Variedades Algebraicas

Grado en Matemáticas

VARIEDADES ALGEBRAICAS

GRADO EN MATEMÁTICAS

PEDRO SANCHO DE SALAS

VARIEDADES ALGEBRAICAS

GRADO EN MATEMÁTICAS

UNIVERSIDAD DE EXTREMADURA

2025

Índice general

Introducción

Este texto pretende ser el manual de referencia de la asignatura cuatrimestral Álgebra II, del tercer curso del Grado de Matemáticas de la UEX. Esta asignatura es una introducción a la teoría de variedades algebraicas. Estudiamos las k-álgebras de tipo finito, la descomposición primaria y la teoría de la dimensión en variedades algebraicas afines y proyectivas. Se introducirán nuevas conceptos: el espectro primo de un anillo, la localización y el lenguaje categorial; y las herramientas necesarias para los cálculos: la resultante de dos polinomios y las bases de Gröbner.

El manual está divido en cinco capítulos. El capítulo 0 es un rápido repaso de la teoría de anillos, módulos, cocientes y productos tensoriales de álgebras y módulos En cada tema incluimos un cuestionario, una lista de problemas (con sus soluciones) y la biografía de un matemático relevante (en inglés).

Demos una breve explicación de las ideas claves que dan sentido a esta asignatura.

Simplificando y hablando de un modo algo pedante podríamos decir que el Álgebra es la ciencia que estudia los polinomios y sus raíces. En términos matemáticos algo más amplios, el Álgebra estudia los sistemas de ecuaciones algebraicas

$$\begin{array}{c} p_1(x_1,\ldots,x_n)=0 \\ \cdots \\ p_r(x_1,\ldots,x_n)=0 \end{array} \qquad (*)$$

y sus soluciones.

Profundicemos en lo que entendemos generalmente por sistemas de ecuaciones algebraicas. Tendemos a identificar los sistemas de ecuaciones con el conjunto de sus soluciones. Así, por ejemplo, si al sistema de ecuaciones anterior le añadimos la ecuación $p_1(x_1,\ldots,x_n)=0$ decimos que tenemos un sistema de ecuaciones equivalente, o si le añadimos una ecuación que sea combinación $k[x_1,\ldots,x_n]$-lineal de $p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n)$ decimos que tenemos un sistema equivalente de ecuaciones algebraicas, porque las soluciones de ambos sistemas son las mismas. En conclusión, cuando consideramos el sistema de ecuaciones $(*)$ estamos considerando el ideal $(p_1,\ldots,p_r)\subset k[x_1,\ldots,x_n]$. Digamos por definición, que dar un sistema de ecuaciones algebraicas es dar un ideal del anillo de polinomios.

¿Las soluciones de un sistema de ecuaciones algebraicas determinan el sistema, es decir, el ideal? El conjunto de soluciones reales del sistema

$$x^2 + y^2 + 1 = 0$$

es vacío, del cual, obviamente, no podríamos deducir que estábamos planteando la ecuación $x^2+y^2+1=0$. Ahora bien, si consideramos el conjunto de todas las soluciones complejas de este sistema, se cumple que el ideal de todos los polinomios de $\mathbb{C}[x,y]$ que se anulan en este conjunto coincide con el ideal (x^2+y^2+1). El teorema de los ceros de Hilbert dice que las soluciones complejas de un sistema de ecuaciones "casi" determinan el sistema. Expliquemos el "casi" de la sentencia anterior. Veamos el pequeño problema con el que nos encontramos. Los dos sistemas de ecuaciones distintos $x=0$ y $x^2=0$ ($(x^2)\subsetneq(x)$) tienen las mismas soluciones. En general, dado un ideal $I\subset\mathbb{C}[x_1,\ldots,x_n]$ y $f\in\mathbb{C}[x_1,\ldots,x_n]$ tal que $f^m\in I$, las soluciones del sistema de ecuaciones algebraicas definido por I son las mismas que el definido por (I,f). Denotemos por $r(I)=\{f\in\mathbb{C}[x_1,\ldots,x_n]:\ \text{existe } n\in\mathbb{N} \text{ tal que } f^n\in I\}$. El teorema de los ceros de Hilbert afirma que dos sistemas de ecuaciones algebraicas $I,J\subseteq\mathbb{C}[x_1,\ldots,x_n]$ tienen el mismo conjunto de soluciones si y solo si $r(I)=r(J)$.

En el estudio de los sistemas de ecuaciones algebraicas hemos ampliado nuestro cuerpo de partida $\mathbb{R}$ a uno algebraicamente cerrado, $\mathbb{C}$. Si ampliamos aún más nuestro "marco", es decir, consideramos en vez de $\mathbb{C}$ cualquier anillo, se cumple que "las soluciones (sobre cualquier anillo) de un sistema de ecuaciones algebraicas I determinan el ideal I". Así por ejemplo, $x=0$ no tiene las mismas soluciones que $x^2=0$: sea $A=\mathbb{C}[z]/(z^2)$, entonces $\bar{z}\in A$ es una solución de $x^2=0$ y no es una solución de $x=0$.

Sea $I\subseteq k[x_1,\ldots,x_n]$ un sistema de ecuaciones algebraicas. Consideremos (para cada anillo A) el conjunto de soluciones de este sistema de ecuaciones algebraicas. Consideremos una función de este conjunto, es decir, una aplicación (para cada anillo A)

$$\{\text{Conjunto de soluciones sobre } A \text{ del sistema } I\} \xrightarrow{\phi_A} A$$

Existe un único $\overline{p(x_1,\ldots,x_n)}\in k[x_1,\ldots,x_n]/I$ de modo que $\phi_A((a_1,\ldots,a_n))=p(a_1,\ldots,a_n)$. Es decir, "el anillo de todas las funciones del conjunto de soluciones del sistema de ecuaciones algebraicas definido por I es $k[x_1,\ldots,x_n]/I$". Este tipo de anillos se denominan k-álgebras[1] de tipo finito.

Dados dos sistemas de ecuaciones algebraicas $I\subseteq k[x_1,\ldots,x_n]$, $J\subseteq k[y_1,\ldots,y_m]$ y una aplicación (para cada anillo A)

$$\{\text{Sol. con valores en } A \text{ del sistema } I\} \xrightarrow{\varphi_A} \{\text{Sol. con valores en } A \text{ del sistema } J\}$$

[1] La palabra álgebra es sinónimo de anillo. Decir que un anillo A es una k-álgebra, solo significa que tenemos un morfismo de anillos (inyectivo) $k\hookrightarrow A$.

existe un único morfismo de k-álgebras $f\colon k[y_1,\dots,y_m]/J \to k[x_1,\dots,x_m]/I$, $f(\bar{y}_i) = \overline{f_i(x_1,\dots,x_n)}$ de modo que

$$\varphi_A(a_1,\dots,a_n) = (f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n)).$$[2]

La teoría (Geometría) que estudia los conjuntos de soluciones (sobre todo anillo) de un sistema de ecuaciones k-algebraicas y sus aplicaciones coincide con la teoría (Álgebra) que estudia las k-álgebras de tipo finito y sus morfismos de k-álgebras.

Sea $\bar{k}$ el cierre algebraico del cuerpo k y $\tau\colon \bar{k} \simeq \bar{k}$ un isomorfismo de k-álgebras. Si $\alpha = (\alpha_1,\dots,\alpha_n) \in \bar{k}^n$ es una solución del sistema de ecuaciones k-algebraicas definido por un ideal I, entonces $\tau(\alpha) := (\overline{\tau(a_1),\dots,\tau(a_n)})$ también es una solución del sistema de ecuaciones. Además, $\mathfrak{p}_\alpha := \{\overline{p(x_1,\dots,x_n)} \in k[x_1,\dots,x_n]/I\colon p(a_1,\dots,a_n) = 0\}$ es un ideal primo maximal y $\mathfrak{p}_\alpha = \mathfrak{p}_{\tau(\alpha)}$. Por el teorema de los ceros de Hilbert, el conjunto de soluciones sobre $\bar{k}$ del sistema de ecuaciones definido por I, módulo automorfismos de k-álgebras de $\bar{k}$, es biyectivo con el conjunto de ideales primos maximales de $k[x_1,\dots,x_n]/I$, conjunto que denotamos $\operatorname{Spec}_{max} k[x_1,\dots,x_n]/I$. Por ejemplo, el conjunto de las soluciones reales de $x^2+y^2+1=0$ es vacío, sin embargo $\operatorname{Spec}_{max} \mathbb{R}[x]/(x^2+y^2+1)$ es biyectivo con el conjunto $\{(\alpha_1,\alpha_2) \in \mathbb{C}^2\colon \alpha_1^2+\alpha_2^2+1=0\}/\sim$.

Sea $\operatorname{Spec} k[x_1,\dots,x_n]/I$ el conjunto de los ideales primos de $k[x_1,\dots,x_n]/I$ y consideremos en este conjunto la topología de Zariski, cuyos cerrados son los subconjuntos $(J)_0 = \{\mathfrak{p} \in \operatorname{Spec} k[x_1,\dots,x_n]/I\colon J \subset \mathfrak{p}\}$, donde J es un ideal de $k[x_1,\dots,x_n]/I$. Consideremos el subespacio topológico $\operatorname{Spec}_{max} k[x_1,\dots,x_n]/I$. Sea X el conjunto de soluciones sobre $\bar{k}$ del sistema I, módulo automorfismos de $\bar{k}$, y cuyos cerrados son $V(J) := \{[\alpha] \in X\colon f(\alpha) = 0, \forall f \in J\}$. El teorema de los cerros de Hilbert prueba que

$$\begin{array}{ccccc} \text{Top. de } \operatorname{Spec} k[x_1,\dots,x_n]/I & = & \text{Top. de } \operatorname{Spec}_{max} k[x_1,\dots,x_n]/I & = & \text{Top. de } X \\ (J)_0 & \longmapsto & (J)_0 \cap \operatorname{Spec}_{max} k[x_1,\dots,x_n]/I & \longmapsto & V(J) \end{array}$$

Vía el espectro, la interacción entre el Álgebra y la Geometría es fecunda. Así los conceptos algebraicos como morfismo de localización, morfismo de paso al cociente cociente y el producto tensorial de álgebras se interpretan geométricamente como la inmersión de un abierto y un cerrado en la variedad algebraica y como el producto directo de variedades algebraicas.

[2] Quisiera hacer aquí un comentario marginal: Nos han aparecido en este curso de Geometría Algebraica conceptos como "espacio de soluciones" (de un sistema de ecuaciones algebraicas) y "aplicaciones' (algebraicas) entre los espacios de soluciones. En Álgebra Lineal aparecen los conceptos de espacio vectorial y las aplicaciones lineales. En Topología aparecen los conceptos de espacio topológico y las aplicaciones continuas. En Geometría Diferencial aparecen las variedades diferenciales y las aplicaciones diferenciales.

¿Cómo podríamos definir la dimensión de X? Dada una variedad lineal afín V, sabemos que todas las cadenas irrefinables de inclusiones de subvariedades lineales $V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_m = V$ tienen el mismo número de eslabones y este número m se dice que es la dimensión de V. Supongamos que X es irreducible. Se cumple que todas las cadenas irrefinables de inclusiones de cerrados irreducibles de X tienen el mismo número de eslabones y se dice que este número es la dimensión de X. Probamos que un cerrado $Y \subset X$ es irreducible si y solo si $\mathfrak{p}_Y = \{f \in k[x_1,\ldots,x_n]\colon f(y) = 0, \forall\, y \in Y\}$ es un ideal primo. Probamos que la dimensión de X coincide con el número de eslabones de las cadenas irrefinables de inclusiones de ideales primos de $k[x_1,\ldots,x_n]/I$.

Un estudio fino de los sistemas de ecuaciones debe distinguir el sistema de ecuaciones $x = 0, y = 0$ del sistema de ecuaciones $x = 0, y^2 = 0$. El ideal (x,y) es el ideal de los polinomios $p(x,y) \in \mathbb{C}[x,y]$ tales que $p(0,0) = 0$ y $(x,y^2) = \{p(x,y) \in \mathbb{C}[x,y]\colon p(0,0) = 0$ y $\frac{\partial p(x,y)}{\partial y} = 0\}$, (x,y^2) es el ideal de las funciones que se anulan en $(0,0)$ y cumplen ciertas condiciones infinitesimales en $(0,0)$. Dado un cerrado irreducible $C \subset \mathbb{C}^n$ y el ideal primo $\mathfrak{p}_C := \{p(x_1,\ldots,x_n) \in \mathbb{C}[x_1,\ldots,x_n]\colon p(c) = 0, \forall\, c \in C\}$, se dice que un ideal $\mathfrak{q}$ es un ideal $\mathfrak{p}_C$ primario si $\mathfrak{q}$ es el ideal de polinomios que se anulan en todos los puntos de C y cumplen ciertas condiciones infinitesimales a lo largo de C (hablo sin precisión). Probamos que dar un sistema de ecuaciones algebraicas es equivalente a dar ciertos cerrados irreducibles C_i (de modo que $\cup_i C_i$ es el conjunto de soluciones complejas del sistema) y ciertas condiciones infinitesimales a lo largo de cada C_i. Con otras palabras, todo ideal es la intersección de ideales primarios.

La pregunta sobre qué es un sistema de ecuaciones algebraicas, nos ha llevado a hablar de las k-álgebras de tipo finito, de su espectro primo, del concepto de dimensión, de la descomposición de un ideal como intersección de ideales primarios, etc. Otro problema de orden distinto es dar los algoritmos necesarios para que las operaciones y conceptos teóricos introducidos sean efectivamente calculables. En el capítulo 6, estudiaremos la resultante de dos polinomios y las bases de Gröbner de un ideal. Con estas herramientas resolveremos los sistemas de ecuaciones k-algebraicos, los sistemas de ecuaciones $k[x_1,\ldots,x_n]$-lineales, calcularemos la descomposición primaria de un ideal, el cierre de la imagen de un morfismo entre variedades algebraicas, el polinomio de Hilbert de una variedad proyectiva, etc.

Capítulo 0

Anillos y módulos

0.1. Introducción

El anillo por excelencia es el anillo de los números enteros, $\mathbb{Z}$. Clásicamente la rama de las Matemáticas que estudia el anillo de los números enteros es la Aritmética, actualmente la Teoría de Números.

Hay otros anillos también muy importantes. Dado un conjunto con cierta estructura se puede considerar el anillo formado por las funciones del conjunto que respeten la estructura considerada en el conjunto. Por ejemplo, dado $\mathbb{R}^n$ podemos estudiar el anillo de las funciones continuas reales de $\mathbb{R}^n$, o el anillo de las funciones infinito diferenciables de $\mathbb{R}^n$, o el anillo $\mathbb{R}[x_1,\ldots,x_n]$ de las funciones algebraicas de $\mathbb{R}^n$. Así desde este punto de vista, la Topología es la rama de las Matemáticas que estudia los anillos de las funciones continuas reales de los espacios topológicos, la Geometría Diferencial es la rama de las Matemáticas que estudia los anillos de las funciones infinito diferenciables reales de las variedades diferenciables, la Geometría Algebraica es la rama de las Matemáticas que estudia los anillos de las funciones algebraicas de las variedades algebraicas.

0.2. Anillos. Cuerpos

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

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

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

3. $ab = ba$, para todo $a, b \in A$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

0.2.1. Anillos euclídeos

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

1. $\delta(a) \leq \delta(ab)$, para todo $a, b \in A\backslash\{0\}$.
2. Para cada $a \in A$ y $b \in A$ no nulo, existen $c, r \in A$, de modo que $a = bc + r$, y r es nulo ó $\delta(r) < \delta(b)$.

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

Veamos algunos ejemplos de anillos euclídeos.

9. El anillo de los números enteros: *Definimos $\delta : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$, $\delta(n) := |n|$, donde $|n| = n$ si n es positivo y $|n| = -n$ si n es negativo. Es fácil demostrar que $(\mathbb{Z}, \delta)$ es un anillo euclídeo.*

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

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

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

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

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

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

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

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

2. $gr(r(x)) < gr(q(x))$.

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

Unicidad: Al lector. □

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

0.2.2. Ideales de un anillo

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

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

Dado $a \in A$, el conjunto $a \cdot A := \{a \cdot b \in A, \forall b \in A\}$ es un ideal de A. Si $I \subseteq \mathbb{Z}$ es un ideal no nulo, entonces si n es el número natural más pequeño que pertenece a I se cumple que $I = n \cdot \mathbb{Z}$.

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

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

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

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

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

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

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

□

El ideal $\mathfrak{p} = (2, x_1)$ del anillo $\mathbb{Z}[x_1, \ldots x_n]$ no es principal: un generador de $\mathfrak{p}$ sería un divisor de 2 y éstos son ± 1 y ± 2, y $1 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ y $2 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ son ideales distintos de $\mathfrak{p}$. 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 $n > 1$).

0.2.3. Morfismo de anillos. Cociente por un ideal

15. 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. $f(1) = 1$.

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

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

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

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

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

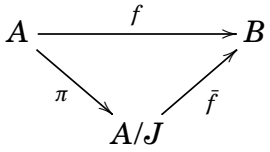
y $\bar{a} + \bar{b} := \overline{a+b}$. Recordemos que $\bar{a} = \bar{b}$ si y solo si $a - b \in I$. Podemos definir en A/I la operación "producto", $\bar{a} \cdot \bar{a'} := \overline{a \cdot a'}$, que dota a A/I de estructura de anillo (compruébese), y es la única estructura de anillo que podemos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

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

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

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

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

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

es un isomorfismo de anillos.

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

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

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

Observemos que el polinomio mínimo anulador de α, $p(x)$, es irreducible (es decir, no es producto de dos polinomios de grado menor que el de $p(x)$), porque si no lo es entonces $p(x)=p_1(x)\cdot p_2(x)$, con $\operatorname{gr}(p_1(x)),\operatorname{gr}(p_2(x))<\operatorname{gr}(p(x))$ y $p_1(x)$ ó $p_2(x)$ anula a α. Recíprocamente, si $p(x)$ es mónico, anula a α y es irreducible, entonces es el polinomio mónico mínimo anulador de α.

$k[x]/(p(x))$ es un k-espacio vectorial de base $\{\bar1,\bar x,\cdots,\bar x^{n-1}\}$, con $n=\operatorname{gr}(p(x))$: En efecto dado $\overline{q(x)}\in k[x]/(p(x))$, como $q(x)=c(x)\cdot p(x)+r(x)$, con $\operatorname{gr}(r(x))<n$, tenemos que $\overline{q(x)}=\overline{r(x)}$. Como $r(x)$ es combinación lineal de $1,\cdots,x^{n-1}$, $\{\bar1,\bar x,\cdots,\bar x^{n-1}\}$ es un sistema generador. Veamos que $\bar1,\bar x,\cdots,\bar x^{n-1}$ son linealmente independientes. Si

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

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

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

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

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

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

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

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

es un isomorfismo

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

Dados dos ideales $I_1, I_2 \subset A$, denotamos por $I_1 \cdot I_2$ el mínimo ideal de A que contiene al conjunto $\{i_1 \cdot i_2,\ \forall i_1 \in I_1, \forall i_2 \in I_2\}$. Si $I_1 + I_2 = A$ entonces $I_1 \cap I_2 = I_1 \cdot I_2$: Evidentemente $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. Sea $i_1 \in I_1$ e $i_2 \in I_2$, tales que $i_1 + i_2 = 1$. Dado $i \in I_1 \cap I_2$, se cumple que $i = i \cdot 1 = i \cdot i_1 + i \cdot i_2 \in I_1 \cdot I_2$. Por tanto, $I_1 \cap I_2 \subseteq I_1 \cdot I_2$.

0.2.4. Ideales primos. Ideales maximales

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

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

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

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

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

25. 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.

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

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

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

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

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

son inversas entre sí (y conservan inclusiones).

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

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

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

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

30. Proposición: *Un ideal $\mathfrak{m} \subsetneq A$ es maximal si y solo si $A/\mathfrak{m}$ es un cuerpo. En particular, por la proposición 0.2.23, los ideales maximales son ideales primos.*

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

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

32. Observación: Decimos que -5 es un elemento primo de $\mathbb{Z}$.

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

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

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

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

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

2. $\Rightarrow$ 1. Es consecuencia de 0.2.33.

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

□

0.2.5. Dominios de factorización única

35. Definición: Diremos que un anillo íntegro es un dominio de factorización única si todo elemento propio del anillo es producto de elementos irreducibles, de modo único salvo multiplicación por invertibles y orden de los factores.

36. Lema: *Sea A un anillo íntegro y $a, b \in A$. Si $(a) = (b)$, entonces $a = b \cdot i$, con $i \in A$ invertible.*

Demostración. Si $a = 0$, entonces $b = 0$ y $a = b \cdot 1$. Podemos suponer $a \neq 0$. $a = bc$ y $b = ad$, para ciertos $c, d \in A$. Por tanto, $a = bc = adc$ y $a(1 - dc) = 0$ y $1 - dc = 0$. Por tanto, c es invertible. □

37. Proposición: *Los dominios de ideales principales son dominios de factorización única.*

Demostración. Sea $a \in A$ un elemento propio. Probemos que a es producto de un numero finito de irreducibles. Si no lo es, entonces en particular $a = a_1 \cdot a_1'$, donde a_1 y a_1' son elementos propios. Además, uno de los dos, digamos a_1, no es producto de un número finito de irreducibles. De nuevo, $a_1 = a_2 a_2'$, donde a_2 y a_2' son elementos propios y a_2 no es producto de un número finito de elementos propios. Argumentando así sucesivamente, hemos obtenido una cadena de inclusiones estrictas (por el lema anterior)

$$(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} (a_n) \underset{\neq}{\subset}$$

$I := \underset{n\in\mathbb{N}}{\cup} (a_n)$ es un ideal, luego es principal $I = (b)$. Para cierto n, $b \in (a_n)$, luego $I = (a_n)$ y $(a_{n+1}) = (a_n)$ y hemos llegado a contradicción.

Probemos la unicidad. Supongamos que tenemos dos descomposiciones de a en producto de irreducibles $a = p_1 \cdots p_n = q_1 \cdots q_m$. Como p_1 es primo, entonces divide a alguno de los q_i. Como q_i es irreducible, $q_i = p_1 \cdot invertible$. Reordenado los factores, podemos suponer que $q_1 = p_1 \cdot invetible$. Por lo tanto, salvo multiplicación por invertibles $p_2 \cdots p_n = q_2 \cdots q_m$. Repitiendo este argumento de modo sucesivo terminamos con la demostración.

□

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

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

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

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

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

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

39. 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*

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

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

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

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

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

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

0.3. Módulos

El espacio vectorial es 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.

Sea A un anillo. Sin precisar, un A-módulo es un A-espacio vectorial, pero donde A es un anillo y no necesariamente un cuerpo. En esta capítulo iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (subespacios, sistemas generadores, cocientes, sumas y productos

directos, 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 estas operaciones (cocientes, sumas directas, etc.) aclara y simplifica muchos enunciados y demostraciones.

1. Definición: Sea A un anillo y M un conjunto. Diremos que una operación

$$M \times M \xrightarrow{+} M, (m, m') \mapsto m + m' \text{ y una aplicación } A \times M \xrightarrow{\cdot} M, (a, m) \mapsto a \cdot m,$$

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 $m \in M$.

Sea M un A-módulo. Cada elemento $a \in A$ define una aplicación

$$a\cdot \colon M \to M,\ m \mapsto a \cdot m.$$

El segundo punto expresa que $a\cdot$ es morfismo de grupos. En particular, $a \cdot 0 = 0$ y $a \cdot (-m) = -(a \cdot m)$.

Observemos que $0 \cdot m = 0$: $0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$, luego $0 \cdot m = 0$. Observemos que $(-a) \cdot m = -(a \cdot m)$, para todo $m \in M$: $0 = 0 \cdot m = (a + -a) \cdot m = a \cdot m + (-a) \cdot m$, despejando $(-a) \cdot m = -(a \cdot m)$.

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

3. Ejemplos:

1. Todo anillo A es un A-módulo: con la suma definida en A y con el producto por los elementos de A definido en A.
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 $T \colon E \to E$ 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 $T \colon E \to E$ definida por $T(e) = x \cdot e$, es un endomorfismo de k-espacios vectoriales.

5. Sea $\{M_i\}_{i\in I}$ una familia de A-módulos con índices en un conjunto I. Su producto directo se denotará $\prod_{i\in I} M_i$, mientras que $\oplus_{i\in I} M_i$ denotará el subconjunto de $\prod_{i\in I} M_i$ formado por los elementos (m_i) que tienen todas sus componentes nulas salvo un número finito de ellas, y se llamará suma directa de los $\{M_i\}_{i\in I}$. Tanto $\prod_{i\in I} M_i$ como $\oplus_{i\in I} M_i$ son A-módulos con la siguiente suma y producto por elementos de A:

$$(m_i)_{i\in I} + (m'_i)_{i\in I} := (m_i + m'_i)_{i\in I}$$
$$a\cdot(m_i)_{i\in I} := (a\cdot m_i)_{i\in I}$$

4. Definición: Un subconjunto N de un A-módulo M, decimos que es un A-submódulo si con la operación + de M y con la multiplicación $\cdot$ por elementos de A, N es un A-módulo.

Puede comprobarse que un subconjunto no vacío $X \subseteq M$ es un A-submódulo si y solo si para todo $x, x' \in X$ y $a \in A$ se cumple que $ax + x' \in X$.

La intersección de submódulos es submódulo.

5. Ejemplos: 1. Los K-subespacios vectoriales de un K-espacio vectorial E son justamente los K-submódulos de E.

2. Los ideales de un anillo A son justamente los A-submódulos de A.

3. Los subgrupos de un grupo abeliano G son justamente los $\mathbb{Z}$-submódulos de G.

4. Dado un endomorfismo k-lineal $T\colon E \to E$, los subespacios vectoriales $E' \subseteq E$ estables por T ($T(E') \subseteq E'$) son justamente los $k[x]$-submódulos de E.

5. $\oplus_{i\in I} M_i$ es un submódulo de $\prod_{i\in I} M_i$.

6. Dado un conjunto $\{M_i\}_{i\in I}$ de submódulos de M denotaremos

$$\sum_{i\in I} M_i = \{m \in M\colon m = \sum_{i\in I} m_i \text{ con } m_i \in M_i \text{ nulos para todo } i \in I \text{ salvo un número finito}\},$$

que es el menor submódulo de M que contiene a los submódulos M_i.

6. Definición: Dado un subconjunto $X \subseteq M$, llamaremos submódulo generado por X y lo denotaremos $\langle X\rangle$, al mínimo submódulo de M que contiene a X.

Se cumple que

$$\langle X\rangle = \{\sum_{i=1}^{n} a_i m_i \in M, \forall\ a_i \in A, m_i \in X, n \in \mathbb{N}\}.$$

Por ejemplo, $\langle m\rangle = \{am \in M\colon \forall\, a \in A\} =: A\cdot m$.

7. Definición: Diremos que un conjunto de elementos de M, $\{m_i\}_{i\in I}$, es un sistema generador de M si $\langle m_i\rangle_{i\in I} = M$, es decir, para cada $m \in M$ existen $i_1,\dots,i_n \in I$ y $a_{i_1},\dots,a_{i_n} \in A$ de modo que $m = a_{i_1}m_{i_1} + \cdots + a_{i_n}m_{i_n}$.

Evidentemente, todo módulo tiene sistemas generadores, por ejemplo el formado por todos los elementos de M.

8. Definición: Diremos que un módulo M es finito generado si existe un sistema generador de M formado por un número finito de elementos. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M, si es un sistema generador y los elementos son linealmente independientes, es decir, cumplen que siempre que $\sum_i a_i m_i = 0$, entonces $a_i = 0$, para todo i.

9. Ejemplo: Por ejemplo, $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ es un $\mathbb{Z}$-módulo finito generado, ya que $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} = \langle(1,0),(0,\bar{1})\rangle$.

10. Definición: Se dice que un módulo es libre si existe una base en el módulo.

En general los módulos no son libres, no tienen bases. Ésta es la gran diferencia de la teoría de módulos con la teoría de espacios vectoriales.

11. Ejemplo: $\mathbb{Z}/2\mathbb{Z}$ no es un $\mathbb{Z}$-módulo libre, porque si $\{\bar{n}_i\}_{i\in I}$ fuese una base, entonces $0 \neq 2\cdot\bar{n}_i = \overline{2\cdot n_i} = 0$, contradicción.

12. Ejercicio: Da una base del A-módulo libre $A[x]$.

0.3.1. Morfismos de módulos. Cocientes

13. Definición: Una aplicación $f: M \to M'$ entre A-módulos M, M', diremos que es un morfismo de A-módulos (o una aplicación A-lineal) 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.

14. Ejemplos: 1. Sea M un A-módulo y $a \in A$. La aplicación $a\cdot M \to M$, $m \mapsto a\cdot m$ es un morfismo de A-módulos.

2. Sean G y G' dos grupos abelianos, es decir, dos $\mathbb{Z}$-módulos. Una aplicación $f: G \to G'$ es un morfismo de grupos si y solo si es un morfismo de $\mathbb{Z}$-módulos, y f es un isomorfismo de grupos si y solo si f es un isomorfismo de $\mathbb{Z}$-módulos.

3. **Submódulos en suma directa:** 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 si $m_1 + m_2 = m_1' + m_2'$ (con $m_1, m_1' \in M_1$ y $m_2, m_2' \in M_2$) entonces $m_1 = m_1'$ y $m_2 = m_2'$, 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.

En general, diremos que un conjunto $\{M_i\}_{i\in I}$ de submódulos de M están en suma directa si $M_i \cap \sum_{j\neq i} M_j = 0$ para todo i, que equivale a decir que si $\sum_{i\in I} m_i = \sum_{i\in I} m_i'$ (con $m_i, m_i' \in M_i$ para todo i, y todos son nulos salvo un número finito) entonces $m_i = m_i'$ para todo $i \in I$, que equivale a decir que el morfismo natural

$$\bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i$$

es un isomorfismo. Se dice que M es la suma directa de los submódulos $\{M_i\}_{i\in I}$ si el morfismo $\bigoplus_{i\in I} M_i \to M$, $(m_i)_{i\in I} \mapsto \sum_{i\in I} m_i$ es un isomorfismo, que equivale a decir que todo $m \in M$ se escribe de modo único como $m = \sum_{i\in I} m_i$.

15. Definición: Sea $f : M \to M'$ un morfismo de A-módulos. El conjunto

$$\operatorname{Ker} f := \{m \in M : f(m) = 0\},$$

se denomina núcleo de f.

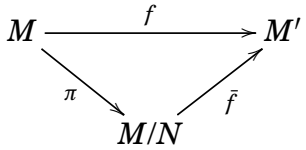
Se cumple que $\operatorname{Ker} f$ es un submódulo de M y que $f(m_1) = f(m_2)$ si y solo si $m_2 \in m_1 + \operatorname{Ker} f$, luego f es inyectiva si y solo si $\operatorname{Ker} f = 0$. El conjunto de los elementos de la imagen, $\operatorname{Im} f$, forman un submódulo de M'.

Si N es un submódulo de M entonces es un subgrupo conmutativo de M. Por tanto, podemos considerar el grupo cociente M/N, donde

$$M/N = \{\bar{m} \text{ (donde } \bar{m} =: m + N) \,, \forall\, m \in M\}$$

Recordemos que $\bar{m} = \bar{m'} \iff m - m' \in N$ y $\overline{m_1} + \overline{m_2} := \overline{m_1 + m_2}$. 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.

16. Teorema: *Sea $f : M \to M'$ un morfismo de A-módulos. Sea $N \subseteq \operatorname{Ker} f$ 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.

17. Teorema de isomorfía: *Sea $f : M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ M/\mathrm{Ker}\, f & \xrightarrow[\bar{f}]{} & \mathrm{Im}\, f \end{array}$$

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. □

18. Ejemplo: Sean $N \subseteq M$ y $N' \subseteq M'$ dos A-submódulos. Consideramos la inclusión obvia $N \oplus N' \subseteq M \oplus M'$, $(n, n') \mapsto (n, n')$. Probemos que

$$(M \oplus M')/(N \oplus N') \simeq M/N \oplus M'/N'.$$

El morfismo $M \oplus M' \to M/N \oplus M'/N'$, $(m, m') \mapsto (\bar{m}, \bar{m}')$ es epiyectivo y el núcleo es $N \oplus N'$. Por el teorema de isomorfía se concluye.

