde{X}$ 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 $f \in \mathcal{O}_X$. 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 7.2.5, $G_{\mathfrak{p}}\mathcal{O}_X = \mathcal{O}_Y[t_1,\dots,t_{n-r}]$. Sea g el punto genérico de Y y $\Sigma = \mathcal{O}_{Y,g}$ el cuerpo de fracciones de $\mathcal{O}_Y$. Entonces $G_{\mathfrak{p}}\mathcal{O}_{X,g} = \Sigma[t_1,\dots,t_{n-r}]$. Por tanto, $\mathcal{O}_{X,g}$ es un anillo local regular y $f \in \mathfrak{p}^m\mathcal{O}_{X,g}\setminus\mathfrak{p}^{m+1}\mathcal{O}_{X,g}$. Si denotamos $\operatorname{in}_{\mathfrak{p}} f$ la clase de f en $\mathfrak{p}^m/\mathfrak{p}^{m+1} \subset G_{\mathfrak{p}}\mathcal{O}_{X,g}$, entonces, por 4.2.5,

$$G_{\bar{\mathfrak{p}}}\mathcal{O}_{H,g} = \Sigma[t_1,\dots,t_{n-r}]/(\operatorname{in}_{\mathfrak{p}} f)$$

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 6.5.1, $G_{\bar{\mathfrak{p}}}\mathscr{O}_H$ es plano $\iff$ la sucesión anterior tensada por el cuerpo residual de y sigue siendo exacta. Al tensar se obtiene

$$\begin{array}{ccccc} \underset{n}{\oplus}(\mathfrak{p}^n/\mathfrak{m}_y\mathfrak{p}^n) & \xrightarrow{\cdot[\mathrm{in}_{\mathfrak{p}} f]\in(\mathfrak{p}^m/\mathfrak{m}_y\mathfrak{p}^m)} & \underset{n}{\oplus}(\mathfrak{p}^{n+m}/\mathfrak{m}_y\mathfrak{p}^{n+m}) & \longrightarrow & G_{\bar{\mathfrak{p}}}\mathscr{O}_H \otimes_{\mathscr{O}_Y} k(y) \longrightarrow 0 \\ \| & & \| & & \\ k(y)[t_i] & & k(y)[t_i] & & \end{array}$$

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 sólo 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 sólo 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 sólo 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 así:

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.

[1] Si H no es una hipersuperficie, son equivalentes

1. H es normalmente plano a lo largo de Y.
2. La función de Hilbert-Samuel es constante a lo largo de los puntos cerrados 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 exacta

$$[G_{\bar{\mathfrak{p}}}\mathscr{O}_H] \underset{\mathscr{O}_Y}{\otimes} k(y) \to G_{\mathfrak{m}_y}\mathscr{O}_H \to G_{\mathfrak{m}_y}\mathscr{O}_Y \to 0$$

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

$$\begin{array}{ccc}
([G_{\bar{\mathfrak{p}}}\mathscr{O}_H] \underset{\mathscr{O}_Y}{\otimes} k(y)) \underset{k(y)}{\otimes} G_{\mathfrak{m}_y}\mathscr{O}_Y & \xrightarrow{\sim} & G_{\mathfrak{m}_y}\mathscr{O}_H \\
\| & & \| \\
k(y)[t_1,\ldots,t_{n-r},x_1,\ldots,x_r]/(\mathrm{in}_{\mathfrak{p}} f) & & k(y)[t_1,\ldots,t_{n-r},x_1,\ldots,x_r]/(\mathrm{in}_{\mathfrak{m}_y} f)
\end{array}$$

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.

7.3. Contacto maximal para hipersuperficies

Sea X una variedad regular, $H = \mathrm{Spec}\mathscr{O}_X/(f)$ una hipersuperficie, e $Y = \mathrm{Spec}\mathscr{O}_X/\mathfrak{p} = \mathscr{O}_H/\bar{\mathfrak{p}}$ una subvariedad regular. Denotemos por $\widetilde{H}$ y $\widetilde{X}$ las explosiones de H y X a lo largo de Y. Tenemos el diagrama conmutativo

$$\begin{array}{ccc}
\widetilde{H} & \longrightarrow & \widetilde{X} \\
\downarrow & & \downarrow \\
H & \longrightarrow & X
\end{array}$$

Escribamos $\mathfrak{p} = (t_1, \ldots, t_{n-r})$. Entonces $\mathscr{O}_{\widetilde{X}}$ 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 verifica que $\mathscr{O}_{\widetilde{H}} = \mathscr{O}_{\widetilde{X}}/(f/t^m)$ 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 $x_1, \ldots, x_n$ es un sistema de parámetros regulares de X en y, entonces $\mathrm{Der}_k(\mathscr{O}_X, \mathscr{O}_X) = \mathscr{O}_X \frac{\partial}{\partial x_1} \oplus \ldots \oplus \mathscr{O}_X \frac{\partial}{\partial x_n}$ 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 $D : \mathscr{O}_X \to \mathscr{O}_X$ un operador diferencial de orden 1. Sea f de multiplicidad m en el punto genérico de Y. Entonces existe un operador diferencial $\tilde{D} : \mathscr{O}_{\tilde{X}} \to \mathscr{O}_{\tilde{X}}$ tal que*

$$\frac{Df}{t^{m-1}} = \tilde{D}\left(\frac{f}{t^m}\right)$$

Demostración. Es análoga al lema fundamental 5.10.10 para curvas planas. □

4. Proposición: *Sea $\pi : \widetilde{H} \to H$ 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 7.2.7 $\widetilde{H}$ 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 $\tilde{S} \to .^{\pi}. \to S$ de explosiones en centros permisibles de modo que $\pi(\mathrm{Sing}_m(\tilde{S}))$ 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 sólo 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 7.3.1, $\widetilde{H}$ 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 sólo 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 sólo 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 7.3.6, 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.

7.4. 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 $\mathfrak{m}_y = (t_1,\ldots,t_n)$ y $\mathfrak{p}_Y = (t_1,\ldots,t_{n-r})$. Entonces los anillos afines de $\widetilde{W}$ son $\mathcal{O}_W[\frac{t_1}{t},\ldots,\frac{t_{n-r}}{t}]$ ($t=t_i$, 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 sólo 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 sólo si $m_p(g_i(x,y)) \ge m-i$ para todo i. Veamos que $m_p(g_i(x,y)) \ge m-i$ para todo $i \iff m_p((D^i f)_{|W}) \ge m-i$ para todo i. El directo es obvio. Veamos el recíproco. Observemos que $m_p(g_0(x,y)) = m_p((D^0 f)_{|W}) \ge m$. Por hipótesis de inducción supongamos que $m_p(g_i(x,y)) \ge m-i$ 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 $m_p(D^r(f)_{|W}) \ge m-r$ se ha de cumplir que $m_p(g_r)\ge m-r$ 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,

$$\mathrm{Sing}_m(S) = \mathrm{Sing}_W(I,r)$$

[2] Si se conoce la teoría de divisores y haces de línea, estamos diciendo que $\widetilde{I} = I\cdot\mathcal{O}_{\widetilde{W}} \otimes_{\mathcal{O}_{\widetilde{W}}} \mathscr{L}_{rE}$, donde E es la fibra excepcional del morfismo de explosión.

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 7.3.1 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 $i<n$, $\tilde{D}^i(\frac{a}{t^m})=\tilde{D}^{i-1}(\frac{Da}{t^{m-1}}+z^n)=\tilde{D}^{i-1}(\frac{Da}{t^{m-1}}) \mod z=\cdots=\frac{D^i a}{t^{m-i}} \mod z$. Por tanto, $(\tilde{D}^i\tilde{f})^{\frac{r}{m-i}}=(\frac{D^i f}{t^{m-i}})^{\frac{r}{m-i}} \mod z$. En conclusión, $\widetilde{I}=(\tilde{f}^{\frac{r}{m}},(\tilde{D}\tilde{f})^{\frac{r}{m-1}},\ldots,(\tilde{D}^{m-1}\tilde{f})^{\frac{r}{1}})_{|\widetilde{W}}$ 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 $I=(f_1,\ldots,f_s)$. 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 sólo 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

$$\begin{cases} f=x^a\cdot\mathrm{inv.}\\ g=y^b\cdot\mathrm{inv.}\end{cases}$$

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 $p\in\mathrm{Sing}_w(I,r)$ un punto cerrado. Podemos tomar parámetros en un entorno de p de modo que $g=x^a y^b\cdot\mathrm{inv.}$

1. Se puede conseguir que $a,b<r$: En efecto, supongamos $a\geq r$. Entonces la curva $(x)_0$ está contenida en $\mathrm{Sing}_W(I,r)$. 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, $S=(y^2-x^2z)_0$.

Las singularidades son los puntos donde se anula $d(y^2-x^2z)=2ydy-2xzdx-x^2dz$. 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 $I=((y^2-x^2z)^{\frac{2}{2}},(2y)^2)_{|W}=(x^2z)$ y $r=2$. El locus singular del exponente idealístico son los puntos donde x^2z tiene multiplicidad 2, que son los puntos $x=0$ (de W).

Explotemos en la recta $x=0$. La transformada propia del exponente idealístico es $I_1=(\frac{x^2z}{x^2})=(z)$. 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 $1-(\frac{x}{y})^2zy$).

7.5. Tangente estricto

Sea $H=\mathrm{Spec}\mathscr{O}_X/(f)$ una hipersuperficie de una variedad regular. Consideremos el cono tangente en un punto x, $C_{H,x}=\mathrm{Spec}\,G_{\mathfrak{m}_x}\mathscr{O}_H=\mathrm{Spec}\,k[x_1,\ldots,x_n]/(\mathrm{in}_{\mathfrak{m}_x}f)$, 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 $\mathscr{T}_xH$, a

$$\mathscr{T}_xH=\mathrm{Sing}_m(C_{H,x})=\{\text{Puntos del cono con la misma multiplicidad que el vértice}\}$$

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.,

$$\mathcal{T}_x H = \{v \in C_{X,x} : C_{H,x} + v = C_{H,x}\}$$

2. Definición: Denotaremos $\tau := \dim \mathcal{T}_x H$, que es un invariante asociado a la singularidad.

3. Lema: *Sea $\mathcal{O}$ un anillo noetheriano local de ideal maximal $\mathfrak{m}$ y $\bar{\mathcal{O}} = \mathcal{O}/(t)$, con $t \in \mathfrak{m}$. Supongamos que $\dim \bar{\mathcal{O}} = \dim \mathcal{O} - 1$ (por ejemplo si t no es divisor de cero). Entonces la multiplicidad de $\mathcal{O}$ en el punto cerrado es menor o igual que la de $\bar{\mathcal{O}}$.*