0.4. Localización por un sistema multiplicativo

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

2. Ejemplos: $\mathbb{Z}\backslash\{0\}$ es un sistema multiplicativo de $\mathbb{Z}$. Si A es un anillo íntegro, entonces $A\backslash\{0\}$ es un sistema multiplicativo.

Si $\mathfrak{p}_x \subset A$ es un ideal primo, entonces $A\backslash\mathfrak{p}_x$ es un sistema multiplicativo. Denotaremos $A_x = A_{A\backslash\mathfrak{p}_x}$.

Dado $a \in A$, $S = \{1, a, a^2, \ldots, a^n, \ldots\}$ es un sistema multiplicativo. Denotaremos $A_a = A_{\{}1, a, a^2, \ldots, a^n, \ldots\}$.

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

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

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

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

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

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

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

Con mayor generalidad, dar una aplicación $A_S \times \overset{n}{\cdots} \times A_S \to B$ es asignar a cada elemento $(\frac{a_1}{s_1}, \ldots, \frac{a_n}{s_n}) \in A_S \times \overset{n}{\cdots} \times A_S$ un elemento $\varphi(a_1, s_1, \ldots, a_n, s_n) \in B$ de modo que cumple que $\varphi(t_1a_1, t_1s_1, \ldots, t_na_n, t_ns_n) = \varphi(a_1, s_1, \ldots, a_n, s_n)$ para todo $t_1, \ldots, t_n \in S$.

Con la suma y producto ordinarios de fracciones (bien definidos)

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

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.

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

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

5. 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.

6. Ejemplos:

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

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

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

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

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

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

□

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

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

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

Observemos que si $J \subset A_S$ es un ideal de A_S, entonces $I := \{a \in A : \frac{a}{1} \in J\}$ es un ideal de A y $J = I \cdot A_S$. Ahora es fácil probar la siguiente proposición.

11. Proposición: *Si A es un anillo noetheriano, entonces A_S es un anillo noetheriano.*

12. Proposición: *Sea A una k-álgebra de tipo finito y $a \in A$. Entonces, A_a es una k-álgebra de tipo finito.*

Demostración. Escribamos $A = k[\xi_1, \ldots, \xi_n]$, entonces $A_a = A[\frac{1}{a}] = k[\xi_1, \ldots, \xi_n, \frac{1}{a}]$. □

13. Ejercicio: Sea A un anillo y $a \in A$. Prueba que A_a es isomorfo a $A[x]/(ax - 1)$.

Solución: La aplicación $A[x] \to A_a$, $p(x) \mapsto p(\frac{1}{a})$ es un morfismo de k-álgebras epiyectivo. Evidentemente, $ax - 1$ está en el núcleo del morfismo, luego tenemos el epimorfismo $A[x]/(ax - 1) \to A_a$, $\overline{p(x)} \mapsto p(\frac{1}{a})$. El morfismo $A_a \to A[x]/(ax - 1)$, $\frac{b}{a^n} \mapsto \overline{bx^n}$ está bien definido y es el morfismo inverso.

0.4.1. Localización de módulos

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

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

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

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

$$M_S = \{\frac{m}{s},\ \forall\ m \in M, s \in S\}$$

y diremos que M_S es la localización de M por el sistema multiplicativo S.

Recordemos que que $\frac{m}{s} = \frac{m'}{s'}$ si y solo si existen $s_1, s_2 \in S$ tales que $(s_1 m, s_1 s) = (s_2 m', s_2 s')$. Para definir una aplicación $M_S \to X$, tenemos que asignar a cada $\frac{m}{s} \in M_S$ un elemento $\phi(m,s)$, de modo que $\phi(tm,ts) = \phi(m,s)$, para todo $t \in S$. Igualmente, para definir una aplicación $M_S \times N_S \to X$, tenemos que asignar a cada $(\frac{m}{s}, \frac{n}{s'}) \in M_S \times N_S$ un elemento $\phi(m,s,n,s')$, de modo que $\phi(tm,ts,t'n,t's') = \phi(m,s,n,s')$, para todo $t, t' \in S$.

Con las operaciones (bien definidas)

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$$
$$\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$$

M_S tiene estructura de A_S-módulo. La aplicación canónica

$$M \to M_S,\ m \mapsto \frac{m}{1}$$

es un morfismo de A-módulos y diremos que es el morfismo de localización.

15. Ejercicio: Prueba que $\frac{m}{s} = 0$ si y solo sí existe un $t \in S$ de modo que $t \cdot m = 0$.

Todo morfismo $f : M \to N$ de A-módulos, induce la aplicación (bien definida)

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

que es morfismo de A_S-módulos.

16. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sean M y M' dos A-módulos. Entonces,*

$$(M \oplus M')_S = M_S \oplus M'_S$$

Demostración. Los morfismos de A_S-módulos $(M \oplus M')_S \to M_S \oplus M'_S$, $\frac{(m,m')}{s} \mapsto (\frac{m}{s}, \frac{m'}{s})$ y $M_S \oplus M'_S \to (M \oplus M')_S$, $(\frac{m}{s}, \frac{m'}{s'}) \mapsto \frac{(s'm, sm')}{ss'}$ son inversos entre sí. □

17. Ejemplo: Sea A un anillo íntegro y $\Sigma = A_{A\setminus\{0\}}$. Entonces,

$$(A^n)_{A\setminus\{0\}} = A_{A\setminus\{0\}} \oplus \overset{n}{\cdots} \oplus A_{A\setminus\{0\}} = \Sigma^n.$$

18. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sea M un A-módulo y $N \subseteq M$ un submódulo. Entonces, N_S es un submódulo de M_S (es decir, el morfismo $N_S \to M_S$ es inyectivo) y tenemos un isomorfismo natural*

$$M_S/N_S \simeq (M/N)_S.$$

Demostración. El morfismo $N_S \to M_S$ es inyectivo: Dado $\frac{n}{s} \in N_S$, si $\frac{n}{s} = 0$ en M_S, existe un elemento $s' \in S$ de modo que $s' \cdot n = 0$ en M (luego en N), por tanto $\frac{n}{s} = 0$ en N_S.

Consideremos el epimorfismo de paso al cociente $M \to M/N$. Localizando por S tenemos el morfismo $M_S \to (M/N)_S$, $m/s \mapsto \bar{m}/s$ que es claramente epiyectivo. Calculemos el núcleo: si $\bar{m}/s = 0$ entonces existe un elemento $s' \in S$ tal que $s' \cdot \bar{m} = 0$, es decir, $s' \cdot m \in N$, es decir, existe $n \in N$ de modo que $s' \cdot m = n$, luego $m/s = n/ss' \in N_S$. Recíprocamente, dado $n/s \in N_S$, entonces $\bar{n}/s = 0/s = 0$. □

19. Ejercicio: Sea $I \subseteq A$ un ideal y $S \subset A$ un sistema multiplicativo. Prueba que $I_S = I \cdot A_S$.

20. Proposición: *Dado un ideal primo $\mathfrak{p}_x \subset A$ y un A-módulo M, denotemos por M_x la localización de M por el sistema multiplicativo $A \setminus \mathfrak{p}_x$. Entonces,*

1. *$M = 0$ si y solo si $M_x = 0$ para todo ideal maximal $\mathfrak{p}_x \subset A$.*

2. *Un morfismo de módulos $f : M \to N$ es un isomorfismo si y solo si el morfismo inducido $f_x : M_x \to N_x$, $f_x(\frac{m}{s}) = \frac{f(m)}{s}$ es isomorfismo para todo ideal maximal $\mathfrak{p}_x \subset A$.*

Demostración. 1. $\Leftarrow$) Sea $m \in M$ no nulo y sea $\mathrm{Anul}(m) := \{a \in A : a \cdot m = 0\}$. Sea $\mathfrak{p}_x$ un ideal maximal que contenga a $\mathrm{Anul}(m)$, luego $\mathrm{Anul}(m) \cap (A \setminus \mathfrak{p}_x) = \emptyset$. Por hipótesis $\frac{m}{1} \in M_x = 0$, luego existe $s \in A \setminus \mathfrak{p}_x$ tal que $s \cdot m = 0$, es decir, $\mathrm{Anul}(m) \cap (A \setminus \mathfrak{p}_x)$ y hemos llegado a contradicción. En conclusión, $M = 0$.

2. $\Leftarrow$) Sea $m \in M$ no nulo. Supongamos que $f(m) = 0$. Sea $\mathfrak{p}_x$ un ideal maximal que contenga a $\mathrm{Anul}(m) := \{a \in A : a \cdot m\}$. Como $f_x(\frac{m}{1}) = \frac{f(m)}{1} = 0$, entonces $\frac{m}{1} = 0$ y existe $s \in A \setminus \mathfrak{p}_x$ tal que $0 = s \cdot m$, luego $s \in \mathrm{Anul}(m) \cap (A \setminus \mathfrak{p}_x) = \emptyset$, lo cual es contradictorio. Luego, f es inyectivo y podemos pensarlo como el morfismo de inclusión. Tenemos que $(N/M)_x = N_x/M_x = 0$, para todo ideal maximal $\mathfrak{p}_x$, luego $N/M = 0$ y $M = N$.

□

0.5. Producto tensorial de módulos

1. Sean M y N dos A-módulos. Sea $M\square N$ el A-módulo libre de base $\{m\square n\}_{(m,n)\in M\times N}$ (con otras palabras: $M\square N := \overset{M\times N}{\oplus} A$).

Sea R el submódulo de $M\square N$ generado por los elementos de la forma

$$\begin{aligned}
&(m+m')\square n - m\square n - m'\square n\\
&m\square(n+n') - m\square n - m\square n'\\
&(am)\square n - a(m\square n)\\
&m\square(an) - a(m\square n)
\end{aligned}$$

para todo $m,m'\in M$, $n\in N$ y $a\in A$.

2. Definición: Llamaremos producto tensorial de M y N sobre el anillo A, al A-módulo cociente $(M\square N)/R$ y lo denotaremos $M\otimes_A N$. Cada clase $\overline{m\square n}\in(M\square N)/R = M\otimes_A N$ la denotaremos $m\otimes n$.

De acuerdo con la definición de R tenemos que

$$\boxed{\begin{aligned}
&(m+m')\otimes n = m\otimes n + m'\otimes n\\
&m\otimes(n+n') = m\otimes n + m\otimes n'\\
&am\otimes n = a(m\otimes n)\\
&m\otimes an = a(m\otimes n)
\end{aligned}}$$

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 $M\square N$, 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,

$$\boxed{\text{Si } M=\langle m_i\rangle_{i\in I} \text{ y } N=\langle n_j\rangle_{j\in J}, \text{ entonces } M\otimes_A N=\langle m_i\otimes n_j\rangle_{(i,j)\in I\times J}.}$$

3. Definición: Sea P un A-módulo. Diremos que una aplicación $\beta\colon M\times N\to P$ es A-bilineal si

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

El conjunto de las aplicaciones A-bilineales de $M\times N$ en P se denota $\mathrm{Bil}_A(M\times N;P)$. La aplicación natural $\pi\colon M\times N\to M\otimes N$, $(m,n)\mapsto m\otimes n$ es bilineal.

4. Propiedad universal del producto tensorial: *Una aplicación $\beta\colon M\times N\to P$ es bilineal si y solo si existe un único morfismo de A-módulos $\phi\colon M\otimes_A N\to P$, de modo que el siguiente diagrama*

$$\begin{array}{ccc} M\times N & \xrightarrow{\beta} & P \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \phi} & \\ M\otimes_A N & & \end{array}$$

es conmutativo. Con concisión,

$$\mathrm{Hom}_A(M\otimes_A N,P)=\mathrm{Bil}_A(M\times N;P),\quad \phi\mapsto\phi\circ\pi$$

Demostración. El conjunto de la aplicaciones de $M\times N$ en P, $\mathrm{Aplic}(M\times N,P)$, se identifica con $\mathrm{Hom}_A(M\square N,P)$: Dada una aplicación $\beta\colon M\times N\to P$, tenemos el morfismo de A-módulos $\tilde\beta\colon M\square N\to P$, determinado por $\tilde\beta(m\square n):=\beta(m,n)$. Dada un morfismo de A-módulos $\tilde\beta\colon M\square N\to P$, tenemos la aplicación $\beta\colon M\times N\to P$, $\beta(m,n):=\tilde\beta(m\square n)$. Luego,

$$\begin{aligned}\mathrm{Bil}_A(M,N;P)&=\left\{\beta\in\mathrm{Aplic}(M\times N,P)\colon \begin{array}{c}\beta(m+m',n)=\beta(m,n)+\beta(m',n),\ \beta(am,n)=a\beta(m,n)\\ \beta(m,n+n')=\beta(m,n)+\beta(m,n'),\ \beta(m,an)=a\beta(m,n)\\ \forall\, m,m'\in M,\ \forall\, n,n'\in N,\forall\, a\in A\end{array}\right\}\\ &=\left\{\tilde\beta\in\mathrm{Hom}_A(M\square N,P)\colon \begin{array}{c}\tilde\beta(m+m'\square n)=\tilde\beta(m\square n)+\tilde\beta(m'\square n),\ \tilde\beta(am\square n)=a\beta(m\square n)\\ \tilde\beta(m\square n+n')=\tilde\beta(m\square n)+\tilde\beta(m\square n'),\ \tilde\beta(m\square an)=a\tilde\beta(m\square n)\\ \forall\, m,m'\in M,\ \forall\, n,n'\in N,\forall\, a\in A\end{array}\right\}\\ &=\mathrm{Hom}_A(M\otimes N,P).\end{aligned}$$

□

Este teorema nos dice que definir un morfismo de A-módulos $\phi\colon M\otimes_A N\to P$, es asignar a cada $m\otimes n\in M\otimes_A N$ un elemento $\phi(m\otimes n)\in P$ de modo que $\phi((am+m')\otimes n)=a\phi(m\otimes n)+\phi(m'\otimes n)$ y $\phi(m\otimes(an+n'))=a\phi(m\otimes n)+\phi(m\otimes n')$.

Dados dos morfismos de A-módulos $f\colon M\to M'$, $g\colon N\to N'$, inducen el morfismo en el producto tensorial $f\otimes g\colon M\otimes_A N\to M'\otimes_A N'$, $(f\otimes g)(m\otimes n):=f(m)\otimes g(n)$.

5. Teorema: *Existen isomorfismos naturales*

1. $M \otimes_A N = N \otimes_A M$, $m \otimes n \mapsto n \otimes m$.
2. $A \otimes_A M = M$, $a \otimes m \mapsto am$.
3. $A/I \otimes_A M = M/IM$, $\bar{a} \otimes m \mapsto \overline{am}$.
4. *Sea $M' \subset M$ un submódulo y denotemos la imagen del morfismo $M' \otimes N \to M \otimes N$, $m' \otimes n \mapsto m' \otimes n$ por $\overline{M' \otimes_A N}$, entonces $(M/M') \otimes_A N = (M \otimes N)/\overline{M' \otimes N}$, $\bar{m} \otimes n \mapsto \overline{m \otimes n}$.*
5. $(\underset{i}{\oplus} M_i) \otimes_A N = \underset{i}{\oplus}(M_i \otimes N)$, $(m_i) \otimes n \mapsto (m_i \otimes n)$.
6. $\mathrm{Hom}_A(M \otimes_A N, P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$, $\phi \mapsto \varphi$, *donde* $\varphi(m)(n) := \phi(m \otimes n)$.

Demostración. Dejamos al lector que defina los morfismos inversos. □

6. Observación: Igual que hemos definido-construido el producto tensorial de dos A-módulos, podemos construir el producto tensorial de 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 una propiedad universal similar. 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

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

Es decir,

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

donde $\mathrm{Multl}(M_1 \times \cdots \times M_n; P)$ denota el conjunto de las aplicaciones A-multilineales de $M_1 \times \cdots \times M_n$ en P.

7. Teorema: *Sean $M_1, \ldots, M_n$ A-módulos. El morfismo natural*

$$\begin{array}{rcl} M_1 \otimes_A \cdots \otimes_A M_n & \to & (M_1 \otimes_A \cdots \otimes_A M_r) \otimes_A (M_{r+1} \otimes_A \cdots \otimes_A M_n) \\ m_1 \otimes \cdots \otimes m_n & \mapsto & (m_1 \otimes \cdots \otimes m_r) \otimes (m_{r+1} \otimes \cdots \otimes m_n) \end{array}$$

es un isomorfismo.

Demostración. El morfismo

$$\phi : M_1 \otimes_A \cdots \otimes_A M_r \to \mathrm{Hom}_A(M_{r+1} \otimes_A \cdots \otimes_A M_n, M_1 \otimes_A \cdots \otimes_A M_n)$$

definido por $\phi(m_1 \otimes \cdots \otimes m_r)(m_{r+1} \otimes \cdots \otimes m_n) := m_1 \otimes \cdots \otimes m_n$, se corresponde, por el teorema 0.5.5.6, con el morfismo

$$\begin{array}{rcl} (M_1 \otimes_A \cdots \otimes_A M_r) \otimes_A (M_{r+1} \otimes_A \cdots \otimes_A M_n) & \to & M_1 \otimes_A \cdots \otimes_A M_n \\ (m_1 \otimes \cdots \otimes m_r) \otimes (m_{r+1} \otimes \cdots \otimes m_n) & \mapsto & m_1 \otimes \cdots \otimes m_n, \end{array}$$

que es el inverso del dado.

□

Como corolario obtenemos la propiedad asociativa del producto tensorial

$$(M \otimes_A N) \otimes_A P = M \otimes_A N \otimes_A P = M \otimes_A (N \otimes_A P).$$

8. Proposición: *Sean $\{L_i\}_{1\leq i\leq n}$ A-módulos libres de bases $\{e_{ij}\}_{j\in I_i}$. Entonces, el A-módulo $L_1 \otimes \cdots \otimes L_n$ es libre de base*

$$\{e_{1j_1} \otimes \cdots \otimes e_{nj_n}\}_{\{(j_1,\ldots,j_n)\in I_1\times\cdots\times I_n\}}.$$

Demostración. Las bases determinan isomorfismos $L_i \simeq \overset{I_i}{\oplus} A$. Por el teorema 0.5.5,

$$L_1 \otimes \cdots \otimes L_n \simeq (\overset{I_1}{\oplus} A) \otimes_A \cdots \otimes_A (\overset{I_n}{\oplus} A) = \overset{I_1\times\cdots\times I_n}{\oplus} A$$

que aplica la base del enunciado en la base usual de $\overset{I_1\times\cdots\times I_n}{\oplus} A$.

□

0.5.1. Cambio de anillo base

9. Definición: Si $f : A \to B$ es un morfismo de anillos, se dice que B es una A-álgebra. Usualmente denotaremos $f(a) = a$.

10. Ejemplos: $\mathbb{C}$ es una $\mathbb{R}$-álgebra del modo obvio.

Todo anillo A es de modo único una $\mathbb{Z}$-álgebra.

Dado un anillo A, $A[x_1,\ldots,x_n]$ es una A-álgebra: $A \to A[x_1,\ldots,x_n]$, $a \mapsto a$.

Sea B una A-álgebra. Dado un A-módulo M "por cambio de anillo base" obtenemos el A-módulo $M \otimes_A B$, que es un B-módulo pues para cada $b \in B$, tenemos el morfismo $b \cdot M \otimes_A B \to M \otimes_A B, b \cdot (m \otimes b') := m \otimes bb'$. Cada morfismo de A-módulos $f : M \to N$ induce "por cambio de anillo base" el morfismo de B-módulos $f \otimes \mathrm{Id} : M \otimes_A B \to N \otimes_A B$, $(f \otimes \mathrm{Id})(m \otimes b) := f(m) \otimes b$.

11. Ejemplo: Si $\{m_i\}_{i\in I}$ es un sistema de generadores de un A-módulo M, entonces $\{m_i \otimes 1\}_{i\in I}$ es un sistema de generadores del B-módulo $M \otimes_A B$: Dado $m \otimes b \in M \otimes_A B$, tenemos que $m = \sum_i a_i m_i$, luego $m \otimes b = \sum_i m_i \otimes a_i b = \sum_i a_i b \cdot (m \otimes 1) \in \langle m_i \otimes 1\rangle_{i\in I}$. Luego, $\{m_i \otimes 1\}_{i\in I}$ es un sistema generador del B-módulo $M \otimes_A B$.

Además, si $\{e_i\}_{i\in I}$ es una base de un A-módulo libre L, entonces $\{e_i \otimes 1\}_{i\in I}$ es una base del B-módulo libre $L \otimes_A B$: Si $L = \oplus^I A$, entonces $L \otimes_A B = (\oplus^I A) \otimes_A B = \oplus^I A \otimes_A B =$

$\oplus^I B$, es un B-módulo libre. Vía estos isomorfismos se tiene que $e_i \otimes 1 \mapsto (0,\dots,\overset{i}{1},\dots,0) \in \oplus^I B$.

Sea $f: L \to L'$ un morfismo de A-módulos entre A-módulos libres Si (a_{ij}) es la matriz del morfismo f en sendas bases $\{e_1,\dots,e_n\}$ y $\{e'_1,\dots,e'_m\}$ de L y L', la matriz de $f \otimes \mathrm{Id}: E \otimes_k K \to E' \otimes_k K$ en las bases $\{e_1 \otimes 1,\dots,e_n \otimes 1\}$ y $\{e'_1 \otimes 1,\dots,e'_m \otimes 1\}$ es (a_{ij}), ya que $(f \otimes \mathrm{Id})(e_i \otimes 1) = f(e_i) \otimes 1 = \sum_j a_{ji} e'_j \otimes 1 = \sum_j a_{ji}(e'_j \otimes 1)$.

12. Proposición: *Sea B una A-álgebra, M un A-módulo y N, N', B-módulos. Entonces, $(M \otimes_A N) \otimes_B N' = M \otimes_A (N \otimes_B N')$.*

Demostración. El morfismo $M \otimes_A N \to \mathrm{Hom}_B(N', M \otimes_A (N \otimes_B N'))$, $m \otimes n \mapsto (m \otimes n)$, donde $(m \otimes n)(n') := m \otimes (n \otimes n')$, por el teorema 0.5.5.6 define el morfismo de B-módulos $(M \otimes_A N) \otimes_B N' \to M \otimes_A (N \otimes_B N')$, $(m \otimes n) \otimes n' \mapsto m \otimes (n \otimes n')$. Igualmente, tenemos el morfismo $M \otimes_A (N \otimes_B N') \to (M \otimes_A N) \otimes_B N'$, $m \otimes (n \otimes n') \mapsto (m \otimes n) \otimes n'$. Ambos morfismos son inversos entre sí.

□

13. Notación: Denotaremos $M \otimes_A B = M_B$.

14. Proposición: *Sean $A \to B$ y $B \to C$ morfismos de anillos, M y M' A-módulos. Existen isomorfismos naturales*

1. $(M \otimes_A M') \otimes_A B = M_B \otimes_B M'_B$, $(m \otimes m') \otimes b \mapsto (m \otimes b) \otimes (m' \otimes 1)$.

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. 1. $M_B \otimes_B M'_B = (M \otimes_A B) \otimes_B M'_B = M \otimes_A (B \otimes_B M'_B) = M \otimes_A M'_B = (M \otimes_A M') \otimes_A B$.

2. $(M \otimes_A B) \otimes_B C = M \otimes_A (B \otimes_B C) = M \otimes_A C$. □

15. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo y M un A-módulo. El morfismo $M \otimes_A A_S \to M_S$, $m \otimes \frac{a}{s} \mapsto \frac{am}{s}$ es un isomorfismo de A_S-módulos.*

Demostración. El morfismo inverso es $\frac{m}{s} \mapsto m \otimes \frac{1}{s}$.

□

0.6. Producto tensorial de álgebras

1. Definición: Dadas dos A-álgebras B y C, diremos que un morfismo de anillos $\phi\colon B \to C$ es un morfismo de A-álgebras si $\phi(a) = a$, para todo $a \in A$. Denotaremos $\mathrm{Hom}_{A-alg}(B,C)$ al conjunto de todos los morfismos de A-álgebras de B en C.

2. Ejercicio: Prueba que $\mathrm{Hom}_{A-alg}(A[x_1,\ldots,x_n],B) = B^n$.

Si B y C son A-álgebras, el A-módulo $B \otimes_A C$ tiene una estructura de A-álgebra natural: 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.

3. Proposición: *Sean B, C y D A-álgebras. Se tiene la biyección*

$$\begin{array}{rcl} \mathrm{Hom}_{A-alg}(B \otimes_A C, D) & = & \mathrm{Hom}_{A-alg}(B,D) \times \mathrm{Hom}_{A-alg}(C,D) \\ \phi & \longmapsto & (\phi_1,\phi_2), \quad \phi_1(b) := \phi(b \otimes 1), \phi_2(c) := \phi(1 \otimes c) \\ \phi(b \otimes c) := \phi_1(b)\phi_2(c), & \longmapsto & (\phi_1,\phi_2) \end{array}$$

4. Proposición: *Sean B, C A-álgebras y D una C-álgebra. Se tiene la biyección*

$$\begin{array}{rcl} \mathrm{Hom}_{A-alg}(B,D) & = & \mathrm{Hom}_{C-alg}(B_C,D) \\ \phi & \longmapsto & \phi', \quad \phi'(b \otimes c) := \phi(b) \cdot c \\ \phi'_{|B}(b) := \phi'(b \otimes 1), \quad \phi'_{|B} & \longmapsto & \phi' \end{array}$$

0.7. Biografía de Dedekind

DEDEKIND BIOGRAPHY

Richard Dedekind's father was a professor at the Collegium Carolinum in Brunswick. His mother was the daughter of a professor who also worked at the Collegium Carolinum. Richard was the youngest of four children and never married. He was to live with one of his sisters, who also remained unmarried, for most of his adult life.

He attended school in Brunswick from the age of seven and at this stage mathematics was not his main interest. The school, Martino-Catharineum, was a good one and Dedekind studied

science, in particular physics and chemistry. However, physics became less than satisfactory to Dedekind with what he considered an imprecise logical structure and his attention turned towards mathematics.

The Collegium Carolinum was an educational institution between a high school and a university and he entered it in 1848 at the age of 16. There he was to receive a good understanding of basic mathematics studying differential and integral calculus, analytic geometry and the foundations of analysis. He entered the University of Göttingen in the spring of 1850 with a solid grounding in mathematics.

Göttingen was a rather disappointing place to study mathematics at this time, and it had not yet become the vigorous research centre that it turned into soon afterwards. Mathematics was directed by M.A. Stern and G. Ulrich. Gauss also taught courses in mathematics, but mostly at an elementary level. The physics department was directed by Listing and Wilhelm Weber. The two departments combined to initiate a seminar which Dedekind joined from its beginning. There he learnt number theory which was the most advanced material he studied. His other courses covered material such as the differential and integral calculus, of which he already had a good understanding. The first course to really make Dedekind enthusiastic was, rather surprisingly, a course on experimental physics taught by Weber. More likely it was Weber who inspired Dedekind rather than the topic of the course.

In the autumn term of 1850, Dedekind attended his first course given by Gauss. It was a course on least squares:

... fifty years later Dedekind remembered the lectures as the most beautiful he had ever heard, writing that he had followed Gauss with constantly increasing interest and that he could not forget the experience.

Dedekind did his doctoral work in four semesters under Gauss's supervision and submitted a thesis on the theory of Eulerian integrals. He received his doctorate from Göttingen in 1852 and he was to be the last pupil of Gauss. However he was not well trained in advanced mathematics and fully realised the deficiencies in his mathematical education.

At this time Berlin was the place where courses were given on the latest mathematical developments but Dedekind had not been able to learn such material at Göttingen. By this time Riemann was also at Göttingen and he too found that the mathematical education was aimed at students who were intending to become secondary school teachers, not those with the very top abilities who would go on to research careers. Dedekind therefore spent the two years following the award of his doctorate learning the latest mathematical developments and working for his habilitation.

In 1854 both Riemann and Dedekind were awarded their habilitation degrees within a few weeks of each other. Dedekind was then qualified as a university teacher and he began teaching at Göttingen giving courses on probability and geometry.

Gauss died in 1855 and Dirichlet was appointed to fill the vacant chair at Göttingen. This was an extremely important event for Dedekind who found working with Dirichlet extremely profitable. He attended courses by Dirichlet on the theory of numbers, on potential theory, on definite integrals, and on partial differential equations. Dedekind and Dirichlet soon became close friends and the relationship was in many ways the making of Dedekind, whose mathematical interests took a new lease of life with the discussions between the two. Bachmann, who was a student in Göttingen at this time wrote:

... recalled in later years that he only knew Dedekind by sight because Dedekind always arrived and left with Dirichlet and was completely eclipsed by him.

Dedekind wrote in a letter in July 1856:

What is most useful to me is the almost daily association with Dirichlet, with whom I am for the first time beginning to learn properly; he is always completely amiable towards me, and he tells me without beating about the bush what gaps I need to fill and at the same time he gives me the instructions and the means to do it. I thank him already for infinitely many things, and no doubt there will be many more.

Dedekind certainly still continued to learn mathematics at this time as a student would by attending courses, such as those by Riemann on abelian functions and elliptic functions. Around this time Dedekind studied the work of Galois and he was the first to lecture on Galois theory when he taught a course on the topic at Göttingen during this period.

While at Göttingen, Dedekind applied for J L Raabe's chair at the Polytechnikum in Zürich. Dirichlet supported his application writing that Dedekind was 'an exceptional pedagogue'. In the spring of 1858 the Swiss councillor who made appointments came to Göttingen and Dedekind was quickly chosen for the post. Dedekind was appointed to the Polytechnikum in Zürich and began teaching there in the autumn of 1858.

In fact it was while he was thinking how to teach differential and integral calculus, the first time that he had taught the topic, that the idea of a Dedekind cut came to him. He recounts that the idea came to him on 24 November 1858. His idea was that every real number r divides the rational numbers into two subsets, namely those greater than r and those less than r. Dedekind's brilliant idea was to represent the real numbers by such divisions of the rationals.

Dedekind and Riemann travelled together to Berlin in September 1859 on the occasion of Riemann's election to the Berlin Academy of Sciences. In Berlin, Dedekind met Weierstrass, Kummer, Borchardt and Kronecker.

The Collegium Carolinum in Brunswick had been upgraded to the Brunswick Polytechnikum by the 1860s, and Dedekind was appointed to the Polytechnikum in 1862. With this appointment he returned to his home town and even to his old educational

establishment where his father had been one of the senior administrators for many years. Dedekind remained there for the rest of his life, retiring on 1 April 1894. He lived his life as a professor in Brunswick:

... in close association with his brother and sister, ignoring all possibilities of change or attainment of a higher sphere of activity. The small, familiar world in which he lived completely satisfied his demands: in it his relatives completely replaced a wife and children of his own and there he found sufficient leisure and freedom for scientific work in basic mathematical research. He did not feel pressed to have a more marked effect in the outside world: such confirmation of himself was unnecessary.

After he retired, Dedekind continued to teach the occasional course and remained in good health in his long retirement. The only spell of bad health which Dedekind had experienced was 10 years after he was appointed to the Brunswick Polytechnikum when he had a serious illness, shortly after the death of his father. However he completely recovered and, as we mentioned, remained in good health.

Dedekind made a number of highly significant contributions to mathematics and his work would change the style of mathematics into what is familiar to us today. One remarkable piece of work was his redefinition of irrational numbers in terms of Dedekind cuts which, as we mentioned above, first came to him as early as 1858. He published this in Stetigkeit und Irrationale Zahlen in 1872. In it he wrote:

Now, in each case when there is a cut (A_1, A_2) *which is not produced by any rational number, then we create a new, irrational number* a*, which we regard as completely defined by this cut; we will say that this number* a *corresponds to this cut, or that it produces this cut.*

As well as his analysis of the nature of number, his work on mathematical induction, including the definition of finite and infinite sets, and his work in number theory, particularly in algebraic number fields, is of major importance.