Demostración. De la sucesión exacta

$$\mathcal{O}/\mathfrak{m}^n \xrightarrow{t\cdot} \mathcal{O}/\mathfrak{m}^{n+1} \to \bar{\mathcal{O}}/\bar{\mathfrak{m}}^{n+1} \to 0$$

se deduce que $S_{\bar{\mathcal{O}}}(n+1) \geq S_{\mathcal{O}}(n+1) - S_{\mathcal{O}}(n) = \Delta S_{\mathcal{O}}(n)$. Aplicando Δ^{d-1} (con $d = \dim \mathcal{O}$) se concluye. □

4. Proposición: *Sea $\pi : \widetilde{H} \to H$ 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 $\mathcal{T}_x H$.*

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 8

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.

8.1. 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.

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 sólo 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 sólo 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 sólo 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 $f \in R = k[x_1, \ldots, x_r]$ homogénea.

1. Si $max_{>_{hlex}} f \in k[x_s, \ldots, x_r]$ para algún s, entonces $f \in k[x_s, \ldots, x_r]$.
2. Si $max_{>_{ilex}} f \in (x_s, \ldots, x_r)$ para algún s, entonces $f \in (x_s, \ldots, x_r)$.

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 $G_i E := E_i / \cup_{j<i} E_j$ y $GE := \oplus_{i \in I} G_i E$ (si $0 \in I$ es el mínimo de I, definimos $G_0 E := E_0$).

8. Lema: *Si para cada $i \in I$, $\{e_{ij}\}_j$ son vectores de E_i cuyas clases forman una base de $G_i E$ 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 $G_i E$ 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 $0 \neq \bar{e} \in G_i E$, 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, $0 \neq \bar{e'} \in G_i E'$. Sea $\bar{e} \in G_i E$, tal que $GT(\bar{e}) = \bar{e'}$. Entonces, $\overline{e' - T(e)} = 0 \in G_i E'$, 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

$$\{L_{\leq m} := [k\text{-subespacio vectorial de } L \text{ generado por los monomios menores o iguales que } m]\}_{m \in I}.$$

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 8.1.9.

□

8.2. 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 8.1.4), 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 $M = \langle f_1, \ldots, f_t\rangle \subseteq L$ 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 $f_1, \ldots, f_t$. Entonces, $f_1, \ldots, f_t$ forman una base de Gröbner de M si y sólo 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 $\pi\colon R^t \to M$, $\pi(\xi_i) = f_i$.

Consideremos en R^t el orden monomial $>$ definido por: $x^\alpha\cdot\xi_i > x^\beta\cdot\xi_j$ si $max(x^\alpha\cdot f_i) > max(x^\beta\cdot f_j)$ o $max(x^\alpha\cdot f_i) = max(x^\beta\cdot f_j)$ (salvo un escalar) e $i<j$. Sea J el conjunto de los monomios de R^t.

Consideremos en M la filtración $\{M_{\le x^\alpha\cdot\xi_i} := \pi((R^t)_{\le x^\alpha\cdot\xi_i})\}_{x^\alpha\cdot\xi_i\in J}$. Se cumple que

$$G_{x^\alpha\cdot\xi_i}M = \begin{cases} 0, & \text{si existe } x^\beta\xi_j < x^\alpha\cdot\xi_i \text{ de modo que } x^\beta\cdot max(f_j) = x^\alpha\cdot max(f_i).\\ k\cdot\overline{x^\alpha\cdot f_i}\neq 0, & \text{en otro caso.}\end{cases}$$

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 $M_{\le x^\beta\cdot\xi_j}$ porque para todo término $x^{\gamma'}$ de p_k no nulo, se cumple que $x^\gamma\cdot x^{\gamma'}\cdot\text{máx}(f_k) \le x^\gamma\cdot\text{máx}(p_k f_k) \le x^\gamma\cdot\text{máx}(f_{ij}) < \text{máx}(x^\beta f_j) = x^\beta\,\text{máx}(f_j)$. Por tanto, $x^\alpha\cdot f_i \in M_{\le x^\beta\cdot\xi_j}$, $M_{\le x^\alpha\cdot\xi_i} = M_{\le x^\beta\cdot\xi_j}$ 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 $f\in M_{\le x^\alpha\cdot\xi_i}$. Entonces, $0\neq\bar f\in G_{x^\alpha\cdot\xi_i}$ 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, $max(M) = \langle max(f_1),\dots,max(f_t)\rangle$.

□

5. Observación: El criterio de Buchberger nos da un algoritmo para calcular una base de Gröbner. Dado un submódulo $M = \langle f_1,\dots,f_t\rangle \subset L$ si $f_1,\dots,f_t$ no forman una base de Gröbner entonces algún $f'_{ij}\neq 0$ (seguimos notaciones del criterio). Sustituyamos $f_1,\dots,f_t$ por $f_1,\dots,f_t,f'_{ij}$ y repitamos el proceso. Este proceso termina en un número finito de pasos ya que las inclusiones $\langle max(f_1),\dots,max(f_t)\rangle \subsetneq \langle max(f_1),\dots,max(f_t),max(f'_{ij})\rangle$ son estrictas.

6. Teorema de Schreyer: *Sea $M = \langle g_1,\dots,g_t\rangle \subseteq L$ 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 $g_1,\dots,g_t$. Por el criterio de Buchberger, $g'_{ij} = 0$, para todo i,j.

Sea R^t un módulo libre de base $\xi_1,\dots,\xi_t$, $\pi\colon R^t\to M$ el epimorfismo de módulos definido por $\pi(\xi_i) = g_i$ y $\phi\colon \Lambda^2R^t\to R^t$ el morfismo definido por

$$\phi(\xi_i\wedge\xi_j) = \begin{cases} 0, \text{ si } max(g_i) \text{ no contiene el mismo vector de la base de } L \text{ que } max(g_j).\\ (max(g_j)/m_{ij})\cdot\xi_i - (max(g_i)/m_{ij})\cdot\xi_j - \sum_k p_k\xi_k, \text{ si } max(g_i) \text{ contiene el mismo vector}\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{de la base que } max(g_j).\end{cases}$$

Entonces, la sucesión

$$\Lambda^2R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$$

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 8.1.9, 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

$$G_{x^\alpha \cdot \xi_i} M = \begin{cases} 0, & \text{si existe } x^\beta \xi_j < x^\alpha \cdot \xi_i \text{ de modo que } x^\beta \cdot max(g_j) = x^\alpha \cdot max(g_i). \\ k \cdot \overline{x^\alpha \cdot g_i} \neq 0, & \text{en otro caso.} \end{cases}$$

Definamos

$$(\Lambda^2 R^t)_{x^\alpha \cdot \xi_i} := \oplus_{\substack{j > i, \\ x^\gamma \cdot max(g_j)/m_{ij} = x^\alpha}} k \cdot x^\gamma \cdot \xi_i \wedge \xi_j$$

Existe x^γ (único) tal que $x^\gamma \cdot max(g_j)/m_{ij} = x^\alpha$ si y sólo 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 sólo 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 8.1.9, $\Lambda^2 R^t \to \operatorname{Ker}\pi$ 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 $\varphi : R^{t'} \to R^t$ el epimorfismo definido por $\varphi(\xi_i) = \sum_j p_{ij} \xi_j$ y $\pi : R^t \to M$, $\pi(\xi_i) = f_i$. 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.

8.3. Aplicaciones

En las distintas aplicaciones se supondrá que el lector ya conoce diversos conceptos como: extens y tores de módulos (ver sección 6.3), variedad afín, espectro proyectivo (ver sección 3.8), explosión a lo largo de un cerrado (ver sección 5.6), espacio tangente en un punto (ver subsección 4.2.1), etc.

8.3.1. Teoría de la eliminación

Dado un sistema de ecuaciones $p_1(x_1,\dots,x_r)=0,\dots,p_t(x_1,\dots,x_r)=0$ queremos eliminar las variables $x_1,\dots,x_s$. Es decir, queremos calcular qué relaciones algebraicas cumplen

$$\bar{x}_{s+1},\dots,\bar{x}_r \in k[x_1,\dots,x_r]/(p_1,\dots,p_t)$$

Con precisión, queremos calcular el núcleo del morfismo $k[x_{s+1},\dots,x_r]\to k[x_1,\dots,x_r]/(p_1,\dots,p_t)$, que es $k[x_{s+1},\dots,x_r]\cap(p_1,\dots,p_t)$. Geométricamente, queremos calcular el cierre de la imagen del morfismo

$$\operatorname{Spec} k[x_1,\dots,x_r]/(p_1,\dots,p_t)\to \mathbb{A}^{r-s}=\operatorname{Spec} k[x_{s+1},\dots,x_r],\ (\alpha_1,\dots,\alpha_r)\mapsto(\alpha_{s+1},\dots,\alpha_r)$$

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

$$\begin{array}{ccc} X=\operatorname{Spec} k[x_1,\dots,x_r]/(p_1,\dots,p_t) & \to & Y=\operatorname{Spec} k[y_1,\dots,y_s]/(p'_1,\dots,p'_{t'}) \\ (\alpha_1,\dots,\alpha_r) & \mapsto & (q_1(\alpha_1,\dots,\alpha_r),\dots,q_s(\alpha_1,\dots,\alpha_r)) \end{array}$$

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 $x_1,\dots,x_s$, por tanto $max(f)\in\langle max(g_1),\dots,max(g_{t'})\rangle_{k[x_{s+1},\dots,x_r]}$. 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_IA, como sigue

$$D_IA:=A\oplus I\oplus\cdots\oplus I^n\oplus\cdots=A[\xi_1\cdot t,\dots,\xi_s\cdot t]\subseteq A[t]$$

Luego, $D_IA=k[\bar{x}_1,\dots,\bar{x}_r,\xi_1\cdot t,\dots,\xi_s\cdot t]\subset A[t]=k[x_1,\dots,x_r,t]/(p_1,\dots,p_r)$, 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 $\operatorname{Proj} D_IA$ es la explosión de $\operatorname{Spec} A$ a lo largo de $(I)_0$. Se cumple que

$$\operatorname{Proj} D_IA=\cup_i \operatorname{Spec} A[\xi_1/\xi_i,\dots,\xi_s/\xi_i].$$

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.