Dedekind loved to take his holidays in Switzerland, the Austrian Tyrol or the Black Forest in southern Germany. On one such holiday in 1874 he met Cantor while staying in the beautiful city of Interlaken and the two discussed set theory. Dedekind was sympathetic to Cantor's set theory as is illustrated by this quote from Was sind und was sollen die Zahlen (1888) regarding determining whether a given element belongs to a given set:

In what way the determination comes about, or whether we know a way to decide it, is a matter of no consequence in what follows. The general laws that are to be developed do not depend on this at all.

In this quote Dedekind is arguing against Kronecker's objections to the infinite and, therefore, is agreeing with Cantor's views.

Among Dedekind's other notable contributions to mathematics were his editions of the collected works of Peter Dirichlet, Carl Gauss, and Georg Riemann. Dedekind's

study of Dirichlet's work did, in fact, lead to his own study of algebraic number fields, as well as to his introduction of ideals. Dedekind edited Dirichlet's lectures on number theory and published these as Vorlesungen über Zahlentheorie in 1863. It is noted that:

Although the book is assuredly based on Dirichlet's lectures, and although Dedekind himself referred to the book throughout his life as Dirichlet's, the book itself was entirely written by Dedekind, for the most part after Dirichlet's death.

It was in the third and fourth editions of Vorlesungen über Zahlentheorie, published in 1879 and 1894, that Dedekind wrote supplements in which he introduced the notion of an ideal which is fundamental to ring theory. Dedekind formulated his theory in the ring of integers of an algebraic number field. The general term 'ring' does not appear, it was introduced later by Hilbert.

Dedekind, in a joint paper with Heinrich Weber published in 1882, applies his theory of ideals to the theory of Riemann surfaces. This gave powerful results such as a purely algebraic proof of the Riemann-Roch theorem.

Dedekind's work was quickly accepted, partly because of the clarity with which he presented his ideas and partly since Heinrich Weber lectured to Hilbert on these topics at the University of Königsberg. Dedekind's notion of ideal was taken up and extended by Hilbert and then later by Emmy Noether. This led to the unique factorisation of integers into powers of primes to be generalised to ideals in other rings.

In 1879 Dedekind published Über die Theorie der ganzen algebraischen Zahlen which was again to have a large influence on the foundations of mathematics. In the book Dedekind:

... presented a logical theory of number and of complete induction, presented his principal conception of the essence of arithmetic, and dealt with the role of the complete system of real numbers in geometry in the problem of the continuity of space. Among other things, he provides a definition independent of the concept of number for the infiniteness or finiteness of a set by using the concept of mapping and treating the recursive definition, which is so important to the theory of ordinal numbers.

Dedekind's brilliance consisted not only of the theorems and concepts that he studied but, because of his ability to formulate and express his ideas so clearly, he introduced a new style of mathematics that been a major influence on mathematicians ever since. As Edwards writes:

Dedekind's legacy ... consisted not only of important theorems, examples, and concepts, but a whole style of mathematics that has been an inspiration to each succeeding generation.

Many honours were given to Dedekind for his outstanding work, although he always remained extraordinarily modest regarding his own abilities and achievements. He was elected to the Göttingen Academy (1862), the Berlin Academy (1880), the Aca-

demy of Rome, the Leopoldino-Carolina Naturae Curiosorum Academia, and the Académie des Sciences in Paris (1900). Honorary doctorates were awarded to him by the universities of Kristiania (Oslo), Zurich and Brunswick.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

0.8. Cuestionario

1. Consideremos el conjunto $A = \{0\}$ y consideremos las dos operaciones internas:

$$0 + 0 := 0 \text{ y } 0 \cdot 0 := 0$$

   ¿Es $(A, +, \cdot)$ un anillo?

2. Sean $(A, +, \cdot)$ y $(B, +, \cdot)$ dos anillos. Dota a $A \times B$ de estructura de anillo.

3. ¿La serie $1 + x \in \mathbb{Q}[[x]]$ tiene inverso?

4. Sean A y B dos anillos y consideremos en $A \times B$ la estructura de anillo usual ¿Es $A \times B$ un anillo íntegro?

5. ¿Son los cuerpos anillos íntegros?

6. Sea A un anillo íntegro. Sean $a, b, c \in A$ y $a \neq 0$. Si $ab = ac$, prueba que $b = c$.

7. Sea A un anillo y p un número primo. Si $1 + \overset{p}{\cdots} + 1 = 0$ en A, prueba que $(a+b)^p = a^p + b^p$, para todo $a, b \in A$.

8. Sea $I \subset A$ un ideal. Prueba que $A[x]/(I) \simeq (A/I)[x]$.

9. Sean I_1, I_2 dos ideales de A. Prueba que $I_1 + I_2 := \{i_1 + i_2 \in A : i_1 \in I_1, i_2 \in I_2\}$ es un ideal de A. Prueba que $\bar{I}_2 := \{\bar{i}_2 \in A/I_1 : i_2 \in I_2\}$ es un ideal de A/I_1. Prueba que

$$(A/I_1)/\bar{I}_2 = A/(I_1 + I_2).$$

10. Sea A un anillo íntegro. Prueba que $(A[x])^* = A^*$ (definimos B^* como el conjunto de los invertibles de B).

11. Calcula los ideales primos de $A = \{0\}$.

12. Sea K un cuerpo. Calcula los ideales de K.

13. Da un criterio para saber cuándo un número entero escrito en base dos es divisible por $3 \in \mathbb{Z}$.

14. ¿Es el ideal $(x,y) \subset \mathbb{Q}[x,y]$ principal?

15. ¿Es el ideal $(2,x) \subset \mathbb{Z}[x]$ principal?

16. Dados $p(x) = x^3+x^2+x+1, q(x) = 2x^2+3x+1 \in \mathbb{Q}[x]$, calcula $c(x), r(x)$ de modo que $p(x) = q(x)c(x)+r(x)$ y $r(x) = 0$ ó $\mathrm{gr}(r(x)) < \mathrm{gr}(q(x)$.

17. Sean $p(x) = x^3 - x^2 + x - 1$ y $q(x) = x^3 - 3x^2 + 3x - 1 \in \mathbb{Q}[x]$. Calcula mediante el algoritmo de Euclides el máximo común divisor de $p(x)$ y $q(x)$, calcula $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ de modo que $\lambda(x)p(x) + \mu(x)q(x) = m.c.d.(p(x), q(x))$.

18. Sea I un ideal de un anillo A y sea S un sistema multiplicativo de A. Prueba que I_S es un ideal del anillo de fracciones A_S.

19. ¿Si M y N son A-módulos finito generados, es $M \otimes_A N$ finito generado?

20. Sea $m \in M$ y $0 \in N$. ¿Es $m \otimes 0 = 0$?

21. ¿Es $(am) \otimes n = m \otimes (an)$?

22. Sea $2 \otimes \bar{1} \in \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. ¿Es $2 \otimes \bar{1} = 0$?

23. ¿Es $f : A[x] \otimes_A A[y] \to A[x,y]$, $f(\sum_{i=1}^{n} p_i(x) \otimes q_i(y) := \sum_{i=1}^{n} p_i(x) \cdot q_i(y)$ un morfismo de A-módulos bien definido? ¿Es f epiyectivo?

24. ¿Es $(M \otimes_A N) \otimes_A P$ isomorfo a $M \otimes_A N \otimes_A P$?

25. ¿Es $A^n \otimes_A A/I$ isomorfo a $(A/I)^n$?

26. ¿Es $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C}$ isomorfo a $\mathbb{C}[x]$?

27. Sea $A = \mathbb{Z}/3\mathbb{Z}$ y $M = A^3$ ¿Cuántos elementos tiene $M \otimes_A M$? ¿Es $M \otimes_A M = \{m \otimes m'\}_{m,m' \in M}$?

28. Calcula $(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z})$.

29. ¿Es $\mathbb{Q}[x]/(x^2+1) \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$?

30. ¿Es $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$? ¿Es $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$?

0.9. Problemas

1. Calcula todos los automorfismos de anillos de $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.

2. Sea A un anillo, $a \in A$ y $p(x) \in A[x]$. Prueba que $p(a) = 0$ si y solo si $p(x)$ es múltiplo de $x - a$. Prueba que $A[x]/(x-a) \simeq A$.

3. Prueba que $\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) \simeq \mathbb{C} \times \mathbb{R} \times \mathbb{R}$.

4. Prueba

   a) $s(x) = \sum_{i=0}^{n} a_i x^i \in k[[x]]$ es invertible si y solo si $a_0 \neq 0$.

   b) El morfismo $k[x]/(x^n) \to k[[x]]/(x^n)$, $\overline{p(x)} \mapsto \overline{p(x)}$ es un isomorfismo.

5. Sea $I \subseteq A$, $J \subseteq B$ dos ideales. Prueba que $I \times J \subseteq A \times B$ es un ideal. Prueba que $(A \times B)/I \times J \simeq A/I \times B/J$.

6. Propiedad universal de la localización: Sea S un sistema multiplicativo del anillo A, $i : A \to A_S$ el morfismo de localización . Dado un morfismo de anillos $f : A \to B$, prueba que existe un morfismo (único) $g : A_S \to B$ tal que $f = g \circ i$ si y solo si $f(s)$ es invertible para todo $s \in S$.

7. Sean S y S' dos sistemas multiplicativos de un anillo A y denotemos $S \cdot S' = \{ss', \forall\, s \in S, \forall\, s' \in S'\}$. Prueba que $A_{S \cdot S'}$ es un anillo isomorfo a $(A_S)_{S'}$.

8. Sea $I \subset A$ un ideal, $S \subset A$ un sistema multiplicativo y M un A-módulo. Prueba que $(M/IM)_S \simeq M_S/I \cdot M_S$.

9. Sea $S \subset A$ un sistema multiplicativo y M un A-módulo. Prueba que el morfismo de localización $M \to M_S$ es un isomorfismo si y solo si el morfismo de A-módulos $s\cdot : M \to M$, $m \mapsto s \cdot m$ es un isomorfismo, para todo $s \in S$.

10. Prueba que si $0 \to M_1 \to M_2 \to M_3 \to 0$ es una sucesión exacta[3] de A-módulos y N es un A-módulo libre, entonces

$$0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$$

    es una sucesión exacta de A-módulos.

[3] Una sucesión de morfismos de módulos $\cdots \to M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \to \cdots$ se dice que es una sucesión exacta si $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$, para todo i.

11. Prueba que si $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ es una sucesión exacta de A-módulos y N es un A-módulo, entonces

$$M_1 \otimes_A N \xrightarrow{f\otimes \mathrm{Id}} M_2 \otimes_A N \xrightarrow{g\otimes \mathrm{Id}} M_3 \otimes_A N \to 0$$

es una sucesión exacta de A-módulos.

12. Sea E' un subespacio vectorial de un k-espacio vectorial E. Para todo k-espacio vectorial V, prueba que $(E/E')\otimes_k V = (E\otimes_k V)/(E'\otimes_k V)$.

13. Sea $f: E' \to E$ una aplicación k-lineal, V un k-espacio vectorial y consideremos la aplicación lineal $f\otimes 1: E'\otimes_k V \to E\otimes_k V$. Prueba que $\mathrm{Im}(f\otimes \mathrm{Id}) = (\mathrm{Im}\, f)\otimes_k V$ y $\mathrm{Ker}(f\otimes \mathrm{Id}) = (\mathrm{Ker}\, f)\otimes_k V$.

14. Prueba que $A/I \otimes_A A/J = A/(I+J)$.

15. Sean I y J dos ideales de un anillo A. Si $I+J=A$, demostrar que para todo A-módulo M, tenemos un isomorfismo natural $M/IJM = (M/IM)\oplus(M/JM)$.

16. Prueba que $(\mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$, donde $d = \text{m.c.d.}(m,n)$.

17. Si E es un k-espacio vectorial y $k \hookrightarrow K$ es una extensión de cuerpos, entonces $\dim_K(E\otimes_k K) = \dim_k E$.

18. Sea $\{e_1,\dots,e_n\}$ una base de un k-espacio vectorial E y $k \hookrightarrow K$ es una extensión de cuerpos. Si $(x_1,\dots,x_n)$ son las coordenadas de un vector $e\in E$ en tal base, determina las coordenadas de $e\otimes 1 \in E\otimes_k K$ en la base $\{e_1\otimes 1,\dots,e_n\otimes 1\}$

19. Sea $A\to B$ un morfismo de anillos. Prueba que $A[x_1,\dots,x_n]\otimes_A B = B[x_1,\dots,x_n]$.

20. Sea $A\to B$ un morfismo de anillos. Prueba que

$$\big(A[x_1,\dots,x_n]/(p_1,\dots,p_r)\big)\otimes_A B = B[x_1,\dots,x_n]/(p_1,\dots,p_r)\,.$$

(los polinomios con coeficientes en A, vía el morfismo $A\to B$ los consideramos como polinomios con coeficientes en B).

21. Sea B una A-álgebra y M,N dos B-módulos. Sea R el A-submódulo de $M\otimes_A N$ generado por los elementos $bm\otimes n - m\otimes bn$, variando $m\in M$, $n\in N$ y $b\in B$. Prueba que $M\otimes_B N = (M\otimes_A N)/R$.

22. Si E y F son k-espacios vectoriales y $\dim_k E < \infty$, prueba que $\mathrm{Hom}_k(E,F) = E^*\otimes_k F$.

Capítulo 1

Álgebras de tipo finito

1.1. Introducción

Como hemos comentado, el objetivo principal de la Geometría Algebraica es el estudio del conjunto de soluciones de los sistemas de ecuaciones algebraicas

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

Un primer resultado afirma que si el sistema de ecuaciones estuviese formado por un número infinito de ecuaciones, entonces todas las ecuaciones salvo un número finito serían redundantes. Con otras palabras, para cada un ideal $I = (p_i(x_1,\ldots,x_n))_{j\in J} \subseteq k[x_1,\ldots,x_n]$ existen $j_1,\ldots,j_r \in J$ tales que $I = (p_{j_1}(x_1,\ldots,x_n),\ldots,p_{j_r}(x_1,\ldots,x_n))$. Los anillos cuyos ideales son finito generados se denominan noetherianos. Estamos afirmando que el anillo $k[x_1,\ldots,x_n]$ es noetheriano.

Como probaremos, $A_X = k[x_1,\ldots,x_n]/(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$, el anillo de funciones algebraicas del conjunto X de soluciones del sistema de ecuaciones anterior, es noetheriano. Los anillos $k[x_1,\ldots,x_n]/(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$ se denominan k-álgebras de tipo finito. Por tanto, las k-álgebras de tipo finito son anillos noetherianos.

En los próximos capítulos mostraremos que el estudio del álgebra A_X es equivalente al estudio de X y veremos cuál es el significado geométrico de la localización de A_X por un sistema multiplicativo, del grado de trascendencia del cuerpos de fracciones de A_X (cuando A_X sea íntegro), etc.

1.2. Lema de Gauss

Probaremos que $k[x,y]$ es un dominio de factorización única usando que $k[x,y] \subset k(x)[y]$ y que $k(x)[y]$ es dominio de factorización única.

1. 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.

2. Lema: *Sea A un dominio de factorización única de cuerpo de fracciones $\Sigma = A_{A\setminus 0}$. Entonces,*

1. *Si $p(x), q(x) \in A[x]$ son dos polinomios primitivos entonces $p(x)\cdot q(x)$ es primitivo.*
2. *Para cada $h(x) \in \Sigma[x]$ existen $v \in \Sigma$ y $p(x) \in A[x]$ primitivo, únicos salvo multiplicación por un invertible de A, tales que*

$$h(x) = v \cdot p(x).$$

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. Pasando al cociente $A[x] \to (A/pA)[x]$, 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 $u \in A$ el producto de todos los denominadores de los coeficientes de $h(x)$. Entonces, $u \cdot h(x) \in A[x]$. Sea u' el máximo común divisor de todos los coeficientes de $u \cdot h(x)$. Entonces, $p(x) := \frac{u}{u'} h(x) \in A[x]$ es primitivo. Si definimos $v := \frac{u'}{u}$, entonces $h(x) = v \cdot p(x)$.

Sea otra descomposición $h(x) = v' \cdot p(x)'$. Basta probar que $v = v'$ salvo multiplicación por un invertible. Sea $w \in A$ tal que $w \cdot v, w \cdot v' \in A$. Observemos que $w \cdot v \cdot p(x) = w \cdot v' \cdot p(x)'$. Ahora bien, el máximo común divisor de los coeficientes del polinomio $w \cdot v \cdot p(x)$ es $w \cdot v$ (salvo multiplicación por un invertible) y el de $w \cdot v' \cdot p(x)'$ es $w \cdot v'$. Luego, $v = v'$ salvo multiplicación por un invertible. □

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

Demostración. Supongamos que $p(x)$ es irreducible en $\Sigma[x]$. Si $p(x) = p_1(x) \cdot p_2(x)$, con $p_1(x), p_2(x) \in A[x]$, entonces como $p(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $p_1(x)$ o $p_2(x)$ ha de ser de grado cero, digamos $p_1(x) = a$. Como $p(x)$ es primitivo $p_1(x) = a \in A$ es invertible. En conclusión, $p(x)$, es irreducible en $A[x]$.

Supongamos que $p(x)$ es irreducible en $A[x]$. Supongamos que $p(x) = \tilde{p}_1(x) \cdot \tilde{p}_2(x)$, siendo $\tilde{p}_1(x)$ y $\tilde{p}_2(x)$ dos polinomios de $\Sigma[x]$. Sean $v_1, v_2 \in \Sigma$ y $p_1(x), p_2(x) \in A[x]$ primitivos, salvo multiplicación por invertibles de A, tales que $\tilde{p}_1(x) = v_1 \cdot p_1(x)$ y $\tilde{p}_2(x) = v_2 \cdot p_2(x)$. Entonces,

$$p(x) = (v_1 \cdot v_2) \cdot (p_1(x) \cdot p_2(x)).$$

Por el lema 1.2.2 1., $p_1(x) \cdot p_2(x)$ es primitivo. Por el lema 1.2.2 2., $v_1 \cdot v_2$ es un invertible de A. Luego $p(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

4. Corolario: *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

$$q(x) = \tilde{q}_1(x) \cdots \tilde{q}_r(x)$$

la descomposición en irreducibles en $\Sigma[x]$. Por el lema 1.2.2 se puede escribir $\tilde{q}_i(x) = v_i \cdot q_i(x)$ con $v_i \in \Sigma$ y $q_i(x) \in A[x]$ primitivos. Luego,

$$q(x) = v \cdot q_1(x) \cdots q_r(x).$$

• Por el lema 1.2.2 1., $q_1(x) \cdots q_r(x)$ es primitivo. Por el lema 1.2.2 2., v es un invertible de A.

• Cada $q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por 1.2.3.

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

$$p(x) = a \cdot q(x) = v \cdot p_1 \cdots p_s q_1(x) \cdots q_r(x)$$

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 1.2.3. $\Sigma[x]$ es DFU, por tanto, los polinomios $p_i(x)$ (una vez reordenados) son iguales a los $q_i(x)$, salvo multiplicación por un elemento de Σ, que ha de ser un invertible de A. Tachando los términos polinómicos comunes se obtiene salvo multiplicación por invertibles de A la igualdad $q_1 \cdots q_l = p_1 \cdots p_s$, de donde $q_i = p_i$ (salvo permutación de los factores y multiplicación de éstos por invertibles de A).

□

Como corolario del teorema anterior, se obtiene el siguiente teorema.

5. 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.*

1.3. Anillos y módulos noetherianos

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.

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

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

3. 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 $M' = \bigcup_{i=1}^{\infty} M_i \subseteq M$. Como M' es un submódulo de M, es finito generado. Escribamos $M' = \langle m_1,\ldots,m_r\rangle$, con $m_j \in M_{i_j}$. Si r es el máximo de todos los i_j, $M' = M_r$, luego $M_r = M_{r+1} = \cdots$.

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

□

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

5. Teorema : *Sea M un A-módulo y $N \subset M$ un submódulo. M es un A-módulo noetheriano si y solo si N y M/N son módulos noetherianos.*

Demostración. Sea $\pi\colon M \to M/N$, $\pi(m) := \bar{m}$ el morfismo de paso al cociente.

$\Rightarrow$) Evidentemente N es noetheriano. Dado un submódulo $\bar{M} \subset M/N$, tenemos que $\pi^{-1}(\bar{M}) = \langle m_1, \ldots, m_r \rangle$. Por tanto, $\bar{M} = \langle \pi(m_1), \ldots, \pi(m_r) \rangle$.

$\Leftarrow$) Sea $M' \subset M$ un submódulo. $M' \cap N$ es finito generado porque es un submódulo de N, y $M'/M' \cap N$ es finito generado porque podemos considerarlo como submódulo de M/N, vía el morfismo inyectivo $M'/M' \cap N \hookrightarrow M/N$, $\bar{m} \mapsto \bar{m}$. Escribamos $M' \cap N = \langle m_1, \ldots, m_r \rangle$ y $M'/M' \cap N = \langle \bar{m}_{r+1}, \ldots, \bar{m}_n \rangle$, entonces $M' = \langle m_1, \ldots, m_n \rangle$. En conclusión, M es un módulo noetheriano.

□

6. Ejercicio: Prueba que M y M' son módulos noetherianos si y solo si $M \oplus M'$ es noetheriano.

7. Definición: Se dice que un anillo A 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.

8. 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.

9. Ejercicio: Da un ejemplo de módulo finito generado que no sea noetheriano.

10. Proposición: *Si A es un anillo noetheriano, todo A-módulo finito generado es noetheriano.*

Demostración. Si A es noetheriano, A^n es un A-módulo noetheriano, por el ejercicio 1.3.6. 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.

11. Proposición: *Sea A un anillo noetheriano. Todo A-módulo finito generado tiene una presentación por A-módulos libres finito generados.*

Demostración. Sea $M = \langle m_1, \ldots, m_r \rangle$ un A-módulo finito generado. Consideremos el epimorfismo de A-módulos $A^r \to M$, $\pi(a_1, \ldots, a_r) := a_1 m_1 + \cdots + a_r m_r$. $\operatorname{Ker}\pi$ es un submódulo de A^r, luego es finito generado. Escribamos, $\operatorname{Ker}\pi = \langle n_1, \ldots, n_s \rangle$ y consideremos

el epimorfismo $\pi' \colon A^s \to \operatorname{Ker}\pi$, $\pi'(a_1,\dots,a_s) := a_1n_1 + \cdots + a_sn_s$. Sea $i \colon \operatorname{Ker}\pi \hookrightarrow A^r$ el morfismo de inclusión y $f := i \circ \pi'$ y consideremos los morfismos

$$\boxed{A^s \xrightarrow{f} A^r \xrightarrow{\pi} M}$$

Entonces, $\operatorname{Im} f = i(\pi'(A^s)) = \operatorname{Ker}\pi$ y $A^r/\operatorname{Im} f \simeq M$. Es decir, hemos construido una presentación por módulos libres finito generados de M.

□

1.3.1. k-álgebras de tipo finito

12. 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 $J = \{a \in A \colon \text{existe } p(x) = ax^n + a_1x^{n-1} + \cdots + a_n \in I\}$. J es un ideal de A: Si $a_0, b_0 \in J$, existen $p(x) = a_0x^n + \cdots + a_n, q(x) = b_0x^m + \cdots + b_m \in I$, luego $x^m p(x) + x^n q(x) = (a_0+b_0)x^{n+m} + \cdots \in I$ y $a_0 + b_0 \in J$. Además, para todo $b \in A$, $bp(x) = ba_0x^n + \cdots + ba_n \in I$, luego $ba_0 \in J$.

Por ser A noetheriano, $J = (b_1,\dots,b_r)$ es finito generado, y existen $p_1,\dots,p_r \in I$ cuyos coeficientes del término de grado máximo son $b_1,\dots,b_r$, respectivamente. Además, multiplicando cada p_i por una potencia conveniente de x, podemos suponer que $\operatorname{gr} p_1 = \cdots = \operatorname{gr} p_r$. Escribamos $\operatorname{gr} p_i = m$, para todo i.

Queremos probar que

$$I = (p_1,\dots,p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}.$$

Dado $q(x) \in I$, tenemos que probar que $q(x) \in (p_1,\dots,p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}$. Procedemos por inducción sobre el grado de $q(x)$. Si $\operatorname{gr}(q(x)) \le m$,entonces evidentemente $q(x) \in I \cap \{A + Ax + \cdots + Ax^{m-1}\} \subseteq (p_1,\dots,p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}$. Si $\operatorname{gr}(q(x)) = n > m$, escribamos $q(x) = a_0x^n + \cdots + a_n$. Sean $\lambda_i \in A$ tales que $a_0 = \lambda_1b_1 + \cdots + \lambda_rb_r$. Entonces. $q_1(x) := q(x) - \sum_i \lambda_i x^{n-m} p_i \in I$ y $\operatorname{gr}(q_1(x)) < \operatorname{gr} q(x)$. Por inducción, $q_1(x) \in (p_1,\dots,p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}$, luego $q(x)$ también.

$I \cap \{A + Ax + \cdots + Ax^{m-1}\}$ 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 $I \cap \{A + Ax + \cdots + Ax^{m-1}\} = \langle q_1,\dots,q_s\rangle_A$, tenemos que $I = (p_1,\dots,p_r,q_1,\dots,q_s)$.

□

13. Definición: Se dice que B es una A-álgebra de tipo finito si existen $\xi_1,\dots,\xi_r \in B$ que generan A-algebraicamente B, es decir,

$$B = A[\xi_1,\dots,\xi_r] := \{ \sum_{n_1,\dots,n_r} a_{n_1,\dots,n_r} \xi_1^{n_1} \cdots \xi_r^{n_r} \in B, \forall\, a_{n_1,\dots,n_r} \in A\},$$

que equivale a decir que el morfismo

$$A[x_1,\dots,x_r] overset \pi \to B, \sum_{n_1,\dots,n_r} a_{n_1,\dots,n_r} x_1^{n_1} \cdots x_r^{n_r} \mapsto \sum_{n_1,\dots,n_r} a_{n_1,\dots,n_r} \xi_1^{n_1} \cdots \xi_r^{n_r}$$

es epiyectivo. Por tanto, si $I = \operatorname{Ker}\pi$, B es una A-álgebra iomorfa a $A[x_1,\dots,x_n]/I$.

14. 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 $k[x_1,\dots,x_n]$ es noetheriano y todo cociente $k[x_1,\dots,x_n]/I$ también. Luego toda k-álgebra de tipo finito es noetheriana.

□

15. Definición: Sean B y C dos A-álgebras. Diremos que un morfismo de anillos $\phi\colon B \to C$ es un morfismo de A-álgebras si $\phi(a) = a$ para todo $a \in A$.

Si $\phi\colon B \to C$ es un morfismo de A-álgebras, $a_{n_1,\dots,n_r} \in A$, $b_1,\dots,b_r \in B$, entonces $\phi(\sum_{n_1,\dots,n_r} a_{n_1,\dots,n_r} b_1^{n_1} \cdots b_r^{n_r}) = \sum_{n_1,\dots,n_r} a_{n_1,\dots,n_r} \phi(b_1)^{n_1} \cdots \phi(b_r)^{n_r}$.

1.4. Extensiones de cuerpos

1.4.1. Cierre algebraico de un cuerpo

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

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

2. Definiciones: Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos. Se dice que $\dim_k \Sigma$ es el grado de la k-extensión Σ. Si $\dim_k \Sigma < \infty$ se dice que Σ es una k-extensión de cuerpos finita.

3. Consideremos una composición de extensiones de cuerpos $k \hookrightarrow K \hookrightarrow \Sigma$. Si $\dim_k K = n$ y $\dim_K \Sigma = m$, entonces $\Sigma = \overset{m}{\oplus} K = \overset{m}{\oplus}(\overset{n}{\oplus} k) = \overset{nm}{\oplus} k$, luego

$$\boxed{\dim_k \Sigma = \dim_k K \cdot \dim_K \Sigma}$$

En particular, la composición de dos extensiones finitas de cuerpos es finita.

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

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

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x - \alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K_1 = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = p_1(\bar{x}_1) = \overline{p(x_1)} = 0$, luego $p(\alpha_1) = 0$. Por tanto, $p(x) = (x - \alpha_1) \cdot p_2(x)$ en $K_1[x]$. Por hipótesis de inducción, existe una extensión $K_1 \hookrightarrow K$ y $\alpha_2, \ldots, \alpha_n \in K$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Como $\alpha_1 \in K$ y $p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n)$ hemos concluido. □

5. Dadas dos k-extensiones de cuerpos K y K', existe una k-extensión de cuerpos, L, que contiene a K y K': Sea $\mathfrak{m} \subset K \otimes_k K'$ un ideal maximal y $L = (K \otimes_k K')/\mathfrak{m}$. Los morfismos $K \hookrightarrow L$, $\lambda \mapsto \overline{\lambda \otimes 1}$ y $K' \hookrightarrow L$, $\lambda' \mapsto \overline{1 \otimes \lambda'}$ son los morfismos buscados.

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

6. Definiciones: Sea $k \hookrightarrow K$ una extensión de cuerpos. Diremos que $\alpha \in K$ es k-algebraico si existe un polinomio $p(x) \in k[x]$ no nulo tal que $p(\alpha) = 0$. Diremos que α es k-trascendente si no es k-algebraico. Diremos que K es una k-extensión algebraica si todo elemento de K es k-algebraico.

7. Ejemplo: Consideremos la extensión de cuerpos $\mathbb{Q} \hookrightarrow \mathbb{C}$. Entonces, $\sqrt{2} \in \mathbb{C}$ es $\mathbb{Q}$-algebraico y $\pi \in \mathbb{C}$ es $\mathbb{Q}$-trascendente (probado por Lindemann en 1882).

8. Definiciones: Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in \Sigma$, se define $k[\alpha_1, \ldots, \alpha_n]$ como el mínimo subanillo de Σ que contiene a k, $\alpha_1, \ldots, \alpha_n$, se define $k(\alpha_1, \ldots, \alpha_n)$ como el mínimo subcuerpo de Σ que contiene a k, $\alpha_1, \ldots, \alpha_n$ y puede comprobarse que

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

9. Si A es una k-álgebra íntegra y $\dim_k A < \infty$, entonces A es una k-extensión finita de cuerpos: Dado $a \in A$ no nulo, la aplicación k-lineal $A \xrightarrow{a\cdot} A$, $b \mapsto a \cdot b$ es inyectiva, luego $\dim_k A = \dim_a \operatorname{Im} a\cdot$ y es epiyectiva, es decir, un isomorfismo lineal. Por tanto, existe $b \in A$ tal que $a \cdot b = 1$, a es inverible y A es un cuerpo.

Por lo tanto, si $\dim_k k[\alpha_1,\dots,\alpha_n] < \infty$, entonces la k-álgebra íntegra $k[\alpha_1,\dots,\alpha_n]$ es un cuerpo y $k[\alpha_1,\dots,\alpha_n] = k(\alpha_1,\dots,\alpha_n)$.

10. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos. Entonces, $\alpha \in K$ es k-algebraico si y solo si* $\dim_k k(\alpha) < \infty$.

Demostración. $\Rightarrow$) Sea $p(x) \in k[x]$ el polinomio mónico mínimo anulador de α. Por 0.2.20, sabemos que $k(\alpha) \simeq k[x]/(p(x)$ y que $\dim_k k(\alpha) = \operatorname{gr} p(x)$.

$\Leftarrow$) Sea $\dim_k k(\alpha) = n < \infty$. Los $n+1$ elementos $1, \alpha, \dots, \alpha^n$ son k-linealmente dependientes, luego existen $\lambda_0,\dots,\lambda_n \in k$ (no todos nulos) tales $\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + \cdots + \lambda_n \alpha^n = 0$. Por tanto, α es raíz del polinomio no nulo $\lambda_0 + \lambda_1 \cdot x + \cdots + \lambda_n x^n$.

□

11. Proposición: *Sea $k \hookrightarrow k(\xi_1,\dots,\xi_n)$ una extensión de cuerpos. Las siguientes condiciones son equivalentes*

1. *$k(\xi_1,\dots,\xi_n)$ es una k-extensión algebraica.*
2. *$\xi_1,\dots,\xi_n$ son k-algebraicos.*
3. *$k(\xi_1,\dots,\xi_n)$ es una k-extensión de cuerpos finita.*

Demostración. 1. $\Rightarrow$ 2. Es obvio.