8.3.2. 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 $k[x_1,\ldots,x_r]$. La filtración $\{S_{\leq x^\alpha} := \overline{k[x_1,\ldots,x_r]_{\leq x^\alpha}}\}_{x^\alpha\in I}$ 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,

$$\dim_k [S]_n = \dim_k([S]_{\leq n}/[S]_{\leq n-1}) = \sum_{|x^\alpha|=n} \dim_k G_{x^\alpha} S = \dim_k [GS]_n$$

□

Sea ahora $I = (m_1,\ldots,m_t) \subseteq k[x_1,\ldots,x_r]$ un ideal generado por monomios. Calculemos, por inducción sobre t, la función de Hilbert de R/I. Sean

$$I' := (m_2,\ldots,m_t) \text{ e } I'' := (m_2/m.c.d.(m_2,m_1),\ldots,m_t/m.c.d.(m_t,m_1))$$

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 $d = \mathrm{gr}(m_1)$.

8.3.3. 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.

4. 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. □

8.3.4. 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 $C = \mathrm{Proj}\, k[x_1,\ldots,x_{r+1}]/I$ y $C_0 = \mathrm{Proj}\, k[x_1,\ldots,x_{r+1}]/I_0$. El polinomio de Hilbert de C, que es el polinomio de Hilbert de $k[x_1,\ldots,x_r]/I$, coincide con el polinomio de Hilbert de C_0, pues es el polinomio de Hilbert de $k[x_1,\ldots,x_r]/I_0$.

Sea m_i' el máximo grado con el que aparece la variable x_i en todos los monomios 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 $C_t := \text{Proj}\, k[t][x_1,\dots,x_r]/I_t$ y consideremos el morfismo natural $\pi\colon C_t \to \text{Spec}\, k[t] = \mathbb{A}^1$. 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 [23]). En conclusión, hemos obtenido el siguiente teorema.

5. Teorema: *El morfismo $\pi\colon C_t \to \mathbb{A}^1$ es una deformación plana de C a C_0.*

8.3.5. 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 $X = \text{Spec}\, k[x_1,\dots,x_r]/I$, se denomina espacio tangente a X en el origen a $T_0X := \text{Spec}\, k[x_1,\dots,x_r]/I_b$. Calculemos I_b.

6. 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 $\{k[x_0,\dots,x_r]_{\le(m,n)} := \{\text{polinomios de grado menor o igual que } m, \text{ de grado en } x_0 \text{ menor o igual que } n\}\}_{(m,n)}$ (suponemos $m \ge n$ 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, $n = m - \text{gr}\, f_b$ 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, $F \in k[x_0,\dots,x_r]_{\le(m,n)}$ 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 $\{k[x_0,\dots,x_r]_{\le(m,n)} \cap J\}$, 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: $k[x_0,\dots,x_r]_{\le(m,n)} = k[x_0,\dots,x_r]_{\le x_0^n\cdot x_1^{m-n}}$. Por tanto, graduar primero por la filtración recién definida y después por la filtración del orden lexicográfico homogéneo (que denotaremos $G_\le$) es igual a graduar por el orden lexicográfico homogéneo. Tenemos que $(max(G_1),\dots,max(G_{t'})) \subseteq G_\le(\bar{G}_1,\dots,\bar{G}_{t'}) \subseteq G_\le GJ = G_\le J = (max(G_1),\dots,max(G_{t'}))$. Por tanto, la inclusión $(\bar{G}_1,\dots,\bar{G}_{t'}) \subseteq GJ$ al graduar es epiyectiva, luego es epiyectiva.

□

8.3.6. 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 8.2.2, 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 $f=\sum_i p'_i f_i$.

Recordemos que (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 8.2.2, 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.

8.3.7. 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 $L_2\to L_1\to N\to 0$.

7. 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.

8. Dado un módulo $N=L/\langle l_i\rangle$ y $N'=\langle\overline{l'_j}\rangle\subseteq N$, entonces tenemos dado $N/N'=L/\langle l_i,l'_j\rangle$.

9. 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 8.2.7. 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.

10. 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 $F\colon L_1\to L'_1$ 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 $\phi'\colon L'_2\to M$ un epimorfismo de un libre L'_2 en M. Consideremos el morfismo $H\colon L_1\oplus L'_2\to L'_1$, $H(l_1,l'_2):=F(l_1)-\phi'(l'_2)$. Por el teorema de Schreyer, sabemos calcular $\operatorname{Ker} H$ y si $\pi_1\colon L_1\oplus L'_2\to L_1$ es la proyección en el primer factor tenemos que $\pi_1(\operatorname{Ker} H)=F^{-1}(M)$.

Consideremos, ahora, un morfismo $F\colon L_1\to L'_1$ que haga conmutativo el diagrama de filas exactas

$$\begin{array}{ccccccc} L_2 & \xrightarrow{\phi} & L_1 & \xrightarrow{\pi} & N & \longrightarrow & 0\\ & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f} & & \\ L'_2 & \xrightarrow{\phi'} & L'_1 & \xrightarrow{\pi'} & N' & \longrightarrow & 0 \end{array}$$

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.