2. $\Rightarrow$ 3. Consideremos la cadena de inclusiones

$$k \hookrightarrow k(\xi_1) \hookrightarrow k(\xi_1,\xi_2) \hookrightarrow \cdots \hookrightarrow k(\xi_1,\dots,\xi_{n-1}) \hookrightarrow k(\xi_1,\dots,\xi_n).$$

Entonces,

$$\dim_k k(\xi_1,\dots,\xi_n) = \dim_k k(\xi_1) \cdot \dim_{k(\xi_1)} k(\xi_1,\xi_2) \cdots \dim_{k(\xi_1,\dots,\xi_{n-1})} k(\xi_1,\dots,\xi_n) < \infty.$$

3. $\Rightarrow$ 1. Dado $\alpha \in k(\xi_1,\dots,\xi_n)$, tenemos que $\dim_k k(\alpha) \le \dim_k k(\xi_1,\dots,\xi_n) < \infty$, luego α es k-algebraico y $k(\xi_1,\dots,\xi_n)$ es una k-extensión de cuerpos algebraica.

□

12. Corolario: *Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos. El conjunto de todos los elementos k-algebraicos de Σ es una k-subextensión de cuerpos de Σ.*

13. Proposición: *La composición de extensiones de cuerpos algebraicas es algebraica.*

Demostración. Consideremos dos extensiones algebraicas $k \hookrightarrow K$ y $K \hookrightarrow \Sigma$. Dado $\alpha \in \Sigma$, existe un polinomio no nulo $p(x) = a_0x^n + \cdots + a_n \in K[x]$ tal que $p(\alpha) = 0$. Las extensiones de cuerpos $k \hookrightarrow k(a_0,\ldots,a_n)$ y $k(a_0,\ldots,a_n) \hookrightarrow k(a_0,\ldots,a_n,\alpha)$ son finitas, luego

$$\dim_k k(a_0,\ldots,a_n,\alpha) = \dim_k k(a_0,\ldots,a_n) \cdot \dim_{k(a_0,\ldots,a_n)} k(a_0,\ldots,a_n,\alpha) < \infty.$$

Por tanto, $k(a_0,\ldots,a_n,\alpha)$ es una k-extensión de cuerpos algebraica, α es k-algebraico y Σ es una k-extensión de cuerpos algebraica. □

14. Definición: Diremos que un cuerpo K es algebraicamente cerrado si todo polinomio con coeficientes en K tiene todas sus raíces en K.

15. Ejercicio: Prueba que un cuerpo k es algebraicamente cerrado si y solo no existe más k-extensión finita que la extensión $k = k$.

16. Teorema: *Sea k un cuerpo. Existe una única extensión de cuerpos k-algebraica $k \hookrightarrow \bar{k}$, salvo isomorfismos de k-álgebras, tal que $\bar{k}$ es algebraicamente cerrado. Diremos que $\bar{k}$ es el cierre algebraico de k.*

Demostración. Para cada $0 \neq p \in k[x]$, sea $K_p = k(\alpha_1,\ldots,\alpha_n)$, donde $\alpha_1,\ldots\alpha_n$ son todas las raíces del polinomio p. Para cada conjunto finito $\{p_1,\ldots,p_n\} \subset k[x]\backslash\{0\}$ 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 inyectivo

$$K_{p_1} \otimes \ldots \otimes K_{p_n} \to K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m},\ a_1 \otimes \cdots \otimes a_n \mapsto a_1 \otimes \cdots \otimes a_n \otimes 1 \otimes \cdots \otimes 1.$$

Identifiquemos $K_{p_1} \otimes \ldots \otimes K_{p_n}$ con su imagen en cada $K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m}$ y sea

$$A := \bigcup_{\{p_1,\ldots,p_n\} \subset k[x]\backslash\{0\}} K_{p_1} \otimes \ldots \otimes K_{p_n}$$

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 en $\bar{k}$ de las extensiones K_p. Sea $\bar{k} \hookrightarrow K$ una extensión algebraica de cuerpos y $\alpha \in K$, luego α es algebraica sobre k. Sea $p = p(x) \in k[x]$ tal que $p(\alpha) = 0$ anulador de α. K_p contiene todas las raíces de $p(x)$, luego $\bar{k}$ también y $\alpha \in \bar{k}$. En conclusión, $K = \bar{k}$ y $\bar{k}$ es algebraicamente cerrado.

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 $\bar{k} = k'$.

□

17. Definición: Se dice que una k-extensión algebraica de cuerpos K es el cierre algebraico de k, si K es un cuerpo algebraicamente cerrado.

18. Si K es un cuerpo algebraicamente cerrado y $K \hookrightarrow \Sigma$ es una extensión de cuerpos algebraica, entonces $K = \Sigma$, ya que todo $\alpha \in \Sigma$ es raíz de un polinomio $p(x)$ con coeficientes en K y todas las raíces de $p(x)$ están en K.

19. Si $k \hookrightarrow K$ y $k \hookrightarrow K'$ son el cierre algebraico de k, sea $\mathfrak{m} \subset K \otimes_k K'$ un ideal maximal y $\Sigma = (K \otimes_k K')/\mathfrak{m}$. Entonces, $K \hookrightarrow \Sigma$ es una extensión algebraica, luego $K \simeq \Sigma$, e igualmente $K' \simeq \Sigma$. En conclusión, existe un isomorfismo de k-álgebras $K \simeq K'$.

Teorema fundamental del álgebra

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:

$$\begin{aligned}
a_0 &= c \\
a_1 &= -c\cdot(\alpha_1 + \cdots + \alpha_n) \\
&\cdots \\
a_i &= (-1)^i c \cdot \sum_{1\le j_1<\cdots<j_i\le n} \alpha_{j_1}\cdots\alpha_{j_i} \\
&\cdots \\
a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n
\end{aligned}$$

20. Definición: Llamaremos *funciones simétricas elementales* (o polinomios simétricos elementales) en las letras $x_1,\ldots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\ldots,x_n]$ $(i = 1,\ldots,n)$ definidos por:

$$\begin{aligned}
s_1 &= x_1 + \cdots + x_n \\
&\cdots \\
s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\
&\cdots \\
s_n &= x_1\cdots x_n
\end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

y $a_i = (-1)^i a_0\cdot s_i(\alpha_1,\ldots,\alpha_n)$, donde seguimos las notaciones del principio de las sección.

Sea S_n el grupo de las permutaciones de n letras. Consideremos la operación de S_n en $A[x_1,\dots x_n]$ siguiente:

$$\sigma(p(x_1,\dots,x_n)) := p(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

para cada $\sigma \in S_n, p(x_1,\dots,x_n) \in A[x_1,\dots x_n]$.

21. Definición: Diremos que un polinomio $p(x_1,\dots,x_n) \in A[x_1,\dots x_n]$ es simétrico cuando $\sigma(P) = P$ para toda $\sigma \in S_n$. Al conjunto de las funciones simétricas las denotaremos $A[x_1,\dots x_n]^{S_n}$.

22. Teorema de las funciones simétricas: *Se verifica la igualdad:*

$$A[x_1,\dots,x_n]^{S_n} = A[s_1,\dots,s_n]$$

Es decir, un polinomio en $x_1,\dots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y solo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Procedemos por inducción sobre el número n de variables. Para $n = 1$ es trivial. Sea $p(x_1,\dots,x_n) \in A[x_1,\dots,x_n]^{S_n}$. Descomponiendo $p(x_1,\dots,x_n)$ en la suma de sus componentes homogéneas, podemos suponer que $p(x_1,\dots,x_n)$ es un polinomio homogéneo de grado m. Haciendo cociente por x_n se obtiene que $p(x_1,\dots,x_{n-1},0)$ es un polinomio homogéneo de grado m en $n-1$ variables e invariante por las permutaciones de éstas, luego $p(x_1,\dots,x_{n-1},0) = q'(s'_1,\dots,s'_{n-1})$, siendo s'_i la i-ésima función simétrica elemental en las $n-1$ primeras variables. Observemos que en $q'(s'_1,\dots,s'_{n-1})$ cada sumando $\lambda_{m_1,\dots,m_{n-1}} s'^{m_1}_1 \cdots s'^{m_{n-1}}_{n-1}$ es un polinomio homogéneo en las variables $x_1,\dots,x_{n-1}$ de grado $m_1 + 2m_2 + \cdots + (n-1)m_{n-1}$. Podemos suponer que $\lambda_{m_1,\dots,m_{n-1}} = 0$, cuando $m_1 + 2m_2 + \cdots + (n-1)m_{n-1} \neq m$. Por tanto, $q'(s_1,\dots,s_{n-1})$ es un polinomio en $x_1,\dots,x_n$ homogéneo de grado m. Sea $h(x_1,\dots,x_n) = p(x_1,\dots,x_n) - q'(s_1,\dots,s_{n-1})$. Se verifica que $h(x_1,\dots,x_n)$ 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, $h(x_1,\dots,x_n) = s_n \cdot h'(x_1,\dots,x_n)$ y, por tanto, $h'(x_1,\dots,x_n)$ es simétrico también y homogéneo de grado $gr(h'(x_1,\dots,x_n)) = gr(h(x_1,\dots,x_n)) - n = gr(p(x_1,\dots,x_n)) - n < gr(p(x_1,\dots,x_n))$, luego por recurrencia sobre el grado m de $p(x_1,\dots,x_n)$ se concluye que $h'(x_1,\dots,x_n) = \widetilde{q}(s_1,\dots,s_n)$. Sustituyendo en la definición de $h(x_1,\dots,x_n)$ y despejando se obtiene:

$$p(x_1,\dots x_n) = q'(s_1,\dots,s_{n-1}) + s_n \cdot \widetilde{q}(s_1,\dots,s_n)$$

con lo que se concluye. □

23. 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 $q(x) \in \mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} q(x) = -\lim_{x\to-\infty} q(x), \quad (\text{y } |\lim_{x\to+\infty} q(x)| = +\infty)$$

Luego por el teorema de Bolzano existe un $\alpha \in \mathbb{R}$ tal que $q(\alpha) = 0$. Supongamos que $\operatorname{gr} q(x) = r = 2^n \cdot m$, con m impar. Para probar que $q(x)$ 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 $q(x)$ 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 $q(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2} = 2^{n-1} \cdot m \cdot (r-1) = 2^{n-1} \cdot m'$ 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 $\alpha_r, \alpha_s = (a \pm \sqrt{a^2 - 4b})/2 \in \mathbb{C}$. □

24. Ejercicio: Prueba que $\mathbb{C}$ es el cierre algebraico de $\mathbb{R}$.

1.4.2. Grado de trascendencia de una k-extensión de cuerpos de tipo finito

25. Definiciones: Sea Σ una k-extensión de cuerpos. Diremos que $\xi_1, \ldots, \xi_n \in \Sigma$ son k-algebraicamente independientes cuando cualquier relación k-algebraica

$$\sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} \xi_1^{i_1} \ldots \xi_n^{i_n} = 0, \text{ con coeficientes } a_{i_1 \ldots i_n} \in k$$

implica que todos los coeficientes $a_{i_1 \ldots i_n}$ son nulos. Los elementos $\xi_1, \ldots, \xi_n \in \Sigma$ son k-algebraicamente independientes si y solo si el morfismo de k-álgebras

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

es inyectivo, y en este caso el morfismo $k(x_1,\dots,x_n) \to k(\xi_1,\dots,\xi_n)$, $\frac{p(x_1,\dots,x_n)}{q(x_1,\dots,x_n)} \mapsto \frac{p(\xi_1,\dots,\xi_n)}{q(\xi_1,\dots,\xi_n)}$ es un isomorfismo. Si $\Sigma = k(\xi_1,\dots,\xi_n)$ diremos que Σ es una k-extensión de cuerpos de tipo finito.

26. Ejercicio: Sea Σ una k-extensión de cuerpos y $\xi_1,\dots,\xi_n \in \Sigma$ k-algebraicamente independientes. Dado $\alpha \in \Sigma$ se cumple que $\xi_1,\dots,\xi_n,\alpha$ son k-algebraicamente independientes si y solo si α es $k(\xi_1,\dots,\xi_n)$-trascendente.

27. 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 k-algebraicamente independientes y Σ es una $k(\xi_1,\dots,\xi_n)$-extensión algebraica.

28. Proposición: *Sea $k \to \Sigma$ una extensión de cuerpo, $\xi_1,\dots,\xi_n \in \Sigma$ y $\eta_1,\dots,\eta_m \in \Sigma$ dos bases de k-trascendencia de Σ. Entonces, $n = m$.*

Demostración. Probemos que Σ es una extensión algebraica de $k(\xi_1,\dots,\xi_i,\eta_{i+1},\dots,\eta_m)$, dado $0 \le i \le n$, reordenando si es preciso los elementos η_j. Procedemos por inducción sobre i. Si $i = 0$ sabemos que $k(\eta_1,\dots,\eta_m) \hookrightarrow \Sigma$ es algebraica. Si $i \ge 1$, por hipótesis de inducción ξ_i es $k(\xi_1,\dots,\xi_{i-1},\eta_i,\dots,\eta_m)$-algebraico. Entonces existe un polinomio no nulo $p(x_1,\dots,x_i,y_i,\dots,y_m) \in k[x_1,\dots,x_i,y_i,\dots,y_m]$ tal que $p(\xi_1,\dots,\xi_i,\eta_i,\dots,\eta_m) = 0$. Como $\xi_1,\dots,\xi_i$ son algebraicamente independientes, alguna de las variables y_j (podemos suponer reordenando que $j = i$) aparece en el polinomio antes mencionado y $p(\xi_1,\dots,\xi_i,x,\eta_{i+1},\dots,\eta_m) \neq 0$. Por tanto, η_i es algebraico sobre $k(\xi_1,\dots,\xi_i,\eta_{i+1},\dots,\eta_m)$ y se tienen las extensiones algebraicas

$$k(\xi_1,\dots,\xi_{i-1},\xi_i,\eta_{i+1},\dots,\eta_m) \hookrightarrow k(\xi_1,\dots,\xi_{i-1},\xi_i,\eta_i,\eta_{i+1},\dots,\eta_m) \hookrightarrow \Sigma$$

luego Σ es algebraico sobre $k(\xi_1,\dots,\xi_i,\eta_{i+1},\dots,\eta_m)$.

Ahora, si m fuera menor estricto 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 k-algebraicamente independientes. Del mismo modo podemos probar que n no puede ser menor estricto m. □

29. Teorema: *Sea $k \hookrightarrow \Sigma = k(\xi_1,\dots,\xi_r)$ una extensión de cuerpos de tipo finito. Existen bases de trascendencia de Σ sobre k.*

Demostración. Sea n el número máximo de los elementos $\xi_1,\dots,\xi_n$ k-algebraicamente independientes. Reordenándolos, si fuera preciso, podemos suponer que $\xi_1,\dots,\xi_n$ son k-algebraicamente independientes y que $\xi_1,\dots,\xi_n,\xi_i$ no son k-algebraicamente independientes para todo $i > n$. Por tanto, existe un polinomio no nulo $p(x_1,\dots,x_n,x_i) \in k[x_1,\dots,x_n,x_i]$ tal que $p(\xi_1,\dots,\xi_n,\xi_i) = 0$. Como $\xi_1,\dots,\xi_n$ son algebraicamente independientes, la variable x_i ha de aparecer en el polinomio $p(x_1,\dots,x_n,x_i)$ y ξ_i es raíz de

$p(\xi_1,\dots,\xi_n,x) \in k(\xi_1,\dots,\xi_n)[x]$. Por tanto, ξ_i es $k(\xi_1,\dots,\xi_n)$-algebraico, para todo $i > n$. Por 1.4.11, 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.

□

30. Definición: El número de elementos de una base de trascendencia de una extensión de cuerpos $k \hookrightarrow \Sigma$ se dice que es el grado de trascendencia de Σ sobre k y se denota $\mathrm{gr\,tr}_k\,\Sigma$.

31. Ejemplo: Sea k un cuerpo. El cuerpo de fracciones polinómicas en n variables $k(x_1,\dots,x_n)$ tiene grado de trascendencia n, porque las funciones $x_1,\dots,x_n$ forman claramente una base de trascendencia sobre k.

32. Ejemplo: Sea $p(x_1,\dots,x_n)$ un polinomio irreducible no constante con coeficientes en un cuerpo k. Sea $k(\bar{x}_1,\dots,\bar{x}_n)$ 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 $p(x_1,\dots,x_n) = 0$. Se cumple que $k(\bar{x}_1,\dots,\bar{x}_n)$ 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 $\{\bar{x}_1,\dots,\bar{x}_{n-1}\}$ es una base de trascendencia.

1.5. Biografía de Hilbert

HILBERT BIOGRAPHY

David Hilbert's father, Otto Hilbert, was the son of a judge who was a high ranking Privy Councillor. Otto was a county judge who had married Maria Therese Erdtmann, the daughter of Karl Erdtmann, a Königsberg merchant. Maria was fascinated by philosophy, astronomy and prime numbers. Otto Hilbert had a brother who was a lawyer and another who was the director of a Gymnasium. After Otto was promoted to become a senior judge, he and Maria moved to 13 Kirchenstrasse in Königsberg and this was the home in which David spent much of his childhood. He had a strict upbringing by his father who was a man who lived his life to a standard pattern, always walking the same way every day and only leaving Königsberg once a year for the annual family holiday. David was his parents' first child and only son. He was six years old when his sister Elsie was born.

The usual age for someone to begin schooling was six but David did not enter his first school, the Royal Friedrichskolleg, until he was eight years old. It is almost certain that his mother taught him at home until he was eight. The Friedrichskolleg, also known as the Collegium Fridericianum, had a junior section which David attended for two years before entering the gymnasium of the Friedrichskolleg in 1872. Although this was reputed to be the best school in Königsberg, the emphasis was on Latin and Greek with mathematics considered as less important. Science was not taught at all in the Friedrichskolleg. The main approach to learning was having pupils memorise large amounts of material, something David was not particularly good at. Perhaps surprisingly for someone who was to make a gigantic impact on mathematics, he did not shine at school. In later life he described himself as a "dull and sill" boy at the Friedrichskolleg. Although doubtless there is modesty in these words, nevertheless they probably reflect Hilbert's own feeling about his school days. In September 1879 he transferred from the Friedrichskolleg to the Wilhelm Gymnasium where he spent his final year of schooling. Here there was more emphasis on mathematics and the teachers encouraged original thinking in a way that had not happened at the Friedrichskolleg. Hilbert was much happier and his performance in all his subjects improved. He received the top grade for mathematics and his final report stated:

"*For mathematics he always showed a very lively interest and a penetrating understanding: he mastered all the material taught in the school in a very pleasing manner and was able to apply it with sureness and ingenuity.*"

After graduating from the Wilhelm Gymnasium, he entered the University of Königsberg in the autumn of 1880. In his first semester he took courses on integral calculus, the theory of determinants and the curvature of surfaces. Then following the tradition in Germany at this time, in the second semester he went to Heidelberg where he attended lectures by Lazarus Fuchs. Returning to Königsberg for the start of session 1881-82, Hilbert attended lectures on number theory and the theory of functions by Heinrich Weber. In the spring of 1882, Hermann Minkowski returned to Königsberg after studying in Berlin. Hilbert and Minkowski, who was also a doctoral student, soon became close friends and they were to strongly influence each others mathematical progress. Ferdinand von Lindemann was appointed to Königsberg to succeed Heinrich Weber in 1883 and Adolf Hurwitz was appointed as an extraordinary professor there in the spring of 1884. Hurwitz and Hilbert became close friends, another friendship which was important factor in Hilbert's mathematical development, while Lindemann became Hilbert's thesis advisor. He received his oral examination on 11 December 1884 for his thesis entitled Über invariante Eigenschaften specieller binärer Formen, insbesondere der Kugelfunctionen. Lindemann had suggested that Hilbert study invariant properties of certain algebraic forms and Hilbert showed great originality in devising an approach that Lindemann had not envisaged. Minkowski, after reading

the thesis, wrote to Hilbert:

"*I studied your work with great interest and rejoiced over all the processes which the poor invariants had to pass through before they manage to disappear. I would not have supposed that such a good mathematical theorem could have been obtained in Königsberg.*"

On 7 February 1885 he defended two propositions in a public disputation. One of Hilbert's chosen propositions was on physics, the other on philosophy. This was the final stage of his doctorate, which was then duly awarded. He spent the month following the award of his doctorate taking, and passing, the Staatsexamen so that he was qualified to teach in a Gymnasium, and he also attended Lindemann's geometry course on Plücker's line geometry and Lie's sphere geometry, and he also attended Hurwitz's lectures on modular functions. Hurwitz suggested that Hilbert make a research visit to Leipzig to speak with Felix Klein. Taking this advice, he went to Leipzig and attended Klein's lectures. He also got to know Georg Pick and Eduard Study. Klein suggested that both Hilbert and Study should visit Erlangen and discuss their research with Paul Gordan who was the leading expert on invariant theory. However, the visit did not take place at that time. Klein then told both Study and Hilbert that they should visit Paris. They both went in early 1886, Hilbert at the end of March. Klein had given them instructions as to which of the Paris mathematicians they should visit and they did as he told them, alternately writing to Klein about their experiences. One of the first mathematicians they visited was Henri Poincaré who returned their visit a few days later. The two young visitors read their letters to Klein out loud to each other so that they would not both tell him the same things. He replied to each in turn, making clear that he was treating them equally. In Paris, Camille Jordan gave a dinner for Hilbert and Study to which George-Henri Halphen, Amédée Mannheim and Gaston Darboux were invited. On this occasion the French mathematicians all spoke German out of politeness to their German guests who complained to Klein afterwards that the mathematical conversation had been very superficial. They were also disappointed with their meeting with Pierre Bonnet who they felt was too old for mathematical discussions. The mathematician with whom they seemed to get on best was Charles Hermite. Although they considered him very old (he was 64), he was "extraordinarily friendly and hospitable" and discussed the big problems of invariant theory. Since they had found their visit especially useful, they returned to Hermite's home for a second visit a few days later. It is clear that Hilbert's thoughts were entirely on mathematics during his time in Paris and he wrote nothing of any sightseeing. Towards the end of his visit he suffered an illness and was probably homesick. Certainly by the spring of 1886 he was in good spirits as he returned to Germany. On his way back to Königsberg he visited Göttingen, where Klein was about to take up the chair, where he met Hermann Amandus Schwarz. Telling Schwarz that he was next going to Berlin,

Hilbert was advised to expect a cold reception by Leopold Kronecker. However, Hilbert described his welcome in Berlin as very friendly.

From Berlin, Hilbert continued back to Königsberg where he prepared to submit his habilitation paper on invariant theory. He also had to give an inaugural lecture in the main auditorium of the Albertina and, from the two options offered by Hilbert, he was asked to deliver the lecture The most general periodic functions. Klein had told Hilbert that Königsberg may not be a good place for him to habilitate but Hilbert was happy to do so. He wrote to Klein:

"*I am content and full of joy to have decided myself for Königsberg. The constant association with Professor Lindemann and, above all, with Hurwitz is not less interesting than it is advantageous to myself and stimulating. The bad part about Königsberg being so far away from things I hope I will be able to overcome by making some trips again next year, and perhaps then I will get to meet Herr Gordan.*"

He was a member of staff at Königsberg from 1886 to 1895, being a Privatdozent until 1892, then as Extraordinary Professor for one year before being appointed a full professor in 1893. The tour that he spoke about after habilitating at Königsberg happened in 1888:

"*... he set off in March 1888 on a tour of several leading mathematical centres in Germany, including Berlin, Leipzig, and Göttingen. During the course of a month, he spoke with some twenty mathematicians from whom he gained a stimulating overview of current research interests throughout the country.*"

In Berlin he met Kronecker and Weierstrass who presented the young Hilbert with two rather different views of the future. Next, in Leipzig, he finally met Paul Gordan:

"*... the two hit it off splendidly, as both loved nothing more than to talk about mathematics.*

Hilbert spent eight days in Göttingen before returning to Königsberg. He married his second cousin, Käthe Jerosch, on 12 October 1892; they had one son Franz Hilbert born on 11 August 1893.

In 1892 Schwarz moved from Göttingen to Berlin to occupy Weierstrass's chair and Klein wanted to offer Hilbert the vacant Göttingen chair. However Klein failed to persuade his colleagues and Heinrich Weber was appointed to the chair. Klein was probably not too unhappy when Weber moved to a chair at Strasbourg three years later since on this occasion he was successful in his aim of appointing Hilbert. So, in 1895, Hilbert was appointed to the chair of mathematics at the University of Göttingen, where he continued to teach for the rest of his career.

Hilbert's eminent position in the world of mathematics after 1900 meant that other institutions would have liked to tempt him to leave Göttingen and, in 1902, the University of Berlin offered Hilbert Fuchs's chair. Hilbert turned down the Berlin chair, but only after he had used the offer to bargain with Göttingen and persuade them to

set up a new chair to bring his friend Minkowski to Göttingen.

As we saw above, Hilbert's first work was on invariant theory and, in 1888, he proved his famous Basis Theorem. Twenty years earlier Gordan had proved the finite basis theorem for binary forms using a highly computational approach. Attempts to generalise Gordan's work to systems with more than two variables failed since the computational difficulties were too great. Hilbert himself tried at first to follow Gordan's approach but soon realised that a new line of attack was necessary. He discovered a completely new approach which proved the finite basis theorem for any number of variables but in an entirely abstract way. Although he proved that a finite basis existed his methods did not construct such a basis.

Hilbert submitted a paper proving the finite basis theorem to Mathematische Annalen. However Gordan was the expert on invariant theory for Mathematische Annalen and he found Hilbert's revolutionary approach difficult to appreciate. He refereed the paper and sent his comments to Klein:

"*The problem lies not with the form ... but rather much deeper. Hilbert has scorned to present his thoughts following formal rules, he thinks it suffices that no one contradict his proof ... he is content to think that the importance and correctness of his propositions suffice. ... for a comprehensive work for the 'Annalen' this is insufficient.*"

However, Hilbert had learnt through his friend Hurwitz about Gordan's letter to Klein and Hilbert wrote himself to Klein in forceful terms.

"*... I am not prepared to alter or delete anything, and regarding this paper, I say with all modesty, that this is my last word so long as no definite and irrefutable objection against my reasoning is raised.*"

At the time Klein received these two letters from Hilbert and Gordan, Hilbert was an assistant lecturer while Gordan was the recognised leading world expert on invariant theory and also a close friend of Klein's. However Klein recognised the importance of Hilbert's work and assured him that it would appear in the Annalen without any changes whatsoever, as indeed it did.

Hilbert expanded on his methods in a later paper, again submitted to the Mathematische Annalen and Klein, after reading the manuscript, wrote to Hilbert saying:

"*I do not doubt that this is the most important work on general algebra that the 'Annalen' has ever published.*"

In 1893 while still at Königsberg Hilbert began a work Zahlbericht on algebraic number theory. The German Mathematical Society requested this major report three years after the Society was created in 1890. The Zahlbericht (1897) is a brilliant synthesis of the work of Kummer, Kronecker and Dedekind but also contains a wealth of Hilbert's own ideas. The ideas of the present day subject of "Class field theory" are all contained in this work. Rowe describes this work as:

"*... not really a Bericht in the conventional sense of the word, but rather a piece*

of original research revealing that Hilbert was no mere specialist, however gifted. ... he not only synthesized the results of prior investigations ... but also fashioned new concepts that shaped the course of research on algebraic number theory for many years to come."

Hilbert's work in geometry had the greatest influence in that area after Euclid. A systematic study of the axioms of Euclidean geometry led Hilbert to propose 21 such axioms and he analysed their significance. He published Grundlagen der Geometrie in 1899 putting geometry in a formal axiomatic setting. The book continued to appear in new editions and was a major influence in promoting the axiomatic approach to mathematics which has been one of the major characteristics of the subject throughout the 20th century.

Hilbert's famous 23 Paris problems challenged (and still today challenge) mathematicians to solve fundamental questions. Hilbert's famous speech The Problems of Mathematics was delivered to the Second International Congress of Mathematicians in Paris. It was a speech full of optimism for mathematics in the coming century and he felt that open problems were the sign of vitality in the subject:

"*The great importance of definite problems for the progress of mathematical science in general ... is undeniable. ... [for] as long as a branch of knowledge supplies a surplus of such problems, it maintains its vitality. ... every mathematician certainly shares ..the conviction that every mathematical problem is necessarily capable of strict resolution ... we hear within ourselves the constant cry: There is the problem, seek the solution. You can find it through pure thought...*

Hilbert's problems included the continuum hypothesis, the well ordering of the reals, Goldbach's conjecture, the transcendence of powers of algebraic numbers, the Riemann hypothesis, the extension of Dirichlet's principle and many more. Many of the problems were solved during this century, and each time one of the problems was solved it was a major event for mathematics.

Today Hilbert's name is often best remembered through the concept of Hilbert space. Irving Kaplansky explains Hilbert's work which led to this concept:

"*Hilbert's work in integral equations in about 1909 led directly to 20th -century research in functional analysis (the branch of mathematics in which functions are studied collectively). This work also established the basis for his work on infinite-dimensional space, later called Hilbert space, a concept that is useful in mathematical analysis and quantum mechanics. Making use of his results on integral equations, Hilbert contributed to the development of mathematical physics by his important memoirs on kinetic gas theory and the theory of radiations.*"

Many have mistakenly claimed that in 1915 Hilbert discovered the correct field equations for general relativity before Einstein but never claimed priority.

In 1934 and 1939 two volumes of Grundlagen der Mathematik were published

which were intended to lead to a 'proof theory', a direct check for the consistency of mathematics. Gödel's paper of 1931 showed that this aim is impossible.

Hilbert contributed to many branches of mathematics, including invariants, algebraic number fields, functional analysis, integral equations, mathematical physics, and the calculus of variations. His mathematical abilities were nicely summed up by Otto Blumenthal, his first student:

"*In the analysis of mathematical talent one has to differentiate between the ability to create new concepts that generate new types of thought structures and the gift for sensing deeper connections and underlying unity. In Hilbert's case, his greatness lies in an immensely powerful insight that penetrates into the depths of a question. All of his works contain examples from far-flung fields in which only he was able to discern an interrelatedness and connection with the problem at hand. From these, the synthesis, his work of art, was ultimately created. Insofar as the creation of new ideas is concerned, I would place Minkowski higher, and of the classical great ones, Gauss, Galois, and Riemann. But when it comes to penetrating insight, only a few of the very greatest were the equal of Hilbert.*"

Among Hilbert's students were Hermann Weyl, the famous world chess champion Emanuel Lasker, and Ernst Zermelo. But the list includes many other famour names including Wilhelm Ackermann, Felix Bernstein, Otto Blumenthal, Richard Courant, Haskell Curry, Max Dehn, Rudolf Fueter, Alfred Haar, Georg Hamel, Erich Hecke, Earle Hedrick, Ernst Hellinger, Edward Kasner, Oliver Kellogg, Hellmuth Kneser, Otto Neugebauer, Erhard Schmidt, Hugo Steinhaus, and Teiji Takagi.

In 1930 Hilbert retired but only a few years later, in 1933, life in Göttingen changed completely when the Nazis came to power and Jewish lecturers were dismissed. By the autumn of 1933 most had left or were dismissed. Hilbert, although retired, had still been giving a few lectures. In the winter semester of 1933-34 he gave one lecture a week on the foundations of geometry. After he finished giving this course he never set foot in the Institute again. In early 1942 he fell and broke his arm while walking in Göttingen. This made him totally inactive and this seems to have been a major factor in his death a year after the accident.