11. 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, $i^{-1}(I') = I \cap I'$. □

8.3.8. Cálculo de extens y tores.

Sabemos calcular $\mathrm{Hom}_{R'}(N, N')$: Tomemos $\mathrm{Hom}_{R'}(-, N')$ en la presentación $L_2 \xrightarrow{\phi} L_1 \xrightarrow{\pi} N \to 0$ y obtenemos la sucesión exacta

$$0 \to \mathrm{Hom}_{R'}(N, N') \xrightarrow{\pi^*} \mathrm{Hom}_{R'}(L_1, N') = \oplus^{n_1} N' \xrightarrow{\phi^*} \mathrm{Hom}_{R'}(L_2, N') = \oplus^{n_2} N'$$

(donde n_1 y n_2 son los rangos de los módulos libres L_1 y L_2 respectivamente). Luego, $\mathrm{Hom}_{R'}(N, N') = \mathrm{Ker}\,\phi^*$, 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 $N \otimes_{R'} N'$: Si $N = L/M$ 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.

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] BOURBAKI, N.: *Algèbre*, Elements de Mathematique, Masson, Paris, 1981.

[4] BOREVICH, Z.I. AND SHAFAREVICH, I.R.: *Number Theory*, Academic Press, Inc. 1966.

[5] DORRONSORO J. AND HERNÁNDEZ, E.: *Números, grupos y anillos*, Addison-Wesley/Universidad Autónoma de Madrid, Madrid, 1996.

[6] GAAL, L.: *Classical Galois Theory*, Chelsea Publishing Company, NY, 1973.

[7] GROTHENDIECK, A.; DIEUDONNÉ, J. A.: *Eléments de géométrie algébrique I*. Springer-Verlag (1971)

[8] GROTHENDIECK A.;, DIEUDONNÉ J.: *Eléments de géométrie algébrique IV*, Pub. Math. IHES, Springer-Verlag (1971).

[9] HARTSHORNE, R.: *Algebraic Geometry*, GTM, Vol **52**, Springer-Verlag, New York 1977.

[10] KOSTRIKIN, A.I.: *Introducción al algebra*, McGraw-Hill/Interamericana de España, Madrid, 1992.

[11] LANG, S.: *Álgebra*, Aguilar S.A. de ediciones, Madrid, 1971.

[12] MILNE, J.S.: *Field and Galois theory*, 2002.

[13] MATSUMURA, H.: *Commutative ring theory*. Cambridge University Press (1980)

[14] MUMFORD, D.: *Lecture on curves on an algebraic surface*. Annals of Mathematics Studies 59. Princeton University Press (1966).

[15] MUMFORD, D.: *Algebraic Geometry I*, Springer Verlag, 1976.

[16] NAGATA, M.: *Local Rings*, Interscience Tracts, 13, Interscience, 1962

[17] NAVARRO GONZÁLEZ, J.A.: *Teoría de Galois*, Sección de Matemáticas, vol. 5, Universidad de Extremadura, 1984.

[18] NAVARRO GONZÁLEZ, J.A.: *Álgebra conmutativa básica*, Manuales de Unex, vol. 19, Universidad de Extremadura, 1996.

[19] NORTHCOTT, D.G.: *Lessons on rings, modules and multiplicités*, Cambridge University Press, 1968.

[20] NEUKIRCH, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg 1999.

[21] PASTOR, R.: *Lecciones de Álgebra*, Nuevas Gráficas, Madrid, 1960.

[22] ROTMAN, J.:*An introduction to homological Algebra*, New York Academic Press, 1979.

[23] SANCHO, F.; SANCHO, P.J.: *Geometría Alegebraica Global* 2012.

[24] SERRE, J.P.:*Algèbre locale multiplicités*, Lecture Notes in Mathematics, 11, Springer Verlag, 1965.

[25] STEWART, I.:*Galois Theory*, Chapman and Hall mathematics series, London 1973.

[26] VAN DER WAERDEN, B.L.:*Algebra*, vol 1,2, Frederik Ungar Publi. Co. New York, 1970.

[27] ZARISKI, O., SAMUEL, P.:*Commutative Algebra*, vol I,II, Van Nostrand 1958.

Índice alfabético

A-álgebras, 71
Acíclico, 287
Álgebra de tipo finito, 55
Álgebra exterior de un módulo, 75
Álgebra finita, 58
Álgebra graduada, 73, 193
Álgebra graduada anticonmutativa, 75
Álgebra racional, 132
Álgebra simétrica de un módulo, 74
Álgebra tensorial de un módulo, 73
Altura de un ideal primo, 300
Anillo, 25
Anillo íntegramente cerrado, 176
Anillo íntegro, 25
Anillo artiniano, 304
Anillo conmutativo con unidad, 25
Anillo de Cohen-Macaulay, 302
Anillo de enteros, 234
Anillo de enteros de un cuerpo, 235
Anillo de la explosión, 260
Anillo de la transformación cuadrática, 260
Anillo de Rees, 258
Anillo de valoración, 230
Anillo de valoración discreta, 230
Anillo henseliano, 226
Anillo local, 43
Anillo local regular, 217
Anillo noetheriano, 53
Anillo normal, 176
Aplicación bilineal, 69
Aplicación multilineal hemisimétrica, 75
Aplicación multilineal lineal simétrica, 74
Árbol de explosión, 261
Automorfismo de Frobenius, 142
Automorfismo interno, 92