Hilbert received many honours. In 1905 the Hungarian Academy of Sciences gave a special citation for Hilbert. He was awarded the Bolyai Prize in 1910 and elected a fellow of the Royal Society of London in 1928. In 1930 Hilbert retired and the city of Königsberg made him an honorary citizen of the city. He gave an address which ended with six famous words showing his enthusiasm for mathematics and his life devoted to solving mathematical problems:

"*Wir müssen wissen, wir werden wissen - We must know, we shall know.*"

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

1.6. Cuestionario

1. ¿Es $\mathbb{Q}$ un $\mathbb{Z}$-módulo noetheriano?
2. ¿Es $\mathbb{Q}[x]$ un $\mathbb{Z}$-módulo noetheriano?¿Es $\mathbb{Q}[x]$ un anillo noetheriano?
3. ¿Es $\mathbb{Z}[x_1, x_2, x_3]$ un anillo noetheriano?
4. Sea $A \to B$ un morfismo de anillos. Si A es un anillo noetheriano y B, que es de modo natural un A módulo, resulta que es un A-módulo finito generado ¿es B un anillo noetheriano?
5. ¿Es el cociente de un anillo noetheriano por un ideal un anillo noetheriano?
6. Sea $M = \langle m_i \rangle_{i \in I}$ un A-módulo noetheriano. Prueba que existe un subconjunto finito $J \subset I$ tal que $M = \langle m_j \rangle_{j \in J}$.
7. Sea Y un conjunto y $p_i(x_1, \ldots, x_n) = 0$, $\forall\, i \in Y$, un sistema de ecuaciones k-algebraico en n variables. Prueba que salvo un número finito de las ecuaciones todas las demás son redundantes.
8. ¿Es el cociente de una k-álgebra de tipo finito por un ideal una k-álgebra de tipo finito?
9. ¿Toda extensión finita de cuerpos es una extensión de tipo finito?¿Toda extensión de cuerpos de tipo finito es una extensión de cuerpos finita?
10. Da un ejemplo de extensión de cuerpos que no sea de tipo finito.
11. Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos y $\xi_1, \xi_2 \in \Sigma$. Prueba que $k(\xi_1)(\xi_2) = k(\xi_1, \xi_2)$.
12. ¿Cuál es el grado de trascendencia de una extensión de cuerpos algebraica?

1.7. Problemas

1. Sea A un anillo íntegro. Prueba que A es un dominio de factorización si y solo si toda cadena ascendente de ideales principales estabiliza. Prueba $k[x_1, \ldots, x_n]$ y $k[[x_1, \ldots, x_n]]$ son dominios de factorización.
2. Prueba que $k[x_1, \ldots, x_n \ldots]$ es DFU, pero no es un anillo noetheriano
3. Sea M un A-módulo noetheriano. Prueba que todo endomorfismo de A-módulos epiyectivo $f : M \to M$ es un isomorfismo. (Indicación: Considera los submódulos $\operatorname{Ker} f^n$.)

4. Define una aplicación k-lineal epiyectiva $\overset{\mathbb{N}}{\oplus}\mathbb{Q} \to \overset{\mathbb{N}}{\oplus}\mathbb{Q}$ que no sea isomorfismo lineal.

5. Sean N y N_0 dos submódulos de un A-módulo M. Prueba que $N + N_0$ es un A-módulo noetheriano si y solo si N y N_0 son A-módulos noetherianos.

6. Sean N y N_0 dos submódulos de un A-módulo M tales que $N_0 \cap N = 0$. Prueba que M es un A-módulo noetheriano si y sólo si M/N y M/N_0 son A-módulos noetherianos.

7. Sea A un anillo noetheriano. Prueba:

   a) Si $I \subset A$ es un ideal, entonces A/I es un anillo noetheriano.

   b) Si $S \subset A$ es un sistema multiplicativo, entonces A_S es un anillo noetheriano.

8. Sea M un A-módulo noetheriano y N un A-módulo finito generado. Prueba que $\mathrm{Hom}_A(N, M)$ es un A-módulo noetheriano.

9. Sea M un A-módulo noetheriano e $\mathrm{Anul}(M) := \{a \in A : a \cdot m = 0, \forall\, m \in M\}$. Prueba que $A/\mathrm{Anul}(M)$ es un anillo noetheriano.

10. Sea M un A-módulo finito generado y N un A-módulo noetheriano. Prueba que $M \otimes_A N$ es un A-módulo noetheriano.

11. ¿Es $\overset{\mathbb{N}}{\prod}\mathbb{Z}$ un anillo noetheriano?

12. Sea I el ideal de $C^\infty(\mathbb{R}^n)$ formado por las funciones infinitamente diferenciables de $\mathbb{R}^n$ que se anulan en algún entorno del punto $x = 0$. Demuestra que el ideal I no es finito generado y concluye que el anillo $C^\infty(\mathbb{R}^n)$ no es noetheriano cuando $n \geq 1$.

13. Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos y $\xi_1, \ldots, \xi_n \in \Sigma$ elementos k-algebraicamente independientes. Sea $\alpha \in \Sigma$. Prueba que $\xi_1, \ldots, \xi_n, \alpha \in \Sigma$ son k-algebraicamente independientes si y solo si α es $k(\xi_1, \ldots, \xi_n)$-trascendente.

14. Sean $k \hookrightarrow K$ y $K \hookrightarrow \Sigma$ dos extensiones de tipo finito. Prueba que

$$\mathrm{gr\,tr}_k \Sigma = \mathrm{gr\,tr}_k K + \mathrm{gr\,tr}_K \Sigma.$$

15. Cúal es el grado de trascendencia de la $\mathbb{R}$-extensión de cuerpos $\mathbb{R} \hookrightarrow \mathbb{C}(x, y)$?

16. Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos de tipo finito. Prueba que todo conjunto de elementos k-algebraicamente independientes de Σ forma parte de una base de trascendencia.

17. Sea k un cuerpo de característica cero y K y K' dos k-extensiones de cuerpos. Prueba que $K \otimes_k K'$ es un anillo reducido.

Capítulo 2

Espectro primo de un anillo

2.1. Introducción

El espectro primo de un anillo A, denotado $\operatorname{Spec} A$, es un concepto básico de la Geometría Algebraica y del Álgebra Conmutativa. Permite traducir conceptos del Álgebra Conmutativa en términos geométricos, abriendo la puerta a una rica interacción entre el Álgebra y la Geometría.

$\operatorname{Spec} A$ es el conjunto de los ideales primos de A, dotado de una topología natural llamada topología de Zariski. Cada morfismo de anillos $f: A \to B$, define la aplicación continua $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$, $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$. Dados el morfismo de localización $A \to A_a$, $b \mapsto \frac{b}{1}$, el morfismo de paso al cociente $A \to A/I$, $a \mapsto \bar{a}$, la proyección en el primer factor $A \times B \to A$, $(a,b) \mapsto a$ y el morfismo $A \to A \otimes_k B$, $a \mapsto a \otimes 1$ (donde A y B son k-álgebras) interpretaremos geométricamente $\operatorname{Spec} A_a$, $\operatorname{Spec} A/I$, $\operatorname{Spec}(A \times B)$, $\operatorname{Spec}(A \otimes_k B)$ y las aplicaciones continuas inducidas en los espectros por estos morfismos.

Dado un sistema de ecuaciones k-algebraicas

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

consideremos el conjunto de todas las soluciones del sistema de ecuaciones. En este capítulo trataremos de justificar que $A := k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ es el anillo de funciones algebraicas del conjunto de soluciones del sistema de ecuaciones, y estudiaremos en qué sentido $\operatorname{Spec} A$ puede identificarse con el conjunto de soluciones del sistema de ecuaciones anterior.

75

2.2. Espectro racional de una k-álgebra

1. Notación: Sean A y B dos k-álgebras. $\mathrm{Hom}_{k-alg}(A,B)$ denotará el conjunto de los morfismos de k-álgebras de A en B.

2. Proposición: *Las aplicaciones*

$$\begin{array}{rcl} \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_r],A) & = & A^r \\ \phi & \longmapsto & (\phi(x_1),\ldots,\phi(x_r)) \\ \phi_\alpha(p(x)) := p(\alpha) \qquad \phi_\alpha & \longmapsto & \alpha \end{array}$$

son inversas entre si.

3. Proposición: *Sea A una k-álgebra. Las asignaciones*

$$\begin{array}{rcl} \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),A) & \longleftrightarrow & \left\{ a\in A^n : \begin{array}{c} p_1(a)=0 \\ \cdots \\ p_r(a)=0 \end{array} \right\} \\ \phi & \longmapsto & (\phi(\bar{x}_1),\ldots,\phi(\bar{x}_n)) \\ \tilde{\phi}(\overline{q(x_1,\ldots,x_n)}) := q(a_1,\ldots,a_n), \qquad \tilde{\phi} & \longmapsto & (a_1,\ldots,a_n) \end{array}$$

son inversas entre sí.

4. Todo morfismo de k-álgebras $f: A \to B$ induce la aplicación

$$f^*: \mathrm{Hom}_{k-alg}(B,k) \to \mathrm{Hom}_{k-alg}(A,k),\ g \mapsto g\circ f.$$

Así pues, todo morfismo de k-álgebras

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

induce la aplicación

$$\begin{array}{rcl} \mathrm{Hom}_{k-alg}(k[y_1,\ldots,y_m]/(q_1,\ldots,q_s),k) & \stackrel{f^*}{\to} & \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),k) \\ g & \mapsto & g\circ f \end{array}$$

Si $\beta_i = g(\bar{y}_i)$, entonces $(g\circ f)(\bar{x}_i) = g(\overline{f_i(y_1,\ldots,y_m)}) = f_i(\beta_1,\ldots,\beta_m)$ y tenemos el diagrama conmutativo

$$\begin{array}{ccc}
\mathrm{Hom}_{k-alg}(k[y_1,\ldots,y_m]/(q_1,\ldots,q_s),k) & \xrightarrow{f^*} & \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),k) \\
\| & & \| \\
\left\{\begin{array}{ll} \text{Sol.} & \begin{array}{c} q_1(y_1,\ldots,y_m)=0 \\ \cdots \\ q_s(y_1,\ldots,y_m)=0 \end{array} \end{array}\right\} & \longrightarrow & \left\{\begin{array}{ll} \text{Sol.} & \begin{array}{c} p_1(x_1,\ldots,x_n)=0 \\ \cdots \\ p_r(x_1,\ldots,x_n)=0 \end{array} \end{array}\right\} \\
(\beta_1,\ldots,\beta_m) & \longmapsto & (f_1(\beta_1,\ldots,\beta_m),\ldots,f_n(\beta_1,\ldots,\beta_m)
\end{array}$$

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

$$\mathrm{Spec}_{rac} A := \{\text{Ideales } \mathfrak{m} \subset A \text{ tales que } A/\mathfrak{m} = k\}.$$

6. Notación: Dado un ideal racional $\mathfrak{m}_y \subset A$, denotaremos al morfismo de k-álgebras de paso al cociente $A \to A/\mathfrak{m}_y = k$, $a \mapsto \bar{a}$ por y, es decir, $y(a) := \bar{a} \in k$. También denotaremos $a(y) := y(a) = \bar{a}$.

7. Proposición: *Sea A una k-álgebra. Entonces,* $\mathrm{Spec}_{rac} A = \mathrm{Hom}_{k-alg}(A,k)$.

Demostración. Las aplicaciones

$$\begin{array}{ccc}
\mathrm{Hom}_{k-alg}(A,k) & \longleftrightarrow & \mathrm{Spec}_{rac} A \\
\phi & \longmapsto & \mathrm{Ker}\,\phi \\
y & \longmapsto & \mathfrak{m}_y
\end{array}$$

son inversas entre sí. □

8. Ejemplo: $\mathrm{Spec}_{rac}\, k[x_1,\ldots,x_n] = \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n],k) = k^n$. Explícitamente, a cada $(\alpha_1,\ldots,\alpha_n) \in k^n$ le corresponde el ideal racional $(x_1-\alpha_1,\ldots,x_n-\alpha_n)$ de $k[x_1,\ldots,x_n]$ y el morfismo de k-álgebras $k[x_1,\ldots,x_n] \to k$, $p(x_1,\ldots,x_n) \mapsto p(\alpha_1,\ldots,\alpha_n)$.

9. Proposición: *Tenemos las igualdades*

$$\mathrm{Spec}_{rac}\, k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) = \left\{\alpha \in k^n : \begin{array}{c} p_1(\alpha)=0 \\ \cdots \\ p_r(\alpha)=0 \end{array}\right\} = \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),k)$$

$$(\overline{x_1-\alpha_1},\ldots,\overline{x_n-\alpha_n}) \longleftarrow (\alpha_1,\ldots,\alpha_n) \longmapsto \phi_\alpha \qquad (\phi_\alpha(\overline{p(x)}) := p(\alpha)).$$

Demostración. Las aplicaciones definidas son biyectivas como consecuencia de las proposiciones 2.2.7 y 2.2.3

□

10. Cada morfismo de k-álgebras $f: A \to B$ induce la aplicación

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

Tenemos el diagrama conmutativo,

$$\begin{array}{ccc} \operatorname{Spec}_{rac} B & \xrightarrow{f^*} & \operatorname{Spec}_{rac} A \\ \| & & \| \\ \operatorname{Hom}_{k-alg}(B,k) & \xrightarrow{f^*} & \operatorname{Hom}_{k-alg}(A,k) \end{array} \qquad \begin{array}{ccc} \operatorname{Ker} g & \longmapsto & f^{-1}(\operatorname{Ker} g) = \operatorname{Ker}(g \circ f) \\ \uparrow & & \uparrow \\ g & \longmapsto & f^*(g) := g \circ f \end{array}$$

11. Será usual que el ideal racional $(\overline{x_1 - \alpha_1}, \ldots, \overline{x_n - \alpha_n})$ de $k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ (con $p_1(\alpha_1,\ldots,\alpha_n) = \cdots = p_r(\alpha_1,\ldots,\alpha_n) = 0$) lo denotemos $\mathfrak{m}_\alpha$ (con $\alpha = (\alpha_1,\ldots,\alpha_n)$), y cuando lo pensemos como elemento del conjunto $\operatorname{Spec}_{rac} k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ lo denotaremos por α.

Sea $f: k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) \to k[y_1,\ldots,y_m]/(q_1,\ldots,q_s)$ un morfismo de k-álgebras, entonces $f(\bar{x}_i) = \overline{f_i(y_1,\ldots,y_m)}$, para ciertos polinomios $f_i(y_1,\ldots,y_n)$. Sea

$$\beta: k[y_1,\ldots,y_m]/(q_1,\ldots,q_s) \to k,\ \overline{p(y)} \mapsto p(\beta)$$

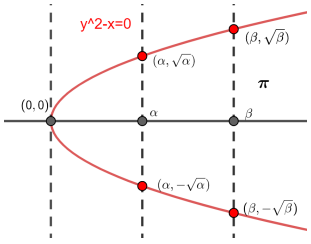
un morfismo de k-álgebras. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) & \xrightarrow{f} & k[y_1,\ldots,y_m]/(q_1,\ldots,q_s) \\ & \searrow^{f^*(\beta)} & \downarrow \beta \\ & & k \end{array} \qquad \begin{array}{ccc} \overline{p(x_1,\ldots,x_n)} & \longmapsto & \overline{p(f_1(y),\ldots,f_m(y))} \\ & \searrow & \downarrow \\ & & p(f_1(\beta),\ldots,f_m(\beta)) \end{array}$$

Luego el diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec}_{rac} k[y_1,\ldots,y_m]/(q_1,\ldots,q_s) & \xrightarrow{f^*} & \operatorname{Spec}_{rac} k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) \\ \| & & \| \\ \left\{ \text{Sol.} \begin{array}{c} q_1(y_1,\ldots,y_m) = 0 \\ \cdots \\ q_s(y_1,\ldots,y_m) = 0 \end{array} \right\} & \longrightarrow & \left\{ \text{Sol.} \begin{array}{c} p_1(x_1,\ldots,x_n) = 0 \\ \cdots \\ p_r(x_1,\ldots,x_n) = 0 \end{array} \right\} \end{array}$$

$$(\beta_1,\ldots,\beta_m) \longmapsto (f_1(\beta_1,\ldots,\beta_m),\ldots,f_n(\beta_1,\ldots,\beta_m))$$



12. Ejemplo: Consideremos el morfismo de $\mathbb{R}$-álgebras

$$\mathbb{R}[x] \hookrightarrow \mathbb{R}[x,y]/(y^2-x),\ p(x) \mapsto \overline{p(x)}.$$

Entonces, $\mathrm{Spec}_{rac}\,\mathbb{R}[x,y]/(y^2-x) \xrightarrow{\pi} \mathrm{Spec}_{rac}\,\mathbb{R}[x]$, $(\alpha,\beta) \overset{\pi}{\mapsto} \alpha$ es el morfismo inducido entre los espectros racionales.

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

Dado un ideal maximal $\mathfrak{m} \subset C(X)$, si $\mathfrak{m} \neq \mathfrak{m}_p$ para todo $p \in X$, entonces para cada $p \in X$ existe una función $f_p \in \mathfrak{m}$ que no se anula en p, luego tampoco en un entorno U_p de p. Como X es compacto, un número finito $U_{p_1},\ldots,U_{p_n}$ 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.

14. Si A es una k-álgebra, entonces $A = \mathrm{Hom}_{k-alg}(k[x],A)$ y cada $a \in A$ induce una aplicación (que seguimos denotando por a) en los espectros racionales

$$\mathrm{Spec}_{rac}\,A \xrightarrow{a} \mathrm{Spec}_{rac}\,k[x] = k,\ y \mapsto a(y) := \bar{a} \in A/\mathfrak{m}_y.$$

Si $A = k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ y $\mathfrak{m} = \mathfrak{m}_\alpha$ (con $\alpha \in k^n$ tal que $p_1(\alpha) = \cdots = p_r(\alpha) = 0$), entonces $\overline{p(x)} = p(\alpha) \in (k[x_1,\ldots,x_n]/(p_1,\ldots,p_r))/\mathfrak{m}_\alpha = k$ y tenemos la aplicación

$$\begin{array}{ccc} \mathrm{Spec}_{rac}\,k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) & \xrightarrow{\overline{p(x_1,\ldots,x_n)}} & k \\ \alpha & \longmapsto & p(\alpha). \end{array}$$

En el ejemplo anterior, dada $f \in C(X)$, el diagrama

$$\begin{array}{ccc} X & \xrightarrow{=\!=} & \mathrm{Spec}_{rac}\,C(X) \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f} & \\ & k & \end{array}$$

es conmutativo.

15. Proposición: *Sean A y B dos k-álgebras, entonces*

$$\mathrm{Spec}_{rac}(A \times_k B) = \mathrm{Spec}_{rac} A \coprod \mathrm{Spec}_{rac} B.$$

Demostración. Dado un morfismo de anillos $f: A \times B \to k$ tenemos que $0 = f(0,0) = f((1,0)\cdot(0,1)) = f(1,0)\cdot f(0,1)$, entonces $f(1,0) = 0$ o $f(0,1) = 0$. En el primer caso f se anula sobre $A \times 0$, es decir, factoriza vía el cociente $(A \times B)/(A \times 0) = B$, en el segundo caso f se anula en $0 \times B$, es decir, factoriza vía el cociente $(A \times B)/(0 \times B) = A$. Luego

$$\begin{aligned}\mathrm{Spec}_{rac}(A \times_k B) &= \mathrm{Hom}_{k-alg}(A \times_k B, k) = \mathrm{Hom}_{k-alg}(A,k) \coprod \mathrm{Hom}_{k-alg}(B,k) \\ &= \mathrm{Spec}_{rac} A \coprod \mathrm{Spec}_{rac} B.\end{aligned}$$

□

16. Ejercicio: Dado $(a,b) \in A \times B$, prueba que

$$\begin{aligned}(a,b)(\alpha) &= a(\alpha), \ \ \forall \alpha \in \mathrm{Spec}_{rac} A \subset \mathrm{Spec}_{rac}(A \times B). \\ (a,b)(\beta) &= b(\beta), \ \ \forall \beta \in \mathrm{Spec}_{rac} B \subset \mathrm{Spec}_{rac}(A \times B).\end{aligned}$$

17. Proposición: *Sean A y B dos k-álgebras, entonces*

$$\mathrm{Spec}_{rac}(A \otimes_k B) = \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B.$$

Demostración. En efecto,

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

□

18. Ejercicio: Dado $a \otimes b \in A \otimes_k B$, prueba que

$$(a \otimes b)(\alpha,\beta) = a(\alpha)\cdot b(\beta), \ \ \forall (\alpha,\beta) \in \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B = \mathrm{Spec}_{rac}(A \otimes_k B).$$

19. El morfismo de k-álgebras $i: A \to A \otimes_k B$, $i(a) := a \otimes 1$, induce en los espectros racionales la aplicación

$$\mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B = \mathrm{Spec}_{rac}(A \otimes B) \to \mathrm{Spec}_{rac} A, \ (\alpha,\beta) \mapsto \alpha.$$

En efecto, $(\phi_1,\phi_2) \in \mathrm{Hom}_{k-alg}(A,k) \times \mathrm{Hom}_{k-alg}(B,k)$ se corresponde con el morfismo de k-álgebras $\phi: A \otimes_k B \to k$, $\phi(a \otimes b) = \phi_1(a)\cdot\phi_2(b)$ y la composición $A \xrightarrow{i} A \otimes_k B \xrightarrow{\phi} k$, es la asignación $a \mapsto a \otimes 1 \mapsto \phi_1(a)\cdot\phi_2(1) = \phi_1(a)$, es decir, es el morphismo ϕ_1. Es decir, i induce la aplicación

$$\begin{array}{rcccc} \mathrm{Hom}_{k-alg}(A,k) \times \mathrm{Hom}_{k-alg}(B,k) & = & \mathrm{Hom}_{k-alg}(A \otimes_k B, k) & \xrightarrow{i^*} & \mathrm{Hom}_{k-alg}(A,k) \\ (\phi_1,\phi_2) & = & \phi & \mapsto & \phi_1 \end{array}$$

20. Dados dos morfismos de k-álgebras $f_1\colon A_1 \to B$ y $f_2\colon A_2 \to B$, el morfismo de k-álgebras $f_1 \otimes f_2\colon A_1 \otimes_k A_2 \to B$, $(f_1 \otimes f_2)(a_1 \otimes a_2) := f_1(a_1)\cdot f_2(a_2)$, induce en los espectros racionales la aplicación

$$\mathrm{Spec}_{rac} B \longrightarrow \mathrm{Spec}_{rac}(A_1 \otimes_k A_2) = \mathrm{Spec}_{rac} A_1 \times \mathrm{Spec}_{rac} A_2,\ \ \alpha \overset{(f_1\otimes f_2)^*}{\longmapsto} (f_1^*(\alpha), f_2^*(\alpha)).$$

En efecto, sean $i_1\colon A_1 \to A_1 \otimes_k A_2$, $i_1(a) = a \otimes 1$ y $i_2\colon A_2 \to A_1 \otimes_k A_2$, $i_2(a) = 1 \otimes a$. Observemos que $(f_1 \otimes f_2)\circ i_1 = f_1$ y $(f_1 \otimes f_2)\circ i_2 = f_2$. Si denotamos $(f_1 \otimes f_2)^*(\alpha) = (\beta_1, \beta_2)$, entonces

$$f_1^*(\alpha) = i_1^*((f_1 \otimes f_2)^*(\alpha)) = i_1^*(\beta_1, \beta_2) = \beta_1 \ \text{ y } \ f_2^*(\alpha) = i_2^*((f_1 \otimes f_2)^*(\alpha)) = i_2^*(\beta_1, \beta_2) = \beta_2.$$

21. Dotemos a $\mathrm{Spec}_{rac} A$ de una topología. Dado un ideal $I \subseteq A$ denotaremos $(I)_0^{rac} :=$ {Ideales racionales $\mathfrak{m} \subset A : I \subseteq \mathfrak{m}$} $= \{x \in \mathrm{Spec}_{rac} A : a(x) = 0, \forall a \in I\}$ y diremos que es un cerrado de $\mathrm{Spec}_{rac} A$. Observemos que

1. $\emptyset = (A)_0^{rac}$ y $\mathrm{Spec}_{rac} A = (0)_0^{rac}$.
2. $(\sum_i I_i)_0^{rac} = \cap_i (I_i)_0^{rac}$.
3. $(I_1 \cap I_2)_0^{rac} = (I_1)_0^{rac} \cup (I_2)_0^{rac}$: obviamente $(I_1)_0^{rac} \cup (I_2)_0^{rac} \subseteq (I_1 \cap I_2)_0^{rac}$; por último, si $x \notin (I_1)_0^{rac} \cup (I_2)_0^{rac}$, existen $a_1 \in I_1$ y $a_2 \in I_2$ tales que $a_1(x) \neq 0 \neq a_2(x)$, luego $(a_1 \cdot a_2)(x) \neq 0$ y $x \notin (I_1 \cap I_2)_0^{rac}$.

2.3. Espectro primo de un anillo

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

2. Ejemplos: $\mathrm{Spec}\,\mathbb{R} = \{(0)\}$, $\mathrm{Spec}\,\mathbb{Z} = \{(0), (p)$, para todo número primo $p\}$, $\mathrm{Spec}\,k[x] = \{(0), (p(x)$ para todo polinomio mónico irreducible $p(x)\}$.

3. Notaciones: Un ideal primo $\mathfrak{p}_z \subset A$ lo denotaremos por z cuando lo consideremos como elemento de $\mathrm{Spec} A$.

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 $a(x) := \bar{a} \in A/\mathfrak{p}_x$).

4. Ejercicio: Prueba que una función $f \in A$ es invertible si y sólo si no se anula en ningún punto de $\mathrm{Spec} A$. Prueba que $p(x,y) \in k[x,y]$ se anula en el ideal primo racional $\mathfrak{m}_{\alpha,\beta} = (x-\alpha, y-\beta) \subset k[x,y]$ si y sólo si $p(\alpha,\beta) = 0$.

Como $\mathfrak{p}_z$ es un ideal primo se cumple:

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

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

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

6. Proposición: *Se cumplen las siguientes igualdades:*

1. $(0)_0 = \operatorname{Spec} A$ *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 quizás 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 $(I_1 \cap I_2)_0 \subseteq (I_1)_0 \cup (I_2)_0$.

□

7. Ejercicio: Demuestra que $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0$, donde denotamos por $I_1 \cdot I_2 = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I_1, b_i \in I_2, n \in \mathbb{N}\}$.

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

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

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

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

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

10. Proposición: *Dado $x \in \operatorname{Spec}A$ su cierre es $\bar{x} = (\mathfrak{p}_x)_0$. 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.*

Demostración. El cierre de x, $\bar{x}$, será de la forma $\bar{x} = (I)_0$, para cierto ideal $I \subset A$. Obviamente, como $x \in \bar{x}$, tenemos que $I \subseteq \mathfrak{p}_x$. Por tanto, $(\mathfrak{p}_x)_0 \subseteq (I)_0$. Ahora bien, $(I)_0$ es el menor cerrado que contiene a x y $x \in (\mathfrak{p}_x)_0$, luego $(\mathfrak{p}_x)_0 = (I)_0 = \bar{x}$.

□

11. 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 $\operatorname{Spec}k[x]$ es la recta afín sobre k.

Dado un ideal $((x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}) \subset \mathbb{C}[x]$, entonces $((x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}))_0 = \{\alpha_1, \ldots, \alpha_r\}$.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).

12. 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 maxima-

les 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. Cada punto $x \in X$ es subespacio irreducible, luego su cierre $\bar{x}$ es un cerrado irreducible de X. Como consecuencia del lema de Zorn, todo irreducible está incluido en alguna componente irreducible. X es unión de sus componentes irreducibles.

13. Proposición : *Cada cerrado irreducible del espectro de un anillo es el cierre de un único punto, llamado punto genérico de tal cerrado. En particular, las componentes irreducibles de* $\operatorname{Spec} A$ *son los cierres de los puntos 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 bien f se anula en C, o bien g, porque C es irreducible. Es decir, o bien $f \in I$, o bien $g \in I$.

$C = \bar{x}$ es una componente irreducible si y sólo si no está incluido estrictamente en otro cerrado irreducible $C' = \bar{y}$, es decir, si y sólo si $\mathfrak{p}_y \not\subseteq \mathfrak{p}_x$, es decir, si y sólo si $\mathfrak{p}_x$ es un ideal primo minimal.

□

14. 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.

□

15. Denotemos por $\mathrm{Spec}_{max}\,A$ el conjunto de todos los puntos cerrados de $\mathrm{Spec}\,A$, es decir, el conjunto de todos los ideales primos maximales de A. Consideremos $\mathrm{Spec}_{max}\,A$ como subespacio de $\mathrm{Spec}\,A$ y denotemos $(I)_0^{max} = (I)_0 \cap \mathrm{Spec}_{max}\,A$. Como consecuencia de la proposición 2.3.6, cortando con $\mathrm{Spec}_{max}\,A$, tenemos que

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

16. Teorema: *$\mathrm{Spec}_{max}\,A$ es un espacio topológico compacto.*

Demostración. Cópiese la demostración de 2.3.14

□

2.3.1. Espectro primo de un anillo noetheriano

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

18. 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.*

Demostración. Probemos solo 3. Sea X el espacio topológico noetheriano. Supongamos que X no es unión de un número finito de cerrados irreducibles. En particular, X no es irreducible, luego es unión de dos cerrados propios, $X = C_1 \cup C_2$. C_1 y C_2 no pueden ser los dos a la vez unión de un número finito de cerrados irreducibles. Digamos que C_1 no es unión de un número finito de cerrados irreducibles. En particular, C_1 no es un cerrado irreducible, luego es unión de dos cerrados propios $C_1 = C_{11} \cup C_{12}$. C_{11} y C_{12} no pueden ser los dos a la vez unión de un número finito de cerrados irreducibles. Digamos que C_{11} no es unión de un número finito de cerrados irreducibles. En particular, C_{11} no es un cerrado irreducible, luego es unión de dos cerrados propios $C_{11} = C_{111} \cup C_{112}$. Así sucesivamente, vamos construyendo la cadena descendente de inclusiones estrictas

$$C_1 \supset C_{11} \supset C_{111} \supset \cdots$$

lo que contradice la noetherianidad de X. En conclusión, X es unión de un número finito de cerrados irreducibles.

□

19. Proposición: *Si A es un anillo noetheriano, entonces* Spec$A$ *es un espacio topológico noetheriano. En particular,* Spec$A$ *es unión de un número finito de componentes irreducibles y el número de ideales primos minimales de A es finito*

Demostración. Sea $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_n \supseteq \cdots$ una cadena descendente de cerrados. Sean I_i los ideales de funciones que se anulan en C_i. Luego $(I_i)_0 = C_i$ y tenemos la cadena

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

Cadena que estabiliza por ser A noetheriano. Es decir, existe $m \in \mathbb{N}$ de modo que $I_m = I_{m+1} = \cdots$. Luego, $C_m = C_{m+1} = \cdots$.

□

Sea A un anillo noetheriano, $I \subset A$ un ideal y $\mathfrak{p}_{x_1}, \ldots, \mathfrak{p}_{x_n}$ los ideales primos mínimos conteniendo a I (que se corresponden con los ideales primos minimales de A/I), entonces

$$(I)_0 = (p_{x_1})_0 \cup \ldots \cup (p_{x_n})_0 = \bar{x}_1 \cup \ldots \cup \bar{x}_n.$$

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

20. Teorema: *Consideremos un sistema de ecuaciones k-algebraicas*

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

y sea k' una k-extensión de cuerpos algebraicamente cerrada y de grado de trascendencia mayor o igual que n. Dadas $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in k'^n$, diremos que $\alpha \sim \beta$ si existe $\tau \in Aut_{k-alg} k'$, tal que

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

Se cumple que

$$\begin{array}{rcl} \{\alpha \in k'^n : p_1(\alpha) = \cdots = p_r(\alpha) = 0\} \Big/ \sim & \longrightarrow & \text{Spec}\, k[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \\ [\alpha] & \longmapsto & \mathfrak{p}_\alpha := \{\bar{p} \in k[x_1, \ldots, x_n]/(p_1, \ldots, p_r) : p(\alpha) = 0\} \end{array}$$

Demostración. 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 $i\colon k(y) \hookrightarrow k'$ porque el cierre algebraico de $k(y)$ es igual al cierre algebraico de un cuerpo de funciones racionales en s variables, con $s = \operatorname{gr}\operatorname{tr}_k k(y) \leq n$ y k' es igual al cierre algebraico de un cuerpo de funciones racionales en $m \geq n$ variables.