Base de Gröbner, 331
Base de trascendencia, 104

Cambio de base, 71
Característica de un cuerpo, 136
Categoría, 65
Categoría abeliana, 68
Categoría aditiva, 68
Categorías anti-equivalentes, 66
Categorías equivalentes, 66
Centro de un grupo, 21
Centro permisible de explosión, 322
Cerrado irreducible, 37
Ciclo excepcional, 259
Ciclos y bordes, 287
Cierre algebraico, 103
Cierre entero, 176
Codimensión, 183
Cohomología de un complejo, 289
Complejo, 289
Complejo de Koszul, 296
Componente irreducible, 37
Componente sumergida, 171
Conúcleo o Coker, 68
Congruencia de Euler, 31
Conjunto filtrante creciente, 86
Conjunto filtrante decreciente, 85
Cono de un morfismo, 291
Cono normal, 212
Cono tangente, 212
Contacto maximal, 265
Criterio de Buchberger, 331
Criterio de Eisenstein, 41
Criterio ideal de platitud, 293
Criterio local de platitud, 306
Criterio topológico de Nagata, 310
Cuasi-isomorfismo, 289
Cuerpo, 25
Cuerpo algebraicamente cerrado, 103
Cuerpo de descomposición, 134
Cuerpo de fracciones, 40
Cuerpo de números, 234
Cuerpo finito, 141
Cuerpo residual de un punto del espectro, 78
Curva íntegra afín, 235
Curva proyectiva, 195

Derivación, 185
Descomposición primaria reducida, 171
Determinante de Vandermonde, 108
DFU, 40
Diferencial, 184
Diferente, 278
Dimensión de Krull, 176

Dimensión global, 299
Dimensión inyectiva de un módulo, 304
Dimensión proyectiva, 298
Discriminante de la traza, 278
Discriminante de un polinomio, 108
Divisor de cero, 25
Divisores afinmente equivalentes, 245
Divisores afines, 245
Divisores completos, 246
Divisores elementales, 63
Dominio de Dedekind, 232
Dominio de factorización única, 40
Dominio de ideales principales, 25

Elemento algebraico, 102
Elemento entero, 175
Elemento irreducible, 27
Elemento primitivo, 136
Elementos algebraicamente independientes, 104
Elementos de un grupo conjugados, 16
Envolvente normal, 134
Espacio cotangente de Zariski, 217
Espacio noetheriano, 54
Espacio normal, 212
Espacio tangente, 212
Espectro primo, 36
Espectro primo racional, 35
Espectro proyectivo, 193
Exceso de una función racional, 119
Extensión de álgebras, 312
Extensión de cuerpos, 101
Extensión de cuerpos algebraica, 102
Extensión de cuerpos de tipo finito, 104
Extensión finita de cuerpos, 101
Extensión por radicales cuadráticos, 155

Factores invariantes, 64
Fibra excepcional, 261
Filtración I-ádica, 222
Filtración I-estable, 214
Filtración de un módulo, 212
Forma de una permutación, 16
Fórmula de clases, 21
Fórmula de Girard, 107
Fórmula de la fibra, 44
Fórmula de las gráficas, 273
Fórmulas de Cardano, 105
Fórmulas de Newton, 107
Función de Hilbert, 213
Función de Samuel, 213
Función zeta ζ, 255
Funciones simétricas elementales, 105
Functor exacto por la derecha, 69
Functor exacto por la izquierda, 69
Funtor aditivo, 68
Funtor contravariante, 66
Funtor covariante, 66
Funtor de puntos, 68

G-conjunto, 19
Grado de trascendencia, 104
Grado de un divisor, 247
Grado de un polinomio, 26
Grado de una extensión finita de cuerpos, 101
Graduado por una filtración, 212
Grupo, 11
Grupo abeliano, 11
Grupo alternado, 17
Grupo conmutativo, 11
Grupo de cohomología, 287
Grupo de descomposición, 276
Grupo de isotropía, 20
Grupo de Klein, 161
Grupo de Picard, 245
Grupo de Picard completo, 246
Grupo diédrico, 19
Grupo resoluble, 159
Grupo simple, 159

Homología de un complejo, 289

I-filtración, 214
I-idealmente separado, 306
Ideal, 25
Ideal $\mathfrak{p}$-primario, 169
Ideal anulador de un módulo, 51
Ideal de la diagonal, 184
Ideal de valoración, 230
Ideal fraccionario, 245
Ideal homogéneo, 193
Ideal irreducible, 170
Ideal irrelevante, 193
Ideal maximal, 33
Ideal primario, 169
Ideal primo, 33
Ideal primo minimal, 34
Ideal primo racional, 35
Ideal principal, 25
Ideales de Fitting, 64, 82
Ideales primos asociados, 172
Identidad de Bézout, 26
Índice de ramificación, 234
Inducción noetheriana, 311
Inmersión cerrada, 297
Inmersión cerrada regular, 297
Irracional cuadrático, 156

Kunneth, 315

Limite proyectivo, 87

Limite proyectivo, 85
Lema de Euclides, 27
Lema de Hensel, 227
Lema de Krull, 215
Lema de Nakayama, 49
Lema de normalización de Noether, 179
Localización de un anillo, 40
Locus singular del exponente idealístico, 324
Longitud de un módulo, 56