Veamos que dado otro morfismo $j\colon k(y) \to k'$ entonces existe $\tau \in Aut_{k-alg}k'$ tal que $i = \tau \circ j$. Pensemos i como una inclusión y sea $z_1,\ldots,z_s \in k'$ una base de k-trascendencia de $k(y)$. Componiendo j con un automorfismo τ' de k' podemos suponer que $z'_l := j(z_l)$ es igual a z_l, para todo $1 \leq l \leq s$. En efecto, sean $z_{s+1},\ldots,z_m \in k'$ y $z'_{s+1},\ldots,z'_m \in k'$ de modo que $z_1,\ldots,z_m$ y $z'_1,\ldots,z'_m$ sean bases de k-trascendencia de k'. Sea ahora $\sigma\colon k(z'_1,\ldots,z'_m) \to k(z_1,\ldots,z_m)$ el morfismo definido por $\sigma(z'_l) = z_l$, para todo l. Por toma de cierres algebraicos, el morfismo σ extiende al automorfismo $\tau'\colon k' \to k'$ buscado. Sea $h\colon k(y)(z_{s+1},\ldots,z_m) \to k'$ el morfismo definido por $h = j$ sobre $k(y)$ y $h(z_t) = z_t$, para todo $0 < t \leq m - s$. Hemos obtenido el cierre algebraico de $k(y)(z_{s+1},\ldots,z_m)$ vía la inclusión natural en k' y vía h. Por tanto existe un morfismo $\tau\colon k' \to k'$ tal que $\tau \circ h$ es la inclusión natural. En particular, $\tau \circ j$ es el morfismo de inclusión natural i de $k(y)$ en k'.

Denotemos por $\pi\colon A \to k(y)$ el morfismo natural, y sea $f = i \circ \pi\colon A \to k'$. A $\mathfrak{p}_y$ le asignamos $[(f(\bar{x}_1),\ldots,f(\bar{x}_m))]$.

Ambas asignaciones son inversas entre sí.

□

2.4. Aplicación inducida en espectros por un morfismo de anillos

Sea $j\colon A \to B$ un morfismo de anillos. Si J es un ideal de B, entonces $j^{-1}(J) := \{a \in A\colon j(a) \in J\}$ 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

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

1. 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

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

y concluimos que j^* es continua.

□

2.4.1. Espectro de un cociente

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

$$A \xrightarrow{\pi} A/I, \qquad a \overset{\pi}{\longmapsto} \bar{a}$$

$$\operatorname{Spec} A \xleftarrow[\pi^*]{} \operatorname{Spec} A/I$$

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

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

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

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

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

que es justamente el morfismo

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

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.

□

3. 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.

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

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

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

2.4.2. Espectro de una localización

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 $(j(I)) = j(I) \cdot B = I \cdot B$.

5. 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. Las asignaciones

$$\operatorname{Spec} A_S = \{\text{Ideales primos de } A \text{ que no cortan a } S\} \subseteq \operatorname{Spec} A$$
$$\mathfrak{p}' \longmapsto \mathfrak{p}' \cap A \quad (j^*)$$
$$\mathfrak{p} \cdot A_S \longmapsfrom \mathfrak{p}$$

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

6. Ejercicio: Prueba que $\operatorname{Spec} A_{SS'} = \operatorname{Spec} A_S \cap \operatorname{Spec} A_{S'}$.

7. Proposición: *Sean $S, S' \subset A$ dos sistemas multiplicativos. Entonces,* $\operatorname{Spec} A_S = \operatorname{Spec} A_{S'}$ *si y solo si* $A_S = A_{SS'} = A_{S'}$.

Demostración. $\Rightarrow$) Los elementos de S' son invertible en $A_{S'}$, es decir, no se anulan en ningún punto de $\operatorname{Spec} A_{S'}$, luego no se anulan en ningún punto de $\operatorname{Spec} A_S$, es decir, son invertibles en A_S, luego $A_S = (A_S)_{S'} = A_{SS'}$. Igualmente, $A_{S'} = A_{SS'}$.

$\Leftarrow$) Los elementos de S' son invertibles en $A_{S'}$, luego son invertibles en A_S, luego no se anulan en ningún punto de $\operatorname{Spec} A_S$, luego $\operatorname{Spec} A_S \subseteq \operatorname{Spec} A_{S'}$. Igualmente, $\operatorname{Spec} A_{S'} \subseteq \operatorname{Spec} A_S$.

□

8. Notaciones: 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 $\operatorname{Spec} A$.

9. Corolario: *El espectro de A_f es homeomorfo 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 el conjunto de 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 el conjunto de los ideales primos $\mathfrak{p}_x$ de A que no contienen a f, es decir, U_f. □

10. Notación: Dado un abierto $U \subseteq \operatorname{Spec} A$, denotaremos $A_U := A_S$, donde $S := \{a \in A : a(x) \neq 0, \forall x \in U\}$.

11. Corolario: *Se cumple que* $A_f = A_{U_f}$.

Demostración. Sea $S = \{a \in A : a(x) \neq 0 \ \forall x \in U_f\}$. Evidentemente, $f \in S$ y toda $s \in S$ es invertible en A_f (porque no se anulan en ningún punto de $\operatorname{Spec} A_f = U_f$). Luego, $A_f = (A_f)_S = A_S =: A_{U_f}$. □

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

13. Lema: *Dados dos cerrados disjuntos* $C_1, C_2 \subset \operatorname{Spec} A$*, existe* $f \in A$ *que se anula en todos los puntos de* C_1 *y no se anula en ningún punto de* C_2*.*

Demostración. Sea I_i el ideal de todas las funciones que se anulan en todos los puntos de C_i, para $i = 1, 2$. Entonces, $\emptyset = C_1 \cap C_2 = (I_1)_0 \cap (I_2)_0 = (I_1 + I_2)_0$. Por lo tanto, $I_1 + I_2 = A$ y existen $f_1 \in I_1$ y $f_2 \in I_2$ tales que $f_1 + f_2 = 1$. Observemos que f_1 no se nula en ningún punto de C_2, porque f_2 se anula en todos los puntos de C_2; además f_1 se anula en todos los puntos de C_1.

□

14. Proposición: *Si* $\operatorname{Spec} A = U \coprod V$*, donde* U *y* V *son abiertos de* $\operatorname{Spec} A$*, entonces el morfismo*

$$A \to A_U \times A_V,\ a \mapsto (\frac{a}{1}, \frac{a}{1})$$

es un isomorfismo de anillos.

En particular, un anillo no nulo A *es producto directo de dos anillos (no nulos) si y solo si* $\operatorname{Spec} A$ *no es conexo.*

Demostración. $U = \operatorname{Spec} A_U$: Evidentemente $U \subseteq \operatorname{Spec} A_U$, porque estamos localizando por funciones que no se anulan en ningún punto de U. Existe f que se anula en todos los puntos de V y en ningún punto de U. Por tanto, si $x \in V$ entonces $x \notin \operatorname{Spec} A_U$ y $U = \operatorname{Spec} A_U$.

Si $x \in U$, entonces como $\operatorname{Spec} A_x$ es conexo (pues todo cerrado contiene al único punto cerrado, x) entonces $U \cap \operatorname{Spec} A_x = \operatorname{Spec} A_x$ y $V \cap \operatorname{Spec} A_x = \emptyset$. Por tanto, $(A_U)_x = A_x$ (porque $\operatorname{Spec}(A_U)_x = \operatorname{Spec} A_U \cap \operatorname{Spec} A_x = \operatorname{Spec} A_x$) y $(A_V)_x = 0$ (porque $\operatorname{Spec}(A_V)_x = \operatorname{Spec} A_V \cap \operatorname{Spec} A_x = V \cap \operatorname{Spec} A_x = \emptyset$). En consecuencia, para todo $x \in U$, tenemos que $A_x = (A_U \times A_V)_x$. Igualmente, para todo $x \in V$, $A_x = (A_U \times A_V)_x$. Luego, el morfismo $A \to A_U \times A_V$ es isomorfismo.

Por último, si $A = A_1 \times A_2$, entonces $(1,0)\cdot(0,1) = (0,0)$ y $(1,0)+(0,1) = (1,1)$. Por tanto, $\operatorname{Spec} A = ((1,0))_0 \coprod ((0,1))_0$, luego no es conexo.

□

15. Proposición: *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 $\mathfrak{p}_x$. □

16. 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".

17. 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 por la fórmula del binomio de Newton $(a+b)^{n+m} = 0$. Ahora es fácil demostrar que el radical de un anillo es un ideal.

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

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

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

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

Sea ahora $f \in \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$. Por el corolario 2.4.9, $\operatorname{Spec} A_f = \emptyset$. 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 $\operatorname{Spec} A = \operatorname{Spec}(A/\operatorname{rad} A)$.

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

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

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

21. Proposición: *Se cumple que* $r(I) = \bigcap_{x \in (I)_0} \mathfrak{p}_x$.

Demostración. $a \in r(I) \iff$ existe $n \in \mathbb{N}$ tal que $a^n \in I \iff$ existe $n \in \mathbb{N}$ tal que $\bar{a}^n = 0 \in A/I \iff \bar{a} \in \bigcap_{y \in \operatorname{Spec} A/I} \mathfrak{p}_y \iff a \in \bigcap_{x \in (I)_0} \mathfrak{p}_x$.

□

22. Corolario: *Sean* $I, J \subset A$ *dos ideales. Entonces,*

$$(I)_0 = (J)_0 \iff r(I) = r(J).$$

Demostración. $\Rightarrow$) $r(I) = \bigcap_{x \in (I)_0} \mathfrak{p}_x = \bigcap_{x \in (J)_0} \mathfrak{p}_x = r(J)$.

$\Leftarrow$) $(I)_0 = (r(I))_0 = (r(J))_0 = (J)_0$.

□

Se dice que un ideal $I \subset A$ es radical si $r(I) = I$. Por el corolario anterior, tenemos la biyección

$$\begin{array}{ccc} \{\text{Cerrados de } \operatorname{Spec} A\} & = & \{\text{Ideales radicales de } C\} \\ C & \longmapsto & I_C = \bigcap_{x \in C} \mathfrak{p}_x \\ (I)_0 & \longmapsto & I \end{array}$$

23. Proposición: *Sea* A *un anillo noetheriano e* $I \subsetneq A$ *un ideal radical. Sean* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *los ideales primos mínimos conteniendo a* I *(que se corresponden con los ideales primos mínimales 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.

□

2.4.3. Fórmula de la fibra

24. Proposición: *Sea $I \subset A$ un ideal y $S \subset A$ un sistema multiplicativo. Entonces,*

$$\operatorname{Spec}(A/I)_S = \{x \in \operatorname{Spec} A : I \subseteq \mathfrak{p}_x \text{ y } \mathfrak{p}_x \cap S = \emptyset\}.$$

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

$$\begin{aligned}\operatorname{Spec}(A/I)_S &= \{x' \in \operatorname{Spec} A/I : \mathfrak{p}_{x'} \cap \bar{S} = \emptyset\} = \{x' \in \operatorname{Spec} A/I : \pi^{-1}(\mathfrak{p}_{x'}) \cap S = \emptyset\} \\ &= \{x \in \operatorname{Spec} A : I \subseteq \mathfrak{p}_x \text{ y } \mathfrak{p}_x \cap S = \emptyset\}.\end{aligned}$$

□

Observemos que $(A/I)_S = A \otimes_A A/I \otimes_A A_S = A \otimes_A A_S \otimes_A A/I = A_S/I \cdot A_S$.

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

25. Fórmula de la fibra : *Sea $j : A \to B$ un morfismo de anillos y consideremos el morfismo inducido $j^* : \operatorname{Spec} B \to \operatorname{Spec} A$. Para todo punto $x \in \operatorname{Spec} A$ se cumple que*

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

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.

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

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 $\operatorname{Spec} C = \emptyset$.

26. Ejemplo: Calculemos $\operatorname{Spec}\mathbb{C}[x,y]$ usando la fórmula de la fibra. Consideremos el morfismo $i\colon \mathbb{C}[x] \to \mathbb{C}[x,y], p(x) \mapsto p(x)$ y sea $i^*\colon \operatorname{Spec}\mathbb{C}[x,y] \to \operatorname{Spec}\mathbb{C}[x]$ el morfismo inducido en los espectros. Cada punto de $\operatorname{Spec}\mathbb{C}[x,y]$ está en la fibra de un único punto de $\operatorname{Spec}\mathbb{C}[x]$, así que vamos a calcular tales fibras.

Los ideales primos de $\mathbb{C}[x]$ son el ideal (0) y los ideales maximales $\mathfrak{m}_\alpha = (x-\alpha)$. Según la fórmula de la fibra

$$i^{*-1}(\alpha) = \operatorname{Spec}\mathbb{C}[x,y]/\mathfrak{m}_\alpha\mathbb{C}[x,y] = \operatorname{Spec}\mathbb{C}[x,y]/(x-\alpha).$$

Ahora bien, $\mathbb{C}[x,y]/(x-\alpha) \simeq \mathbb{C}[y]$, $x \mapsto \alpha, y \mapsto y$. Luego,

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

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

Solo nos falta calcular la fibra de $(0) = \mathfrak{p}_g$

$$i^{*-1}(g) = \operatorname{Spec}\mathbb{C}[x,y]_{\mathbb{C}[x]-\setminus(0)} = \operatorname{Spec}\mathbb{C}(x)[y]$$

Los ideales primos no nulos de $\mathbb{C}(x)[y]$ están generados por un polinomio irreducible con coeficientes en $\mathbb{C}(x)$ de grado mayor o igual que 1 en y. Por el lema de Gauss se corresponden con los polinomios $p(x,y) \in \mathbb{C}[x,y]$ irreducibles de grado mayor o igual que 1 en y. Por tanto, $i^{*-1}(g)$ está formado por los ideales primos $(p(x,y))$, (0) (donde $p(x,y)$ es un polinomio irreducible de grado mayor o igual que 1 en y)

En resumen, los puntos de $\operatorname{Spec}\mathbb{C}[x,y] \underset{\text{Not}}{=} \mathbb{A}_2(\mathbb{C})$ son

1. Los puntos cerrados (α,β), es decir, los ideales primos $(x-\alpha, y-\beta)$.
2. Los puntos genéricos de las "curvas" irreducibles $(p(x,y))_0$, es decir, los ideales primos $(p(x,y))$, $p(x,y)$ irreducible.
3. El punto genérico del plano afín $(0)_0 = \mathbb{A}_2(\mathbb{C})$, es decir, el ideal primo (0).

27. 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 $(\overline{x-\alpha}, \overline{y-\beta})$ 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 $(q_i(x,y))_0$, es decir, los ideales primos $(\overline{q_i(x,y)})$.

28. 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 $\overline{\operatorname{Im} f^*} = \operatorname{Spec} A$. □

29. Proposición : *Sea $f : A \to B$ un morfismo de anillos y $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación inducida en los espectros. Sea $J \subset B$ un ideal, entonces*

$$\overline{f^*((J)_0)} = (f^{-1}(J))_0.$$

Demostración. Consideremos los diagramas

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A/f^{-1}(J) & \longrightarrow & B/J \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ (f^{-1}(J))_0 = \operatorname{Spec} A/(J \cap A) & \xleftarrow[f^*_{|(J)_0}]{} & \operatorname{Spec} B/J = (J)_0 \end{array}$$

Como el morfismo $A/f^{-1}(J) \hookrightarrow B/J$ es inyectivo, entonces $\overline{f^*((J)_0)} = (f^{-1}(J))_0$.

□

2.5. Apéndice: Funtor de soluciones de un sistema de ecuaciones

2.5.1. Categorías

Dar una categoría $\mathscr{C}$ es dar

1. Una familia de objetos.

2. Unos conjuntos $\mathrm{Hom}_{\mathscr{C}}(M,N)$, para cada par de objetos M,N de $\mathscr{C}$. Cada elemento $f \in \mathrm{Hom}_{\mathscr{C}}(M,N)$ diremos que es un "morfismo de M en N" y lo denotaremos también $f: M \to N$.

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) $(f \circ g) \circ h = f \circ (g \circ h)$.

   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: La categoría $\mathscr{C}_{Conj}$ de conjuntos, es la categoría cuyos objetos son los conjuntos y los morfismos entre los objetos son las aplicaciones de conjuntos.

La categoría de espacios topológicos es la categoría cuyos objetos son los espacios topológicos y los morfismos entre los objetos son los homeomorfismos.

La categoría de las variedades diferenciales es la categoría cuyos objetos son las variedades diferenciales y los morfismos los morfismos de variedades diferenciales.

La categoría de grupos es la categoría cuyos objetos son los grupos y los morfismos los morfismos de grupos.

La categoría de los k-espacios vectoriales es la categoría cuyos objetos son los k-espacios vectoriales y los morfismos las aplicaciones k-lineales.

La categoría de A-módulos, es la categoría cuyos objetos son los A-módulos y los morfismos entre los objetos son los morfismos de módulos.

La categoría de los anillos es la categoría cuyos objetos son los anillos y los morfismos son los morfismos de anillos.

Categoría de las k-álgebras: Sea k un cuerpo. La categoría de k-álgebras $\mathscr{C}_{k-alg}$ es la categoría cuyos objetos son las k-álgebras y los morfismos los morfismos de k-álgebras.

2.5.2. Funtores representables

2. Definición: Sean $\mathscr{C}$ y $\mathscr{C}'$ dos categorías. Dar un funtor covariante $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$ es asignar a cada objeto M de $\mathscr{C}$ un objeto $F(M)$ de $\mathscr{C}'$, y cada morfismo $f: M \to N$ 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 $f : M \to N$ 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 $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

3. Ejemplo: Sea $\mathscr{C}_{k-vect.}$ la categoría de k-espacios vectoriales. Podemos definir el siguiente funtor contravariante

$$\begin{aligned} \mathscr{C}_{k-vect.} &\rightsquigarrow \mathscr{C}_{k-vect} \\ E &\rightsquigarrow E^* \\ f &\rightsquigarrow f^* \end{aligned}$$

4. Sea $\mathscr{C}$ una categoría y N un objeto de $\mathscr{C}$. Un morfismo $f : M \to M'$ induce la aplicación $f_* : \mathrm{Hom}_{\mathscr{C}}(N,M) \to \mathrm{Hom}_{\mathscr{C}}(N,M')$, $g \mapsto f_*(g) := f \circ g$. Sea $\mathrm{Hom}_{\mathscr{C}}(N,-)\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{Conj}$ el funtor covariante de $\mathscr{C}$ en la categoría de los conjuntos definido por:

$$\begin{aligned} \mathrm{Hom}_{\mathscr{C}}(N,-)\colon \mathscr{C} &\rightsquigarrow \mathscr{C}_{Conj} \\ M &\rightsquigarrow \mathrm{Hom}_{\mathscr{C}}(N,M) \\ f &\rightsquigarrow f_* \\ (f \circ g) &\rightsquigarrow (f \circ g)_* = f_* \circ g_* \end{aligned}$$

5. Sea $\mathscr{C}$ una categoría y N un objeto de $\mathscr{C}$. Un morfismo $f : M \to M'$ induce la aplicación $\mathrm{Hom}_{\mathscr{C}}(M',N) \xrightarrow{f^*} \mathrm{Hom}_{\mathscr{C}}(M,N)$, $g \mapsto f^*(g) := g \circ f$. Sea $\mathrm{Hom}_{\mathscr{C}}(-,N)\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{Conj}$ el funtor contravariante definido por:

$$\begin{aligned} \mathrm{Hom}_{\mathscr{C}}(-,N)\colon \mathscr{C} &\rightsquigarrow \mathscr{C}_{Conj} \\ M &\rightsquigarrow \mathrm{Hom}_{\mathscr{C}}(M,N) \\ f &\rightsquigarrow f^* \\ (f \circ g) &\rightsquigarrow (f \circ g)^* = g^* \circ f^* \end{aligned}$$

6. Definición: Sean $F, F'\colon \mathscr{C} \rightsquigarrow \mathscr{C}'$ dos funtores covariantes (o contravariantes). Dar un morfismo $\theta\colon F \to F'$, es dar para cada objeto M de la categoría $\mathscr{C}$ un morfismo $\theta_M\colon F(M) \to F'(M)$, de modo que para cada morfismo $f : M \to N$ 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'. Dado un objeto M, denotemos $M^{\cdot} = \mathrm{Hom}_{\mathscr{C}}(M,-)$.

7. Teorema: *Sea $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{Conj}$ un funtor covariante y $M,N \in \mathscr{C}$. Se cumple que*

1. $\mathrm{Hom}(M^{\cdot},F) = F(M)$.
2. $\mathrm{Hom}(M^{\cdot},M'^{\cdot}) = \mathrm{Hom}_{\mathscr{C}}(M',M)$, $f^* \longleftarrow\!\shortmid f$.
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 $\theta_M(\mathrm{Id}_M) = x \in F(M)$: No es más que considerar, dado $f \in \mathrm{Hom}_{\mathscr{C}}(M,N)$, el diagrama conmutativo

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

2. Es consecuencia inmediata de 1.
3. Es consecuencia inmediata de 2.

□

Dado un objeto M, denotemos ${}^{\cdot}M = \mathrm{Hom}_{\mathscr{C}}(-,M)$. La proposición dual de la anterior es la siguiente.

8. Teorema: *Sea $F\colon \mathscr{C} \rightsquigarrow \mathscr{C}_{Conj}$ un funtor contravariante y $M,N \in \mathscr{C}$. Se cumple que*

1. $\mathrm{Hom}({}^{\cdot}M,F) = F(M)$.
2. $\mathrm{Hom}({}^{\cdot}M, {}^{\cdot}N) = \mathrm{Hom}_{\mathscr{C}}(M,N)$, $f_* \longleftarrow\!\shortmid f$.
3. ${}^{\cdot}M \simeq {}^{\cdot}N$ *si y sólo si* $M \simeq N$.

9. Definición: Si $F \simeq \mathrm{Hom}_{\mathscr{C}}(-,M)$ (resp. $F \simeq \mathrm{Hom}_{\mathscr{C}}(M,-)$) entonces se dice que F es un funtor contravariante (resp. covariante) representable y que M es el representante de F (el cual es único salvo isomorfismos, por 2.5.8 3.).

10. Ejemplo: En Matemáticas, cuando queremos expresar cuál es la propiedad universal de un objeto M (construido de cierto modo), lo que pretendemos es determinar $\mathrm{Hom}_{\mathscr{C}}(M,-)$ (ó $\mathrm{Hom}_{\mathscr{C}}(-,M)$). Pongamos un ejemplo:

Propiedad universal de la topología final de una aplicación: Sea X un espacio topológico, Y un conjunto e $f: X \to Y$ una aplicación de conjuntos. Existe una topología en Y de modo que

$$\mathrm{Hom}_{cont}(Y,Z) = \{g \in \mathrm{Aplic}(Y,Z):\ g \circ f \in \mathrm{Hom}_{cont}(X,Z)\} \qquad (*)$$

para todo espacio topológico Z. En efecto, como puede comprobarse, es la topología de Y, cuyos abiertos son los subconjuntos $U \subset Y$ tales que $f^{-1}(U)$ es un abierto de X. La topología así definida en Y se denomina la topología final en Y definida por f.

Y con la topología final es el representante del funtor $F: \mathscr{C}_{Top} \to \mathscr{C}_{Conj}$ definido por

$$F(Z) := \{g \in \mathrm{Aplic}(Y,Z):\ g \circ f \in \mathrm{Hom}_{cont}(X,Z)\}$$

y se dice que $(*)$ es la propiedad universal de la topología final en Y definida por f.

2.5.3. Espacio de soluciones de un sistema de ecuaciones

Consideremos un sistema de ecuaciones k-algebraicas

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

Sea $\mathscr{C}_{k-alg}$ la categoría de k-álgebras y $\mathscr{C}_{Conj}$ la categoría de conjuntos. Definamos el funtor "espacio de soluciones del sistema de ecuaciones algebraica $p_1 = \cdots = p_r = 0$":

$$\begin{array}{rccc} \mathrm{Esp}(p_1=\cdots=p_r=0): & \mathscr{C}_{k-alg} & \rightsquigarrow & \mathscr{C}_{Conj} \\ & A & \mapsto & \left\{ \begin{array}{l} \text{Conjunto de soluciones con} \\ \text{valores en el anillo } A \\ \text{del sistema } p_1=\cdots=p_r=0 \end{array} \right\} \end{array}$$

Al morfismo de k-álgebras $f: A \to B$, $\mathrm{Esp}(p_1 = \cdots = p_r = 0)$ le asigna la aplicación

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{Conjunto de soluciones con} \\ \text{valores en el anillo } A \\ \text{del sistema } p_1=\cdots=p_r=0 \end{array} \right\} & \to & \left\{ \begin{array}{l} \text{Conjunto de soluciones con} \\ \text{valores en el anillo } B \\ \text{del sistema } p_1=\cdots=p_r=0 \end{array} \right\} \\ (a_1,\ldots,a_n) & \mapsto & (f(a_1),\ldots,f(a_n)) \end{array}$$

$\mathrm{Esp}(p_1 = \cdots = p_r = 0)$ es representable ya que el morfismo de funtores

$$\mathrm{Esp}(p_1 = \cdots = p_r = 0) \to \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),-)$$

definido por $\mathrm{Esp}(p_1 = \cdots = p_r = 0)(A) \to \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),A)$, $\alpha \mapsto \phi_\alpha$ (donde $\phi_\alpha(\overline{p(x)}) := p(\alpha)$) sabemos que es biyectivo.

11. Ejemplo: La recta real es $\mathbb{R}$, la recta compleja es $\mathbb{C}$. Definamos el funtor sobre la categoría de k-álgebras $\mathrm{Recta}^{\cdot}$, como el funtor $\mathrm{Recta}^{\cdot}(A) := A$. Observemos que $\mathrm{Recta}^{\cdot} = \mathrm{Hom}_{k-alg}(k[x],-)$.

Sea

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

un sistema de ecuaciones algebraicas. Consideremos el funtor $\mathrm{Esp}(p_1 = \cdots = p_r = 0)$. Se cumple que

$$\begin{aligned} \mathrm{Hom}(\mathrm{Esp}(p_1 = \cdots = p_r = 0), \mathrm{Recta}^{\cdot}) &= \mathrm{Hom}_{k-alg}(k[x], k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)) \\ &= k[x_1,\ldots,x_n]/(p_1,\ldots,p_r) \end{aligned}$$

"$k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ es el anillo de todas las funciones universales del conjunto de soluciones de un sistema de ecuaciones algebraicas $p_1 = \cdots = p_r = 0$"

Explícitamente, dado $\overline{p(x_1,\ldots x_n)} \in k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ define el morfismo

$$\begin{aligned} \mathrm{Esp}(p_1 = \cdots = p_r = 0) &\to \mathrm{Recta}^{\cdot} \\ \mathrm{Esp}(p_1 = \cdots = p_r = 0)(A) &\to \mathrm{Recta}^{\cdot}(A) = A \\ (a_1,\ldots,a_n) &\mapsto p(a_1,\ldots,a_n) \end{aligned}$$

12. Ejemplo: Sean dos sistemas de ecuaciones algebraicas

$$\left\{\begin{array}{l} p_1(x_1,\ldots,x_n) = 0 \\ \cdots \\ p_r(x_1,\ldots,x_n) = 0 \end{array}\right. \qquad \left\{\begin{array}{l} q_1(y_1,\ldots,y_m) = 0 \\ \cdots \\ q_s(y_1,\ldots,y_m) = 0 \end{array}\right.$$

Se cumple que

$$\begin{aligned} &\mathrm{Hom}(\mathrm{Esp}(p_1 = \cdots = p_r = 0), \mathrm{Esp}(q_1 = \cdots = q_s = 0)) \\ &\qquad = \mathrm{Hom}_{k-alg}(k[y_1,\ldots,y_m]/(q_1,\ldots,q_s), k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)) \end{aligned}$$

Explícitamente, el morfismo de k-algebras

$$f : k[y_1,\ldots,y_m]/(q_1,\ldots,q_s) \to k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)\ f(\bar{y}_i) = \overline{r_(x_1,\ldots,x_n)},$$

define el morfismo

$$\begin{array}{rcl} \mathrm{Esp}(p_1=\cdots=p_r=0) & \stackrel{f^*}{\to} & \mathrm{Esp}(q_1=\cdots=q_s=0) \\ \mathrm{Esp}(p_1=\cdots=p_r=0)(A) & \to & \mathrm{Esp}(q_1=\cdots=q_s=0)(A) \\ (a_1,\ldots,a_n) & \mapsto & (b_1=r_1(a_1,\ldots,a_n),\ldots,b_m=r_m(a_1,\ldots,a_n)) \end{array}$$

13. Teorema: *"Dos sistemas de ecuaciones algebraicas (con las mismas variables) tienen el mismo conjunto de soluciones (para todo anillo) si y sólo si los ideales generados por los polinomios de las ecuaciones de cada sistema coinciden" Con mayor precisión, sean*

$$\left\{\begin{array}{l} p_1(x_1,\ldots,x_n)=0 \\ \cdots \\ p_r(x_1,\ldots,x_n)=0 \end{array}\right. \qquad \left\{\begin{array}{l} q_1(x_1,\ldots,x_n)=0 \\ \cdots \\ q_s(x_1,\ldots,x_n)=0 \end{array}\right.$$

dos sistemas de ecuaciones algebraicas. Se cumple que

$$\mathrm{Esp}(p_1=\cdots=p_r=0)=\mathrm{Esp}(q_1=\cdots=q_s=0) \iff (p_1,\cdots,p_r)=(q_1,\ldots,q_s)$$

Demostración. Decir que $\mathrm{Esp}(p_1=\cdots=p_r=0)=\mathrm{Esp}(q_1=\cdots=q_s=0)$ quiere decir que el morfismo

$$\begin{array}{rcl} \mathrm{Esp}(p_1=\cdots=p_r=0) & \to & \mathrm{Esp}(q_1=\cdots=q_s=0) \\ \mathrm{Esp}(p_1=\cdots=p_r=0)(A) & \to & \mathrm{Esp}(q_1=\cdots=q_s=0)(A) \\ (a_1,\ldots,a_n) & \mapsto & (a_1,\ldots,a_n) \end{array}$$

está bien definido y es un isomorfismo. Es decir, el morfismo

$$k[x_1,\ldots,x_n]/(q_1,\ldots,q_s)\to k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),\ \bar{x}_i\mapsto\bar{x}_i,$$

está bien definido y es un isomorfismo. Ahora bien, este morfismo está bien definido si aplica los $\bar{q}_i$ al cero, es decir $(q_1,\ldots,q_s)\subseteq(p_1,\ldots,p_r)$. El morfismo inverso para que exista ha de estar definido por $k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)\to k[x_1,\ldots,x_n]/(q_1,\ldots,q_s)$, $\bar{x}_i\mapsto\bar{x}_i$. De nuevo este morfismo está bien definido si y sólo si $(p_1,\ldots,p_r)\subseteq(q_1,\ldots,q_s)$.

En conclusión,

$$\mathrm{Esp}(p_1=\cdots=p_r=0)=\mathrm{Esp}(q_1=\cdots=q_s=0) \iff (p_1,\cdots,p_r)=(q_1,\ldots,q_s)$$

□

2.5.4. Espacio de un anillo de funciones

Hemos probado que el anillo de funciones universales de $\mathrm{Esp}(p_1 = \cdots = p_r = 0)$ es la k-álgebra $k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ y que

$$\mathrm{Esp}(p_1 = \cdots = p_r = 0) = \mathrm{Hom}_{k-alg}(k[x_1,\ldots,x_n]/(p_1,\ldots,p_r),-).$$

También denotaremos a $\mathrm{Esp}(p_1 = \cdots = p_r = 0)$ por $\mathrm{Esp}\, k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ (y lo leeremos, espacio de anillo de funciones $k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$). En general:

14. Definición: Sea A una k-álgebra. Definiremos

$$\mathrm{Esp}\, A = \mathrm{Hom}_{k-alg}(A,-)$$

y diremos que $\mathrm{Esp}\, A$ es el espacio de anillo de funciones A.

Todo morfismo de k-álgebras $f\colon A \to B$, define el morfismo $f^*\colon \mathrm{Esp}\, B \to \mathrm{Esp}\, A$, $f^*(g) = g \circ f$.

15. Proposición: $\mathrm{Hom}(\mathrm{Esp}\, A, \mathrm{Recta}^{\cdot}) = A$.

Demostración. $\mathrm{Hom}(\mathrm{Esp}\, A, \mathrm{Recta}^{\cdot}) = \mathrm{Hom}_{k-alg}(k[x], A) = A$. Explícitamente, $a \in A$, define el morfismo

$$\begin{array}{rcl} \mathrm{Esp}\, A & \to & \mathrm{Recta}^{\cdot} \\ \mathrm{Hom}_{k-alg}(A,B) = \mathrm{Esp}\, A(B) & \to & B = \mathrm{Recta}^{\cdot}(B) \\ f & \mapsto & f(a) \end{array}$$

□

16. Notación: Diremos que $x \in \mathrm{Esp}\, A(B) = \mathrm{Hom}_{k-alg}(A,B)$ es un punto de $\mathrm{Esp}\, A$ (con valores en B). Dado $a \in A$ y $x \in \mathrm{Esp}\, A(B)$, denotaremos $a(x) = x(a)$.

17. Proposición: *Una función $a \in A$ es nula si y sólo si $a(x) = 0$ para todo punto de* $\mathrm{Esp}\, A$.

Sea $I \subset A$ un ideal. Recordemos la propiedad universal del cociente:

$$\mathrm{Hom}_{Anillos}(A/I,B) = \{f \in \mathrm{Hom}_{Anillos}(A,B), \text{ tales que } f(I) = 0\}$$

18. Proposición: *"*$\mathrm{Esp}\, A/I$ *se identifica con los puntos de* $\mathrm{Esp}\, A$ *donde se anulan todas las funciones del ideal I"*

Demostración. El epimorfismo natural $A \to A/I$ define la inyección $\mathrm{Esp}\, A/I \hookrightarrow \mathrm{Esp}\, A$. Tenemos que probar que

$$\mathrm{Esp}\, A/I(B) = \{x \in \mathrm{Esp}\, A(B), \text{ tales que } i(x) = 0, \text{ para todo } i \in I\}$$

que es la propiedad universal del cociente por un ideal recién enunciada.

□

19. Proposición: *Se cumple que* $\mathrm{Esp}\, A \times \mathrm{Esp}\, B = \mathrm{Esp}(A \otimes_k B)$.

Demostración. Tenemos que probar, para toda k-álgebra C, que

$$(\mathrm{Esp}\, A \times \mathrm{Esp}\, B)(C) = \mathrm{Esp}(A \otimes_k B)(C)$$

lo cual es la propiedad universal del producto tensorial de k-álgebras □

Como

$$\begin{aligned}\mathrm{Esp}(p_1(x) = \cdots = p_r(x) = 0) \times \mathrm{Esp}(q_1(y) = \cdots = q_s(y) = 0)\\ = \mathrm{Esp}(p_1(x) = \cdots = p_r(x) = q_1(y) = \cdots = q_s(y) = 0),\end{aligned}$$

entonces

$$k[x,y]/(p_i(x), q_j(y)) = k[x]/(p_i(x)) \otimes_k k[y]/(q_j(y))$$

Dados dos morfismo de funtores $f : F_1 \to F$, $g : F_2 \to F$ se define el producto fibrado $F_1 \times_F F_2$, como sigue

$$(F_1 \times_F F_2)(A) := F_1(A) \times_{F(A)} F_2(A) = \{(x_1, x_2) \in F_1(A) \times F_2(A) \text{ tales que } f_A(x_1) = g_A(x_2)\}$$

20. Proposición: *Sean* $C \to A$ *y* $C \to B$ *dos morfismos de* k*-álgebras. Tenemos pues los morfismos* $\mathrm{Esp}\, A \to \mathrm{Esp}\, C$ *y* $\mathrm{Esp}\, B \to \mathrm{Esp}\, C$. *Se cumple que*

$$\mathrm{Esp}\, A \times_{\mathrm{Esp}\, C} \mathrm{Esp}\, B = \mathrm{Esp}(A \otimes_C B)$$

Demostración. Tenemos que probar que

$$\mathrm{Esp}\, A(D) \times_{\mathrm{Esp}\, C(D)} \mathrm{Esp}\, B(D) = \mathrm{Esp}(A \otimes_C B)(D)$$

para toda k-álgebra D. En efecto, tenemos la igualdad

$$\begin{array}{rcll} \mathrm{Hom}_{k-alg}(A \otimes_C B, D) & = & \mathrm{Hom}_{k-alg}(A,D) \times_{\mathrm{Hom}_{k-alg}(C,D)} \mathrm{Hom}_{k-alg}(B,D) \\ f & \longmapsto & (f_1, f_2) \qquad f_1(a) := f(a \otimes 1), f_2(b) := f(1 \otimes b) \\ F(a \otimes b) := f_1(a) \cdot f_2(b), & F & \longmapsto & (f_1, f_2) \end{array}$$

□

21. Sea A una k-álgebra. Dados dos cuerpos K y K' y $x \in \operatorname{Esp} A(K)$ y $x' \in \operatorname{Esp} A(K')$ diremos que $x \sim x'$ si existe un cuerpo Σ y morfismos $i\colon K \hookrightarrow \Sigma$ e $i'\colon K' \hookrightarrow \Sigma$ tales que $i \circ x = i' \circ x'$. Si $x'' \in Esp\, A(K'')$ cumple que $x'' \sim x'$, es decir, existen morfismos $\tilde{i}'\colon K' \hookrightarrow \Sigma'$ y $i''\colon K'' \hookrightarrow \Sigma'$ tales que $\tilde{i}' \circ x' = i'' \circ x''$, y definimos $\Sigma'' = (\Sigma \otimes_{K'} \Sigma')/\mathfrak{m}$ (donde $\mathfrak{m}$ es un ideal maximal de $\Sigma \otimes_{K'} \Sigma'$), entonces tenemos morfismos naturales $j\colon K \to \Sigma''$, $j(\lambda) := \overline{i(\lambda) \otimes 1}$, $j'\colon K' \to \Sigma''$, $j'(\lambda) := \overline{i'(\lambda) \otimes 1} = \overline{1 \otimes \tilde{i}'(\lambda)}$ y $j''\colon K'' \to \Sigma''$, $j''(\lambda) := \overline{1 \otimes i''(\lambda)}$ de modo que $j \circ x = j' \circ x' = j'' \circ x''$, luego $x \sim x''$.

Dado un punto $y \in \operatorname{Spec} A$, sea $k(y) := (A/\mathfrak{p}_y)_y$ el cuerpo residual de y y denotemos por $\tilde{y} \in Esp A(k(y))$ el morfismo natural $\tilde{y}\colon A \to k(y)$, $\tilde{y}(a) := \frac{a(y)}{1}$.

22. Proposición: *La aplicación* $\operatorname{Spec} A \to \coprod_{k\text{-ext. } K} \operatorname{Esp} A(K) \Big/ \sim$, $y \mapsto [\tilde{y}]$ *es biyectiva.*

Demostración. Dado $x \in \operatorname{Esp} A(K)$, si denotamos $\mathfrak{p}_z = \operatorname{Ker} x$, entonces $[\tilde{z}] = [x]$. Es fácil comprobar que $[x] \mapsto \operatorname{Ker} x$ es la asignación inversa. □

2.6. Biografía de Zariski

ZARISKI BIOGRAPHY

Oscar Zariski's father was Bezalel Zaritsky and his mother Hannah Zaritsky. Oscar, born into this Jewish family, was named Ascher Zaritsky by his parents. We will comment below on how his name came to be changed to the now familiar version of Oscar Zariski.

Oscar's mother was the one who ensured that her young son had a good education. A tutor was provided for Oscar from the time he was seven years old and Oscar, under the guidance of the tutor, showed remarkable aptitude for the Russian language and for arithmetic. When the fighting associated with World War I reached Belarus, Oscar's family fled to Chernigov in the Ukraine. It was the first of several moves forced on him by political problems.

Unable to enter the faculty of mathematics at the University of Kiev as all the places were full, he chose philosophy instead. He was a student of philosophy at Kiev from 1918 to 1920. However he was able to pursue his mathematical interests and studied algebra and number theory in addition to philosophy. However Zariski had carried out his studies through a period of turmoil in Kiev.

In January 1918 Ukraine had become an independent state with Kiev as its capital. In the following month minor uprisings by workers in Kiev were suppressed but

Red Army troops entered Kiev to give support to the workers. Kiev was then occupied by the Germans, but with the end of the war in November 1918, an independent Ukraine was declared again in Kiev. In November 1919 Kiev was briefly taken by the White armies, soon after to be replaced by the Red Army. There then followed the Russian-Polish War and, in May 1920, the Polish army captured Kiev but were forced out in a counterattack. Life for Zariski was just too difficult in this city so devastated by war, so he decided to go to Italy to continue his studies.

In Rome Zariski came under the influence of the great algebraic geometers Castelnuovo, Enriques and Severi. He obtained a doctorate from Rome in 1924 for a doctoral thesis on a topic related to Galois theory which was proposed to him by Castelnuovo. Zariski married in 1924; having met his future wife Yole Cagli in Rome they returned to Zariski's home town of Kobin to marry. Returning to Rome he remained there as a fellow of the International Education Board until 1927.

It was while Zariski was in Rome that Enriques suggested that Ascher Zaritsky, as he was then called, change his name to the Italian sounding Oscar Zariski. This was the name which he used on his first publication which was a joint paper with Enriques. Zariski wrote of how his mathematical interests differed from those of his supervisors Castelnuovo and Enriques:

However, even during my Rome period, my algebraic tendencies were showing and were clearly perceived by Castelnuovo who once told me: "You are here with us but are not one of us."This was said not in reproach but good naturedly, for Castelnuovo himself told me time and time again that the methods of the Italian geometric school had done all they could do, had reached a dead end, and were inadequate for further progress in the field of algebraic geometry.

Zariski had gone to Italy to escape the problems in Belarus and the Ukraine. However, the political situation in Italy began to deteriorate rapidly. In October 1922 Mussolini organized the Fascist "March on Rome" and he was asked to form a government. For 18 months he ran the country in reasonably democratic way but, during the years 1925 to 1927, he removed the right of free speech, and removed opposition parties and trade unions. The Fascist hatred of Jews made life for Zariski, because of his Jewish background, particularly difficult.

Helped by Lefschetz, he escaped from the political problems of Italy in 1927 and went to the United States. There he taught at Johns Hopkins University, being a Johnston Scholar until 1929 when he joined the Faculty. He became a full professor at Johns Hopkins in 1937.

Castelnuovo and Severi had encouraged Zariski to view Lefschetz's topological methods as being the road ahead for algebraic geometry, so between 1927 and 1937 Zariski frequently visited Lefschetz at Princeton. Zariski wrote :

I owe a great deal to [Lefschetz] for his inspiring guidance and encouragement.

During this period Zariski wrote Algebraic Surfaces which was published in 1935. He explained how writing this monograph changed the direction of his work:

At that time (1935) modern algebra had already come to life (through the work of Emmy Noether and the important treatise of BL van der Waerden), but while it was being applied to some aspects of the foundations of algebraic geometry by van der Waerden ... the deeper aspects of birational algebraic geometry ... were largely, or even entirely, virgin territory as far as algebraic exploration was concerned. In [Algebraic Surfaces] I tried my best to present the underlying ideas of the ingenious geometric methods and proofs with which the Italian geometers were handling these deeper aspects of the whole theory of surfaces ... I began to feel distinctly unhappy about the rigour of the original proofs (without losing in the least my admiration for the imaginative geometric spirit that permeated these proofs); I became convinced that the whole structure must be done over again by purely algebraic methods.

At Johns Hopkins University between 1939 and 1940 Zariski carried out his project of applying modern algebra to the foundations of algebraic geometry. He worked on the theory of normal varieties, local uniformisation and the reduction of singularities of algebraic varieties.

An important year for Zariski was 1945 which he spent in São Paolo. There he gave a lecture course three days each week which was attended by André Weil and nobody else. Both Zariski and Weil learnt much in discussions, often arguments, about the material that Zariski was presenting. After spending the year 1946-47 at the University of Illinois, Zariski was appointed to a chair at Harvard where he was to remain until he retired in 1969. From the late 1970s he suffered from Alzheimer's disease and his last few years were difficult ones as his health failed.

In 1981 Zariski was awarded the Steele Prize by the American Mathematical Society for the cumulative influence of his total mathematical research. The citation for the prize summarised Zariski's contributions to mathematics throughout his life:

After beginning his work in Italy in 1924 very much in the style of Ïtalian algebraic geometry,"Zariski realised that the whole subject needed proper foundations. Thus in the period 1927 to 1937 he turned first to topological questions and then in 1937 he began to lay the commutative algebraic foundations of his subject. His topological work concentrated mainly on the fundamental group; many of the ideas he pioneered were innovations in topology as well as algebraic geometry and have developed independently in the two fields since then.

In 1937 Zariski completely reoriented his research and began to introduce ideas from abstract algebra into algebraic geometry. Indeed, together with BL van der Waerden and André Weil, he completely reworked the foundations of the subject without the use of topological or analytic methods. His use of the notions of integral independence, valuation rings, and regular local rings, in algebraic geometry proved particularly

fruitful and led him to such high points as the resolution of singularities for threefolds in characteristic 0 in 1944, the clarification of the notion of simple point in 1947, and the theory of holomorphic functions on algebraic varieties over arbitrary ground fields. The theory of equisingularity and saturation begun by Zariski in 1965 has also been of great influence and importance.

All of Zariski's work has served as a basis for the present flowering of algebraic geometry and the current school uses his work and ideas in the modern development of the subject.

Zariski's most famous book is Commutative Algebra, a two volume work written jointly with P Samuel. The first volume appeared in 1958, the second in 1960.

The American Mathematical Society played a large role in Zariski's life and he contributed greatly to the Society over many years. He was vice president of the Society between 1960 and 1961 and president of the Society from 1969 to 1970.

Zariski played an important role in mathematical publishing after his appointment as a full professor. He was an editor of the American Mathematical Journal from 1937 to 1941, served as a member of the editorial committee of the Transactions of the American Mathematical Society from 1941 to 1947, and also served on the editorial boards of the Annals of Mathematics and the American Journal of Mathematics.

After going to the United States in 1927 Zariski spent considerable periods lecturing at other universities both in the United States and in other countries. We have already mentioned that he was a visiting professor at São Paulo in 1945 and a visiting professor at the University of Illinois in 1946-47. Before that, in 1936, he had lectured at the University of Moscow. Later, he lectured at Kyoto (1956), the Institut des Hautes Études Scientifique (1961 and again 1967), and the University of Cambridge (1972).

He was awarded many honours for his work in addition to the Steele Prize described above. He was awarded the Cole Prize in Algebra from the American Mathematical Society in 1944 for four papers on algebraic varieties, two published in the American Journal of Mathematics in 1939 and 1940, and the other two in the Annals of Mathematics also one in 1939 and the second in 1940. He was awarded the National Medal of Science in 1965.

Many academies and societies have honoured him by electing him to membership, including the U.S. National Academy of Sciences (1944), the American Academy of Arts and Sciences (1948), the American Philosophical Society (1951), the Brazilian Academy of Sciences (1958), and the Accademia Nazionale dei Lincei (1958).

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

2.7. Cuestionario

1. Calcula el espectro racional de la $\mathbb{R}$-álgebra $\mathbb{R}[x,y]/(x^2+y^2+1)$. Calcula el espectro racional de la $\mathbb{R}$-álgebra $\mathbb{R}[x,y]/(x^2+y^2-1, x-y)$.

2. Sea A una $\mathbb{C}$-álgebra. Si consideramos A como una $\mathbb{R}$-álgebra, prueba que

$$\mathrm{Spec}_{rac}\, A = \emptyset.$$

3. Sea $A = k[x,y]$ e $I = (x+y, (x^2+y^2-1)^2) \subset k[x,y]$. Calcula $(I)_0 \cap \mathrm{Spec}_{rac}\, A$.

4. Sea A un anillo íntegro. Calcula las componentes irreducibles de $\mathrm{Spec}\, A$.

5. ¿Tiene $\mathrm{Spec}\, A$ tantos cerrados irreducibles como puntos?¿Tiene $\mathrm{Spec}\, A$ tantas componentes irreducibles como ideales primos minimales hay en A? Si A es noetheriano ¿$\mathrm{Spec}\, A$ es unión de un número infinito de componentes irreducibles distintas?

6. Supongamos que $\mathrm{Spec}\, A$ es irreducible. Prueba que todo abierto no vacío de $\mathrm{Spec}\, A$ contiene al punto genérico de $\mathrm{Spec}\, A$. Prueba que todo abierto no vacío de $\mathrm{Spec}\, A$ es denso.

7. ¿Es la intersección de ideales radicales un ideal radical?

8. Sea $I \subset A$ un ideal. Prueba que $r(r(I)) = r(I)$.

9. Sea I un ideal de un anillo noetheriano. Prueba que $I = r(I)$ si y sólo si I es intersección de un número finito de ideales primos.

10. Consideremos el morfismo de anillos $i : \mathbb{C}[x] \hookrightarrow \mathbb{C}[x,y]/(xy-1)$, $i(p(x)) := \overline{p(x^2)}$ y la aplicación i^* inducida en los espectros. Calcula un punto $z \in \mathrm{Spec}\, \mathbb{C}[x]$ tal que $i^{*-1}(z) = \emptyset$.

11. Calcula el espectro primo y el espectro racional de la $\mathbb{C}$-álgebra

$$\mathbb{C}[x,y,z]_z/(x, x^2+y^2+z^2-1).$$

12. Prueba que $\mathrm{Hom}(\mathrm{Recta}^{\cdot}, \mathrm{Recta}^{\cdot}) = k[x]$.

2.8. Problemas

1. Sea $S^1 = \{(\alpha,\beta) \in \mathbb{R}^2 \colon \alpha^2+\beta^2 = 1\}$ y consideremos la aplicación $\pi \colon S^1 \to \mathbb{R}$, donde $\pi(p) \in \mathbb{R}$ es el número real tal que la recta que pasa por $(2,2)$ y p pasa por $(\pi(p),0)$. Calcula un morfismo de $\mathbb{R}$-álgebras $f \colon \mathbb{R}[x] \to (\mathbb{R}[x,y]/(x^2+y^2-1))_{y-2}$ tal que la aplicación inducida entre los espectros racionales sea igual a π.

2. Sea A una k-álgebra, $I \subset A$ un ideal. Prueba que $(I)_0^{rac} = \mathrm{Spec}_{rac}(A/I)$.

3. Da un ejemplo de $\mathbb{R}$-álgebra cuyo espectro racional se identifique con dos puntos unidos disjuntamente con la intersección de un plano con un cono.

4. Sea A una k-álgebra y $S \subset A$ un sistema multiplicativo. Prueba que

$$\mathrm{Spec}_{rac} A_S = \{z \in \mathrm{Spec}_{rac} A \colon s(z) \neq 0 \ \forall\, s \in S\}.$$

5. Sea X un espacio topológico compacto Hausdorff y $C(X)$ su $\mathbb{R}$-álgebra de funciones reales continuas. Consideremos $\mathrm{Spec}_{max} C(X)$ como subespacio topológico de $\mathrm{Spec} C(X)$. Prueba

   a) La aplicación $X \to \mathrm{Spec}_{max} C(X)$, $p \mapsto \mathfrak{m}_p := \{f \in C(X) \colon f(p) = 0\}$ es un homeomorfismo.

   b) Sea Y otro espacio topológico compacto Hausdorff. La aplicación

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

   es biyectiva.

   c) Sea $Y \subset X$ un subespacio cerrado e $I = \{f \in C(X) \colon f_{|Y} = 0\}$. $\mathrm{Spec}_{max} C(X)/I$ es homeomorfo a Y.

6. Sea $\mathscr{C}^\infty(\mathbb{R}^n)$ la $\mathbb{R}$-álgebra de todas las funciones de $\mathbb{R}^n$ con valores en $\mathbb{R}$ infinitamente diferenciables. Prueba que la aplicación

$$\phi \colon \mathbb{R}^n \to \mathrm{Spec}_{rac} \mathscr{C}^\infty(\mathbb{R}^n),\ \phi(p) = \mathfrak{m}_p := \{f \in \mathscr{C}^\infty(\mathbb{R}^n) \colon f(p) = 0\}$$

   es un homeomorfismo.

7. Prueba que un anillo A es el producto directo de dos anillos (no nulos) si y solo si $\mathrm{Spec} A$ no es conexo.

8. Demuestra que $A = \mathbb{Q}[x,x_1,\ldots,x_n,\ldots]/((x-n)x_n)_{\{n\in\mathbb{N}\}}$ es localmente noetheriano pero no es noetheriano.

9. Lema de Nakayama: Sea $\mathcal{O}$ un anillo local (i.e., con un único ideal maximal $\mathfrak{m}$) y M un $\mathcal{O}$-módulo finito generado. Prueba:

   a) $\mathfrak{m}\cdot M = M$ si y solo si $M = 0$.

   b) $m_1,\dots,m_n$ generan M si y sólo si $\bar{m}_1,\dots,\bar{m}_n$ generan el $\mathcal{O}/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}\cdot M$.

   c) Si M es un $\mathcal{O}$-módulo libre, $m_1,\dots,m_n$ es una base de M si y sólo si $\bar{m}_1,\dots,\bar{m}_n$ es una base del $\mathcal{O}/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}\cdot M$.

10. Sea M un A-módulo finito generado. Prueba que $U = \{x \in \operatorname{Spec} A : M_x = 0\}$ es un abierto de $\operatorname{Spec} A$.

11. Sea $I \subset A$ un ideal. Prueba que $I_x = A_x$ si y solo si $x \in \operatorname{Spec} A \setminus (I)_0$. Si $I \subset A$ es un ideal finito generado tal que $I = I^2$, prueba que $(I)_0$ es un abierto de $\operatorname{Spec} A$.

12. Sea $C(X)$ el anillo de las funciones reales continuas sobre un espacio topológico métrico (X,d) y sea x un punto de X no aislado. Consideremos el ideal maximal $\mathfrak{m}_x$ de $C(X)$ formado por las funciones que se anulan en x. Sea $\mathcal{O}$ el anillo de gérmenes en x de funciones reales continuas.

    a) Prueba que $\mathfrak{m}_x = \mathfrak{m}_x^2$. (Indicación: Si $f \in \mathfrak{m}_x$, entonces $f = \sup(f,0) - \sup(-f,0)$ y $\sqrt{\sup(f,0)},\ \sqrt{\sup(-f,0)} \in \mathfrak{m}_x$).

    b) Prueba que el anillo $C(X)$ no es noetheriano.

    c) Prueba que $C(X)_x \to \mathcal{O}$, $\frac{f}{g} \mapsto [f]\cdot[g]^{-1}$ es un isomorfismo de anillos.

13. Sea $\mathfrak{m}_{or}$ el ideal maximal de $C^\infty(\mathbb{R})$ formado por las funciones que se anulan en el punto 0. Prueba que $\mathcal{O} = C^\infty(\mathbb{R})_{or}$ es el anillo de gérmenes de funciones diferenciables en el punto 0. Sea I el ideal de $\mathcal{O}$ formado por los gérmenes cuya serie de Taylor en 0 es nula. Prueba que $xI = I$ y concluye que el anillo $\mathcal{O}$ no es noetheriano.

14. Sea A un anillo noetheriano. Prueba que $\operatorname{rad}(A)^n = 0$ para algún exponente n. Si I es un ideal de A, prueba que $r(I)^n \subseteq I$ para algún exponente n.

15. Sea A un anillo. Prueba que si $a \in A$ pertenece a un ideal primo minimal entonces es divisor de cero.

16. Sea A un anillo. Prueba:

    a) Dados dos puntos $x, x' \in \operatorname{Spec} A$, existen dos abiertos disjuntos U y U' tales que $x \in U$ y $x' \in U'$ si y solo si no existe ningún ideal primo $\mathfrak{p}_y \subseteq \mathfrak{p}_x, \mathfrak{p}_{x'}$.

b) $\operatorname{Spec} A$ es T_1 si y solo si es T_2.

c) Sea $\operatorname{Spec}_{min} A$ el conjunto de los ideales primos minimales. Prueba que el subespacio $\operatorname{Spec}_{min} A \subseteq \operatorname{Spec} A$ es T_2.

d) $\operatorname{Spec} A$ es discreto si y solo si $\operatorname{Spec} A$ es finito y T_1.

17. Sea X un espacio topológico y $\mathscr{C}(X)$ la $\mathbb{R}$-álgebra de funciones continuas de X en $\mathbb{R}$. Prueba que $\operatorname{Spec}_{rac} \mathscr{C}(X)$ es compacto si y solo si $\operatorname{Spec}_{rac} \mathscr{C}(X) = \operatorname{Spec}_{max} \mathscr{C}(X)$.

18. Supongamos que $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ es un espacio topológico discreto (equivalentemente, los puntos $x_1, \ldots, x_n$ son cerrados). Prueba que el morfismo natural de anillos $A \to A_{x_1} \times \cdots \times A_{x_n}$, $a \mapsto (\frac{a}{1}, \ldots, \frac{a}{1})$ es un isomorfismo.

19. Sean $x_1, \ldots, x_n \in \operatorname{Spec} A$ e $I \subset A$ un ideal.

a) Si $I \subseteq \mathfrak{p}_{x_1} \cup \cdots \cup \mathfrak{p}_{x_n}$, prueba que $I \subseteq \mathfrak{p}_{x_i}$, para algún i.

b) Sea $S = A \setminus \bigcup_{i=1}^{n} \mathfrak{p}_{x_i}$. Prueba que $\operatorname{Spec} A_S = \bigcup_{i}^{n} \operatorname{Spec} A_{x_i}$. Por tanto, A_S es un anillo semilocal[1] de ideales maximales $\mathfrak{p}_{x_i} \cdot A_S$ (con $\mathfrak{p}_{x_i}$ no incluido en $\mathfrak{p}_{x_j}$, para ningún $j \neq i$).

20. Prueba que si $\operatorname{Spec} A$ es unión disjunta de dos abiertos U y V, entonces estos abiertos son básicos.

21. Sea $\mathfrak{m}_x \subset A$ un ideal maximal y $1 + \mathfrak{m}_x := \{1 + a; \forall a \in \mathfrak{m}_x\}$. Prueba que $A_x = A_{1+\mathfrak{m}_x}$.

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

a) Si $(I)_0$ está incluido en un abierto U, existe $i \in I$ tal que $(I)_0 \subset U_{1+i} \subset U$.

b) $(I)_0 \subset U_{1+i}$ para todo $i \in I$.

c) $\operatorname{Spec} A_{1+I} = \bigcap_{(I)_0 \subset U} U$.

d) $\operatorname{Spec}_{max} A_{1+I} = (I)_0^{max}$.

23. Prueba que un anillo A es íntegro si y solo si es reducido y $\operatorname{Spec} A$ es irreducible.

24. Prueba que $\operatorname{Spec} A$ es irreducible si y solo si se cumple que si $a \cdot b = 0$ entonces a o b es nilpotente.

25. Calcula $\operatorname{Spec} \mathbb{Z}[x]$.

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

26. Calcula $\operatorname{Spec}\mathbb{R}[x,y]$.

27. Calcula $\operatorname{Spec}\mathbb{Z}[i]$.

28. Prueba que $\mathbb{C}[x,y,z]/(zx-y) \simeq \mathbb{C}[x,y/x]$, como $\mathbb{C}$-álgebras. Consideremos el morfismo $i\colon \mathbb{C}[x,y] \to \mathbb{C}[x,y,z]/(zx-y)$, $p(x,y) \mapsto \overline{p(x,y)}$ y sea i^* el morfismo inducido en los espectros. Prueba:

    a) $i^{*-1}(U_x) \xrightarrow{i^*} U_x$ es un homeomorfismo.

    b) $i^{*-1}((0,0)) = \{(\bar{x}), (\bar{x},\bar{y},\bar{z}-\gamma),\ \forall \gamma \in \mathbb{C}\} = (\bar{x})_0$

    c) $i^{*-1}((y-\lambda x)_0) = (\bar{y}-\lambda\bar{x}, \bar{z}-\lambda)_0 \cup i^{*-1}((0,0))$.

29. Determina si los siguientes sistemas de ecuaciones con coeficientes racionales son equivalentes al sistema $x^2+y^2=1, x^2y^2=0$:

$$\begin{cases} 1 = x^2+y^2 \\ x^4 = x^2 \end{cases} \qquad \begin{cases} 1 = x^2-y^2 \\ 0 = x^2y^2 \end{cases} \qquad \begin{cases} 1 = x^2-y^2 \\ 1 = x^2+y^2 \end{cases}$$

$$\begin{cases} 1 = x^2+y^2 \\ 0 = (x+y+1)^2(x+y-1)^2 \end{cases} \qquad \begin{cases} 1 = x^2+y^2 \\ 0 = (x+y+1)^2(x+y-1) \end{cases}$$

$$\begin{cases} 1 = x^2+y^2 \\ 0 = (x+y+1)(x+y-1)(x-y+1)(x-y-1) \end{cases}$$

30. Prueba que "los puntos de $\operatorname{Esp}A_S$ se identifican con los puntos de $\operatorname{Esp}A$ donde el valor de toda $s \in S$ es invertible".

Capítulo 3

Variedades algebraicas afines

3.1. Introducción

El estudio del conjunto X de soluciones de un sistema de ecuaciones algebraicas

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

es esencialmente equivalente al estudio de "la variedad algebraica" $\operatorname{Spec} A$, donde $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ es el anillo de funciones algebraicas de X.

La cadena de cerrados irreducibles

$$\{\text{punto } p\} \subset \{\text{Curva irred. } C\} \subset \{\text{Superficie irred. } S\} \subset \cdots \text{ (de } X\text{)},$$

se corresponde con la cadena de ideales primos

$$\mathfrak{p}_p \supset \mathfrak{p}_C \supset \mathfrak{p}_S \supset \cdots \text{ (de } A\text{)},$$

donde $\mathfrak{p}_p = \{\overline{p(x)} \in A : p(p) = 0\}$, $\mathfrak{p}_C = \{\overline{p(x)} \in A : p(q) = 0, \forall\, q \in C\}$ y $\mathfrak{p}_S = \{\overline{p(x)} \in A : p(q) = 0, \forall\, q \in S\}$. Definiremos la dimensión de Krull de A como el número de eslabones de la cadena de inclusiones de ideales primos más larga, que coincide con el número de eslabones de la cadena de inclusiones de cerrados irreducibles de $\operatorname{Spec} A$ más larga. El resultado principal será el teorema de normalización de Noether, que nos dice que existe un morfismo $\pi : X \to \mathbb{A}^s$ de fibras finitas, es decir, en términos de los anillos, existe un morfismo finito inyectivo $k[z_1,\dots,z_s] \hookrightarrow A$. Como consecuencia de este teorema obtendremos los siguientes resultados[1]:

- El grado de trascendencia de $A_{A\setminus 0}$ es igual al dimensión de Krull de A.

- El teorema de los ceros de Krull: Los ceros de toda $f \in A$, ni nula ni invertible, es una hipersuperficie de codimensión 1 de $\operatorname{Spec} A$.

[1] Supongamos por sencillez que A es íntegro.

115

- El teorema de los ceros de Hilbert: Los cerrados de $\operatorname{Spec} A$ están determinados por los puntos cerrados que contiene y éstos últimos son racionales (cuando k sea un cuerpo algebraicamente cerrado).

- Todas las cadenas de inclusiones de cerrados irreducibles de una variedad algebraica irreducible irrefinables tienen el mismo número de eslabones.

- $\dim(X \times Y) = \dim X + \dim Y$.

- Si Y, Y' son dos subvariedades irreducibles de $\operatorname{Spec} k[x_1, \ldots, x_n]$ y Z es una componente irreducible (no vacía) de $Y \cap Y'$, entonces

$$\dim Z \geq \dim Y + \dim Y' - n.$$

- Si $f : X \to Y$ es un morfismo entre variedades algebraicas irreducibles e $y \in f(X) \subset Y$ es un punto cerrado, entonces $\dim f^{-1}(y) \geq \dim X - \dim Y$.