Metrica de la traza, 278
Modulo, 46
Modulo de diferenciales de Kähler, 184
Modulo de división, 294
Modulo de presentación finita, 62
Modulo de torsión, 60
Modulo diferencial, 287
Modulo fielmente plano, 79
Modulo finito generado, 48
Modulo graduado, 213
Modulo inyectivo, 294
Modulo libre, 48
Modulo libre de torsión, 60
Modulo monógeno, 63
Modulo noetheriano, 53
Modulo plano, 77
Modulo proyectivo, 79
Modulo simple, 55
Morfismo birracional, 207
Morfismo de anillos, 29
Morfismo de anillos dominante, 308
Morfismo de anillos fielmente plano, 79
Morfismo de anillos plano, 79
Morfismo de explosión, 258
Morfismo de grupos, 13
Morfismo de módulos, 47
Morfismo de variedades algebraicas, 179
Morfismo diferencial, 287
Morfismo dominante, 236
Morfismo entero, 176
Morfismo finito, 175
Morfismo formalmente liso, 314
Morfismo liso, 311
Multiplicidad de intersección, 263
Multiplicidad en un punto, 261

Norma de un ideal fraccionario, 247
Normal platitud, 318
Normalizador de un subgrupo, 18
Núcleo de un morfismo de grupos, 13
Núcleo de un morfismo de módulos, 47
Número de puntos contando multiplicidades, 58
Número de puntos contando multiplicidades y grados, 233

Operador de Euler, 30
Órbita de un punto, 20
Orden lexicográfico, 329
Orden lexicográfico homogéneo, 329
Orden lexicográfico inverso, 329
Orden monomial, 329

p-grupo, 21
Polinomio característico, 65
Polinomio ciclotómico, 32
Polinomio de Hilbert, 214
Polinomio de Samuel, 214
Polinomio primitivo, 41
Presentación libre de un módulo, 62
Primo de Fermat, 158
Primos entre sí, 27
Producto tensorial de módulos, 69
Profundidad de un módulo, 301
Punto cuspidal, 265
Punto de ramificación, 234
Punto genérico, 38
Punto liso, 189
Punto no singular, 232
Punto rama, 234
Punto singular, 232

Radical de Jacobson, 52
Radical de un anillo, 44
Radical de un ideal, 44
Ramas analíticas, 264
Ramificación, 278
Rango de un módulo, 59
Red, 248
Resolución de un módulo por libres, 293
Resolvente de Lagrange, 146
Resultante d Euler, 113
Resultante de Bézout, 114
Resultante de dos polinomios, 110
Resultante de Euler (Cayley-Sylvester), 113
Revestimiento, 271
Revestimiento no ramificado o puro, 273
Revestimiento principal o de Galois, 274
Revestimiento trivial, 272

Serie de composición de módulos, 56
Signo de una permutación, 17
Sistema de parámetros, 216
Sistema generador de un módulo, 48
Sistema inductivo de objetos, 87
Sistema multiplicativo, 39
Sistema proyectivo de objetos, 85
Soporte de un módulo, 51
Subanillo, 29
Subgrupo de Sylow, 22
Subgrupo de un grupo, 11

Subgrupo metacíclico, 163
Subgrupo transitivo, 20
Submódulo, 47
Sucesión exacta de módulos, 50
Sucesión exacta escindida, 95
Sucesión exacta que rompe, 95

Tangente estricto, 326
Teorema chino de los restos, 30
Teorema de Artin-Rees, 215
Teorema de Bézout, 268
Teorema de Budan-Fourier, 123
Teorema de Cauchy, 22
Teorema de Cohen, 225
Teorema de Descartes, 123
Teorema de Dirichlet, 252
Teorema de Govorov-Lazard, 89
Teorema de Hamilton-Cayley, 65
Teorema de Hermite, 251
Teorema de Kronecker, 103
Teorema de la base de Hilbert, 55
Teorema de los ceros de Hilbert, 180
Teorema de Macaulay, 331
Teorema de Pappus, 284
Teorema de Pascal, 284
Teorema de representabilidad, 90
Teorema de Riemann-Roch débil, 250
Teorema de Schreyer, 332
Teorema de Sturm, 122
Teorema del ascenso, 177
Teorema del ascenso de ideales, 177
Teorema del descenso de Cohen-Seidenberg, 178
Teorema del descenso de ideales, 177
Teorema del ideal principal de Krull, 181, 217
Teorema del punto de la red de Minkowski, 250
Teorema formal de la función inversa, 224
Teorema fuerte de los ceros de Hilbert, 180
Teorema fundamental del Álgebra, 107
Topología I-ádica, 222
Topología de Zariski, 36
Tores, 293
Torsión de un módulo, 59
Transformación cuadrática, 258
Transformada propia, 258

Valoración $\mathfrak{m}$-ádica, 230
Valoración discreta, 230
Variedad íntegra, 180
Variedad algebraica afín, 179
Variedad lisa, 189
Variedad proyectiva, 195
Variedad racional, 207
Variedad reducida, 180
Variedad regular, 219
Variedades catenarias, 182
Volumen de un paralelepípedo, 248