3.2. Morfismos de anillos finitos

1. Definiciones: 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: $a \cdot b := f(a) \cdot b$, para todo $a \in A$ y $b \in B$. En este caso, también se dice que B es una A-álgebra finita.

Si $A \to B$ es un morfismo de anillos finito, diremos que el morfismo inducido en los espectros $\operatorname{Spec} B \to \operatorname{Spec} A$ es finito.

2. Ejemplos: Por definición, una extensión de cuerpos $k \hookrightarrow K$ es finita si y solo si el morfismo de anillos $k \hookrightarrow K$ es finito.

El morfismo de anillos $A \to A[x]/(x^n + a_1 x^{n-1} + \cdots + a_n)$ es finito, ya que $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ es una base del A-módulo $A[x]/(x^n + a_1 x^{n-1} + \cdots + a_n)$.

3. Ejercicio: Prueba que el morfismo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3) \to \operatorname{Spec} k[x]$ que en los puntos racionales es la asignación $(\alpha, \beta) \mapsto \alpha$ es un morfismo finito.

4. 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 $C = Bc_1 + \cdots + Bc_m$. Entonces,

$$C = (Ab_1 + \cdots + Ab_n)c_1 + \cdots + (Ab_1 + \cdots + Ab_n)c_m = \sum_{i=1,j=1}^{n,m} Ab_i c_j$$

En conclusión, $A \to C$ es un morfismo finito.

□

5. Los morfismos finitos son estables por cambio de anillo base: *Si $A \to B$ es un morfismo de anillos finito y $A \to C$ un morfismo de anillos, entonces el morfismo de anillos $C = A \otimes_A C \to B \otimes_A C$ es finito.*

Demostración. Basta que probemos que si M es un A-módulo finito generado, entonces $M \otimes_A C$ es un C-módulo finito generado. En efecto, si el A-módulo M está generado por $m_1, \ldots, m_n$, entonces el C-módulo $M \otimes_A C$ está generado por $m_1 \otimes 1, \ldots, m_n \otimes 1$.

□

6. 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*

7. 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

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0, \qquad \text{con } a_i \in A.$$

8. El teorema de Cayley-Hamilton para los endomorfismos de espacios vectoriales de dimensión finita también es cierto para los endomorfismos de módulos. Con precisión: Sea $M = \langle m_1, \ldots, m_r \rangle$ un A-módulo finito generado, $f : M \to M$, $f(m_i) = \sum_j a_{ij} m_j$ un endomorfismo de A-módulos; si $p_c(x) = |x \cdot \mathrm{Id} - (a_{ij})| \in A[x]$ es el polinomio característico de la matriz (a_{ij}), entonces $p_c(f) = 0$. Basta que probemos que $p_c((a_{ij})) = 0$. Consideremos la matriz (x_{ij}) de coeficientes variables y el polinomio característico de esta matriz $P_c(x) = |x \cdot \mathrm{Id} - (x_{ij})|$. $P_c(x)$ es un polinomio con coeficientes en $\mathbb{Z}[x_{ij}] \subset \mathbb{Q}(x_{ij})$. Por el teorema de Hamilton-Cayley $P_c((x_{ij})) = 0$. Por tanto, tomando $x_{ij} = a_{ij}$, es decir, considerando el morfismo $M_n(\mathbb{Z}[x_{ij}]_{0<i,j\leq r}) \to M_n(A)$, $(q_{rs}(x_{ij})) \mapsto (q_{rs}(a_{ij}))$, obtendremos que $0 = P_c((x_{ij})) \mapsto p_c((a_{ij})) = 0$.

9. Proposición: *Sean $f : A \to B$ un morfismo de anillos y $b \in B$. Las siguientes condiciones son equivalentes:*

1. *b es entero sobre A.*
2. *El morfismo de anillos $A \to A[b] = \{p(b) \in B,\ \forall\, p(x) \in A[x]\}$ es finito.*
3. *b pertenece a una A-subálgebra finita de B.*

Demostración. 1. $\Rightarrow$ 2. Sea $p(x)$ un polinomio mónico de grado n 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 generado por $\bar{1}, \ldots, \bar{x}^{n-1}$, entonces es finito generado y $A[b]$ también.

2. $\Rightarrow$ 3. En efecto, $b \in A[b]$.

3. $\Rightarrow$ 1. Sea $C \subseteq B$ una A-subálgebra finita tal que $b \in C$. Consideremos el endomorfismo de A-módulos

$$\begin{array}{ccc} C & \xrightarrow{\cdot b} & C \\ c & \longmapsto & c \cdot b \end{array}$$

Si (a_{ij}) es una matriz asociada a $\cdot b$ en un sistema generador del A-módulo C, entonces el polinomio característico de (a_{ij}) anula a $\cdot b$, luego anula a b, luego b es entero sobre A.

□

10. Corolario: *Un morfismo de anillos $A \to B$ es finito si y solo si existen elementos $b_1, \ldots, b_n \in B$ enteros sobre A tales que $B = A[b_1, \ldots, b_n]$.*

Demostración. $\Rightarrow$) $B = \langle b_1, \ldots, b_n \rangle$ es un A-módulo finito generado. Los elementos b_i son enteros sobre A, porque pertenecen a la A-álgebra finita B y $B = A[b_1, \ldots, b_n]$.

$\Leftarrow$) El morfismo $A[b_1, \ldots, b_i] \to A[b_1, \ldots, b_{i+1}] = A[b_1, \ldots, b_i][b_{i+1}]$ es finito, porque b_{i+1} es entero sobre A, luego sobre $A[b_1, \ldots, b_i]$. La composición de los morfismos finitos

$$A \to A[b_1] \to A[b_1, b_2] \to \cdots \to A[b_1, \ldots, b_n] = B$$

es un morfismo finito. □

11. 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 3.2.4, $A \to A[b_1, b_2]$ es un morfismo finito. Por la proposición 3.2.9, todo elemento $p(b_1, b_2) \in A[b_1, b_2] \in B$, con $p(x, y) \in A[x, y]$, es entero sobre A.

□

12. Definiciones: 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.

Llamaremos cierre entero de A en B al subanillo de B formado por todos los elementos de B enteros sobre A.

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.

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 $\mathbb{Q}$.

3.2.1. Teorema del ascenso. Aplicaciones cerradas

14. Proposición: *Toda k-álgebra finita e íntegra es cuerpo.*

Demostración. Sea A una k-álgebra finita íntegra. Dado $a \in A$ no nula, la homotecia $A \xrightarrow{\cdot a} A, b \mapsto b \cdot a$ es inyectiva, por ser A íntegra. Por tanto, por dimensiones, es isomorfismo. Luego a es invertible y A es cuerpo. □

15. Proposición: *El espectro de una k-álgebra finita es un número finito de puntos cerrados.*

Demostración. Las k-álgebras finitas son anillos noetherianos luego tienen un número finito de ideales primos minimales. Si hacemos cociente por un ideal primo minimal obtenemos una k-álgebra finita íntegra, luego es un cuerpo por la proposición anterior. Por tanto, los ideales primos minimales son maximales y hemos concluido. □

16. Proposición: *Si $f : A \hookrightarrow B$ es un morfismo finito e inyectivo, entonces la aplicación inducida $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva.*

Demostración. Dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to B_x$ es finito e inyectivo. Por el lema de 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.

□

17. Teorema: *Sea $f : A \to B$ un morfismo de anillos finito. La aplicación inducida en los espectros $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación cerrada de fibras espacios topológicos finitos discretos.*

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

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A/f^{-1}(J) & \longrightarrow & B/J \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ f^{-1}(J)_0 = \operatorname{Spec} A/f^{-1}(J) & \xleftarrow[f^*_{|C}]{} & \operatorname{Spec} B/J = C \end{array}$$

Como $A/f^{-1}(J) \hookrightarrow B/J$ es un morfismo finito inyectivo, por 3.2.16 ${f^*}_{|C}$ es epiyectiva y $f^*(C) = (f^{-1}(J))_0$.

La fibra de un punto $x \in \operatorname{Spec} A$ es ${f^*}^{-1}(x) = \operatorname{Spec} B_x/\mathfrak{p}_x B_x$. Observemos que si ${f^*}^{-1}(x) \neq \emptyset$ entonces $B_x/\mathfrak{p}_x B_x$ es una $A_x/\mathfrak{p}_x A_x$-álgebra finita. Por la proposición 3.2.15, concluimos que ${f^*}^{-1}(x)$ es un espacio topológico finito discreto. □

18. Sea $f: A \to B$ un morfismo de anillos finito, $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación inducida en espectros y $(J)_0 \subset \operatorname{Spec} B$ un cerrado. Entonces,

$$f^*((J)_0) = \overline{f^*((J)_0)} = (f^{-1}(J))_0.$$

19. Ejercicio: Prueba que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

20. Teorema del ascenso: *Sea $f: A \to B$ un morfismo finito. Sean $\mathfrak{p}_x \subset \mathfrak{p}_{x'} \subset A$ y $\mathfrak{p}_y \subset B$ ideales primos, de modo que $f^{-1}(\mathfrak{p}_y) = \mathfrak{p}_x$. Existe un ideal primo $\mathfrak{p}_{y'} \subset B$, de modo que $\mathfrak{p}_y \subset \mathfrak{p}_{y'}$ y $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$.*

Demostración. Sea $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido por f. Entonces, $f^*(y) = x$, luego $f^*(\bar{y}) \subseteq \bar{x}$. Como $x \in f^*(\bar{y})$ y $f^*(\bar{y})$ es cerrado, entonces $f^*(\bar{y}) = \bar{x}$. Por tanto, existe $y' \in \bar{y}$ tal que $f^*(y') = x' \in \bar{x}$. Es decir, existe un ideal primo $\mathfrak{p}_{y'} \supset \mathfrak{p}_y$ tal que $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$. □

Diremos que la longitud de una cadena de inclusiones (estrictas) $X_0 \subset X_1 \subset \cdots \subset X_n$ es n.

21. Definición: Llamaremos dimensión de un espacio topológico X al supremo de las longitudes de las cadenas de inclusiones de cerrados irreducibles de X, y lo denotaremos $\dim X$. Llamaremos dimensión de Krull de un anillo A, al supremo de las longitudes de las cadenas de inclusiones de ideales primos de A, o equivalentemente, a la dimensión de $\operatorname{Spec} A$. Denotaremos $\dim A$ la dimensión (de Krull) de A.

22. Ejercicio: Demuestra que la dimensión de Krull de los anillos $\mathbb{Z}$ y $k[x]$ es uno y la de $\mathbb{C}[x,y]$ dos. Prueba que $\dim k[x_1,\ldots,x_n] \geq n$.

23. Proposición: *Si $f: A \hookrightarrow B$ es un morfismo finito inyectivo, entonces* $\dim A = \dim B$.

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 son discretas, por 3.2.17. 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 3.2.16). 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 $\dim A = \dim B$. □

24. Notación: Si $f : A \to B$ es un morfismo de anillos finito, diremos que el morfismo inducido $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es finito.

25. Corolario: *Sea* $\phi : \operatorname{Spec} B \to \operatorname{Spec} A$ *un morfismo finito.*

1. *Si* $C' \subset \operatorname{Spec} B$ *es un cerrado , entonces* $\dim C' = \dim f(C')$

2. *Si* ϕ *es epiyectivo y* $C \subset \operatorname{Spec} A$ *es un cerrado, entonces* $\dim C = \dim \phi^{-1}(C)$.

Demostración. Sea $f : A \to B$ el morfismo de anillos finito tal que $f^* = \phi$.

a) Si $C' = (I')_0$, entonces $\phi(C') = (f^{-1}(I'))_0$ y el morfismo $C' \to \phi(C')$ es el morfismo inducido en espectros por el morfismo de anillos inyectivo y finito $A/f^{-1}(I') \hookrightarrow B/I'$. Luego, $\dim C' = \dim A/f^{-1}(I') = \dim B/I' = \dim \phi(C')$.

b) Si $C = (I)_0$, entonces $\phi^{-1}(C) = (f(I))_0$ y el morfismo $\phi_{|\phi^{-1}(C)} : \phi^{-1}(C) \to C$ es epiyectivo y finito (porque el morfismo $A/I \to B/(f(I))$ es finito). Entonces, $\dim \phi^{-1}(C) = \dim \phi_{|\phi^{-1}(C)}(\phi^{-1}(C)) = C$.

□

3.3. Teorema del descenso. Aplicaciones abiertas

1. Definición: Se dice que un morfismo de anillos $A \to B$ es plano, si para todo morfismo inyectivo de A-módulos $i : N \hookrightarrow M$ se cumple que el morfismo de B-módulos $N \otimes_A B \to M \otimes_A B$, $n \otimes b \mapsto i(n) \otimes b$ es inyectivo.

2. Ejemplos: Si A y B son k-álgebras, el morfismo $A \to A \otimes_k B$, $a \mapsto a \otimes 1$ es un morfismo plano: Si $N \hookrightarrow M$ es un morfismo de A-módulos entonces el morfismo de $A \otimes B$-módulos $N \otimes_A (A \otimes_k B) = N \otimes_k B \hookrightarrow M \otimes_k B = M \otimes_A (A \otimes_k B)$ es inyectivo.

Si $S \subset A$ es un sistema multiplicativo, el morfismo de localización $A \to A_S$ es plano.

3. Proposición: *La composición de morfismos planos es plano. Los morfismos planos por cambio de anillo base son planos.*

4. Proposición: *Sean $\mathscr{O}$ y $\mathscr{O}'$ dos anillos locales de ideales maximales $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente. Si $i : \mathscr{O} \to \mathscr{O}'$ es un morfismo plano tal que $i^{-1}(\mathfrak{m}') = \mathfrak{m}$, entonces la aplicación inducida $i^* : \mathrm{Spec}\mathscr{O}' \to \mathrm{Spec}\mathscr{O}$ es epiyectiva.*

Demostración. Si M es un $\mathscr{O}$-módulo no nulo entonces $M \otimes_{\mathscr{O}} \mathscr{O}'$ es no nulo: Sea $m \in M$ no nulo, entonces $\langle m \rangle \otimes_{\mathscr{O}} \mathscr{O}' \hookrightarrow M \otimes_{\mathscr{O}} \mathscr{O}'$ y basta probar que $\langle m \rangle \otimes_{\mathscr{O}} \mathscr{O}' \neq 0$. Ahora bien, $\langle m \rangle \simeq \mathscr{O}/I$ y el morfismo $\mathscr{O}/I \otimes_{\mathscr{O}} \mathscr{O}' \to \mathscr{O}/\mathfrak{m} \otimes_{\mathscr{O}} \mathscr{O}' = \mathscr{O}'/\mathfrak{m}\mathscr{O}' \neq 0$ es epiyectivo, luego $\mathscr{O}/I \otimes_{\mathscr{O}} \mathscr{O}' \neq 0$.

Dado $x \in \mathrm{Spec}\mathscr{O}$, $i^{*-1}(x) = \mathrm{Spec}\mathscr{O}_x/\mathfrak{p}_x\mathscr{O}_x \otimes_{\mathscr{O}} \mathscr{O}' \neq \emptyset$ porque $\mathscr{O}_x/\mathfrak{p}_x\mathscr{O}_x \otimes_{\mathscr{O}} \mathscr{O}' \neq 0$.

□

5. Teorema del descenso: *Sea $f : A \to B$ un morfismo de anillos plano, $\mathfrak{p}_{x'} \subset \mathfrak{p}_x$ dos ideales primos de A y $\mathfrak{p}_y \subset B$ un ideal primo tal que $f^{-1}(\mathfrak{p}_y) = \mathfrak{p}_x$. Entonces, existe un ideal primo $\mathfrak{p}_{y'} \subset \mathfrak{p}_y$ en B tal que $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$.*

Demostración. La composción de morfismos $A_{x'} \to B_{x'} \to B_{y'}$ es plana y la antimagen de $\mathfrak{p}_{y'}B_{y'}$ es $\mathfrak{p}_{x'}A_{x'}$. Por la proposición anterior, la aplicación $\mathrm{Spec}B_{y'} \to \mathrm{Spec}A_{x'}$ es epiyectiva. Luego existe un ideal primo $\mathfrak{p}_y \subset \mathfrak{p}_{y'}$ tal que $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$.

□

6. Definición: Diremos que un subconjunto irreducible Z de un espacio topológico X es casi-cerrado si existe una abierto $W \subseteq X$ tal que $\emptyset \neq W \cap \bar{Z} \subset Z$.

7. Proposición: *Si $A \to B$ es un morfismo de anillos de tipo finito (es decir, B es una A-álgebra de tipo finito), entonces el morfismo inducido en espectros $\mathrm{Spec}B \to \mathrm{Spec}A$ transforma casi-cerrados en casi-cerrados.*

Demostración. Por ser B de tipo finito sobre A, podemos factorizar $\mathrm{Spec}B \to \mathrm{Spec}A$ como la composición de una inmersión cerrada $\mathrm{Spec}B \hookrightarrow \mathbb{A}^n \times \mathrm{Spec}A$ y la proyección π natural $\mathbb{A}^n \times \mathrm{Spec}A \xrightarrow{\pi} \mathrm{Spec}A$. Como el problema es obvio para las inmersiones cerradas, basta probarlo para π. Ahora bien, podemos escribir π como composición de proyecciones desde rectas afines, así pues basta comprobar el lema para la proyección $\mathbb{A}^1 \times \mathrm{Spec}A \to \mathrm{Spec}A$, que denotaremos por f. Para probar que la imagen de un casi-cerrado Z es un casi-cerrado, podemos suponer que $\overline{f(Z)} = \mathrm{Spec}A$, sin más que considerar la proyección $\mathbb{A}^1 \times \overline{f(Z)} \to \overline{f(Z)}$. Tomando reducidos podemos suponer que A es íntegro.

En conclusión, podemos suponer que $\bar{Z} = \mathrm{Spec}B$, $\overline{f(\bar{Z})} = \overline{f(Z)} = \mathrm{Spec}A$, $B = A[x]/\mathfrak{p}$ con A y B íntegros y $A \hookrightarrow B$ inyectivo. Sea $U_b \subset \mathrm{Spec}B$ un abierto básico no vacío

incluido en Z, con $b = \sum a_i x^i$. Basta ver que $f(U_b)$ contiene un abierto no vacío. Si $\mathfrak{p} = 0$, entonces

$$f(U_b) = \{z \in \operatorname{Spec} A : z \in f(U_b)\} = \{z \in \operatorname{Spec} A : f^{-1}(z) \cap U_b \neq \emptyset\}$$
$$= \{z \in \operatorname{Spec} A : 0 \neq \bar{b} \in k(z)[x]\} = \{z \in \operatorname{Spec} A : 0 \neq \bar{a}_i \in k(z), \forall i\} = \bigcup_i U_{a_i}.$$

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 $U_a = f(f^{-1}(U_a)) \subseteq f(U_b)$.

□

8. Inducción noetheriana: *Si para demostrar cierto teorema hacemos uso de un cierto espacio topológico noetheriano $X \neq \emptyset$, y probamos que el teorema se cumple si y solo si se cumple para un cerrado $X_1 \subsetneq X$ y podemos repetir este argumento con X_1 y sucesivamente, tendremos por la noetherianidad de X, que $X_n = \emptyset$, para $n >> 0$, y solo hay que probar el teorema en este caso (que suele ser trivial). Este modo de proceder se denomina demostración por inducción noetheriana sobre X.*

9. Teorema: *Si A es un anillo noetheriano y $A \to B$ un morfismo de tipo finito plano, entonces el morfismo natural $f : \operatorname{Spec} B \to \operatorname{Spec} A$ es abierto.*

Demostración. Dado que todo abierto básico de $\operatorname{Spec} B$ vuelve a ser de tipo finito y plano sobre A, basta probar que $f(\operatorname{Spec} B)$ es un abierto. Más aún, basta probar que $f(\operatorname{Spec} B)$ contiene un abierto U, porque por inducción noetheriana $f(f^{-1}(U^c))$ será un abierto de $U^c := (\operatorname{Spec} A) \backslash U$ y por tanto $f(\operatorname{Spec} B)$ también. Tomando las componentes irreducibles de $\operatorname{Spec} A$ y sus antimágenes por f, podemos reducirnos al caso en que $\operatorname{Spec} A$ es irreducible. Por la proposición anterior $f(\operatorname{Spec} B)$ es unión de un número finito de casi-cerrados, luego basta ver que es denso en $\operatorname{Spec} A$. Por el teorema del descenso la imagen de los puntos genéricos de $\operatorname{Spec} B$ son el punto genérico de $\operatorname{Spec} A$.

□

3.4. Lema de Normalización de Noether

1. Definiciones: Diremos que $\operatorname{Spec} A$ es una variedad algebraica (afín) sobre un cuerpo k, si A es una k-álgebra de tipo finito. 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.

2. Ejemplo: La variedad algebraica $\mathbb{A}^n := \operatorname{Spec} k[x_1,\dots,x_n]$ se dice que es el espacio afín (n-dimensional). Si A es una k-álgebra de tipo finito, entonces $A \simeq k[x_1,\dots,x_n]/I$ y la variedad algebraica $\operatorname{Spec} A$ es isomorfa a la subvariedad algebraica del espacio afín $\operatorname{Spec} k[x_1,\dots,x_n]/I = (I)_0 \subset \mathbb{A}^n$.

3. Lema de normalización de Noether: *Sea $A = k[\xi_1,\dots,\xi_n]$ una k-álgebra de tipo finito. Existe un morfismo finito e inyectivo*

$$k[x_1,\dots,x_r] \hookrightarrow A \qquad\qquad (\textit{con } r \le n).$$

"Toda variedad algebraica afín se proyecta con fibras finitas en un espacio afín".

Demostración. Vamos a hacerlo por inducción sobre n. Para $n = 0$, $k = A$ (y $r = 0$). Supongamos que el teorema es cierto hasta $n-1$.

Si los $\{\xi_i\}$ son algebraicamente independientes entre sí, entonces $k[\xi_1,\dots,\xi_n] = k[x_1,\dots,x_n]$. Podemos suponer que existe $p(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$, no nulo, tal que $p(\xi_1,\dots,\xi_n) = 0$. Si $p(\xi_1,\dots,\xi_{n-1},x)$ fuese un polinomio mónico (por un $\lambda \in k$ no nulo), entonces ξ_n sería entero sobre $k[\xi_1,\dots,\xi_{n-1}]$. Concluiríamos porque por la hipótesis de inducción, existe un morfismo finito e inyectivo $k[x_1,\dots,x_r] \hookrightarrow k[\xi_1,\dots,\xi_{n-1}]$ (con $r \le n-1$) y la composición de morfismos finitos

$$k[x_1,\dots,x_r] \overset{\text{finito}}{\hookrightarrow} k[\xi_1,\dots,\xi_{n-1}] \overset{\text{finito}}{\hookrightarrow} k[\xi_1,\dots,\xi_{n-1},\xi_n]$$

es un morfismo finito.

Veamos que mediante un cambio de variables estamos en la situación anterior. Consideremos el orden lexicográfico en $\mathbb{N}^n$, es decir, $\alpha > \beta$, si existe i tal que $\alpha_1 = \beta_1,\dots,\alpha_{i-1} = \beta_{i-1}$ y $\alpha_i > \beta_i$. Escribamos $p(x_1,\dots,x_n) = \lambda_\alpha \cdot x^\alpha + \sum_{\beta<\alpha} \lambda_\beta x^\beta$ (con $\lambda_\alpha \neq 0$). Consideremos el cambio de coordenadas $x_1' = x_1 - x_n^{d_1}$, $\dots$, $x_{n-1}' = x_{n-1} - x_n^{d_{n-1}}$, $x_n' = x_n$, con $d_1 \gg d_2 \gg \cdots \gg d_{n-1}$. Sea $m = d_1\alpha_1 + \cdots + d_{n-1}\alpha_{n-1} + \alpha_n$. Entonces,

$$\begin{aligned} q(x_1',\dots,x_n') := p(x_1,\dots,x_n) &= p(x_1' + x_n'^{d_1},\dots,x_{n-1}' + x_n'^{d_{n-1}},x_n') \\ &= \lambda_\alpha \cdot x_n'^m + \sum_{i<m} q_i(x_1',\dots,x_{n-1}')x_n'^i. \end{aligned}$$

Sean $\xi_i' = \xi_i - \xi_n^{d_i}$, para $i < n$ y $\xi_n' = \xi_n$. Entonces, $q(\xi_1',\dots,\xi_{n-1}',\xi_n') = p(\xi_1,\dots,\xi_n) = 0$ y $q(\xi_1',\dots,\xi_{n-1}',x)$ es un polinomio mónico (por λ_α. Por tanto, existe un morfismo finito $k[x_1,\dots,x_r] \hookrightarrow k[\xi_1',\dots,\xi_{n-1}',\xi_n'] = k[\xi_1,\dots,\xi_{n-1},\xi_n]$

□

4. Observación: En la demostración hemos probado que si $\xi_1,\dots,\xi_n$ no son algebraicamente independientes, entonces $r \le n-1$.

3.4.1. Teorema de los ceros de Hilbert

5. Forma débil del teorema los ceros de Hilbert: *Sea A una k-álgebra de tipo finito. Si $\mathfrak{m} \subset A$ es 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 la proposición 3.2.23, $k[x_1,\dots,x_r]$ ha de tener dimensión de Krull cero, luego $r = 0$ y $\dim_k A/\mathfrak{m} < \infty$. □

6. Ejemplo: Sea k un cuerpo algebraicamente cerrado y

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

un sistema de ecuaciones k-algebraicas. Sea $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$. El conjunto de soluciones del sistema se identifica con $\mathrm{Spec}_{rac} A = \mathrm{Spec}_{max} A$. Por lo tanto el sistema de ecuaciones no tiene soluciones si y solo si $\mathrm{Spec}_{max} A = \emptyset$, es decir, $A = 0$, que equivale a decir que $(p_1,\dots,p_r) = k[x_1,\dots,x_n]$, es decir, $1 \in (p_1,\dots,p_r)$.

7. Ejemplo: Sean $X = \mathrm{Spec}\, A$ y $Y = \mathrm{Spec}\, B$ dos variedades algebraicas sobre un cuerpo algebraicamente cerrado k. Definamos $X \times_k Y := \mathrm{Spec}(A \otimes_k B)$. El conjunto de los puntos cerrados de $X \times_k Y$ es igual al producto cartesiano del conjunto de los puntos cerrados de X y del conjunto de los puntos cerrados de Y:

$$\mathrm{Spec}_{max}(A \otimes_k B) = \mathrm{Spec}_{rac}(A \otimes_k B) = \mathrm{Spec}_{rac} A \times \mathrm{Spec}_{rac} B = \mathrm{Spec}_{max} A \times \mathrm{Spec}_{max} B.$$

8. Teorema: *Sea $\bar{k}$ el cierre algebraico de k. Dados $\alpha = (\alpha_1,\dots,\alpha_n), \beta = (\beta_1,\dots,\beta_n) \in \bar{k}^n$, diremos que $\alpha \sim \beta$ si existe $\tau \in \mathrm{Aut}_{k-alg}(\bar{k})$, tal que $\beta = \tau(\alpha) := (\tau(\alpha_1),\dots,\tau(\alpha_n))$. Entonces, la aplicación*

$$\begin{array}{rcl} \left\{ \alpha \in \bar{k}^n : \begin{array}{c} p_1(\alpha) = 0 \\ \cdots \\ p_r(\alpha) = 0 \end{array} \right\} \Big/ \sim & \longrightarrow & \mathrm{Spec}_{max}\, k[x_1,\dots,x_n]/(p_1,\dots,p_r) \\ [\alpha] & \longmapsto & \mathfrak{m}_{[\alpha]} := \{\overline{p(x)} : p(\alpha) = 0\} \end{array}$$

es biyectiva.

Demostración. Denotemos $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$. Observemos que $\mathfrak{m}_{[\alpha]}$ es maximal ya que el morfismo $A/\mathfrak{m}_{[\alpha]} \hookrightarrow \bar{k}$, $\overline{p(x)} \mapsto p(\alpha)$ es inyectivo, luego $A/\mathfrak{m}_{[\alpha]}$ es una k-álgebra de tipo finito y algebraica, luego es una k-álgebra finita íntegra, por tanto es un cuerpo.

Dado un ideal maximal $\mathfrak{m}$ de A, sabemos que $A/\mathfrak{m}$ es una k-extensión finita de k, luego existe un morfismo inyectivo de k-álgebras $A/\mathfrak{m} \hookrightarrow \bar{k}$ (pensémoslo como una inclusión) , único salvo automorfismos de k-álgebras de $\bar{k}$. Sea $\alpha_i = \bar{x}_i \in \bar{k}$, para cada i. Evidentemente, $p_j(\alpha) = \overline{p_j(x)} = 0$, para todo j. La aplicación inversa es la que asigna a $\mathfrak{m}$ la clase de equivalencia $[(\alpha_1,\dots,\alpha_n)]$. □

9. 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. □

10. Corolario : *Los puntos cerrados de un abierto de una variedad algebraica son puntos cerrados en la variedad algebraica.*

Demostración. Sea $X = \operatorname{Spec} A$ la variedad algebraica. Todo abierto es unión de abiertos básicos, luego basta probar el enunciado para un abierto básico $U_a \subset X$. Ahora bien, como A es una k-álgebra de tipo finito entonces $A_a = A[\frac{1}{a}]$ es una k-álgebra de tipo finito. Luego $U_a = \operatorname{Spec} A_a$ es una variedad algebraica. Se concluye por la proposición anterior aplicada a la inclusión $U_a \hookrightarrow X$. □

11. Corolario : *Sea* $\operatorname{Spec} A$ *una k-variedad algebraica y consideremos el subespacio* $\operatorname{Spec}_{max} A \subset \operatorname{Spec} A$. *Entonces, las aplicaciones*

$$\begin{array}{ccc} \textit{Conjunto de cerrados de } \operatorname{Spec} A & \longleftrightarrow & \textit{Conjunto de cerrados de } \operatorname{Spec}_{max} A \\ C & \longmapsto & C \cap \operatorname{Spec}_{max} A \\ \overline{D} & \longleftarrow\!\shortmid & D \end{array}$$

son inversas entre sí. En particular, si k es algebraicamente cerrado, las aplicaciones

$$\begin{array}{ccc} \textit{Conjunto de cerrados de } \operatorname{Spec} A & \longleftrightarrow & \textit{Conjunto de cerrados de } \operatorname{Spec}_{rac} A \\ C & \longmapsto & C \cap \operatorname{Spec}_{rac} A \\ \overline{D} & \longleftarrow\!\shortmid & D \end{array}$$

son inversas entre sí.

Demostración. Si U es un abierto no vacío de una variedad algebraica afín X, entonces contiene puntos cerrados: En efecto, sea $U_a \subset U$ un abierto básico no vacío. U_a contiene puntos cerrados (toda variedad algebraica afín tiene puntos cerrados, pues en todo anillo no nulo hay ideales maximales), que son cerrados en X, luego en U.

Dados dos cerrados distintos $C_1, C_2 \subset \operatorname{Spec} A$, tendremos que $C_1 \not\subset C_2$ o $C_2 \not\subset C_1$. Supongamos el primer caso. Entonces, $C_1 \cap C_2^c$ es un abierto no vacío de C_1 luego contiene un punto cerrado, que es un punto cerrado de C_1 que no está en C_2. En conclusión la asignación $C \mapsto C \cap \operatorname{Spec}_{max} A$ es inyectiva.

Si $Y \subset X$ es un subespacio topológico y $D \subset Y$ es un cerrado de Y, entonces $D = \overline{D} \cap X$. Luego, la composición $D \mapsto \overline{D} \mapsto C \cap \operatorname{Spec}_{max} A$ es la identidad. En particular, la asignación $C \mapsto C \cap \operatorname{Spec}_{max} A$ es epiyectiva, luego biyectiva y ambas asignaciones son inversas entre sí.

□

12. Consecuencias: Sean $C, C' \subset \operatorname{Spec} A$ dos subvariedades algebraicas. $C \subset C'$ si y solo si $C \cap \operatorname{Spec}_{max} A \subset C' \cap \operatorname{Spec}_{max} A$ y $C \neq C'$ si y solo si $C \cap \operatorname{Spec}_{max} A \neq C' \cap \operatorname{Spec}_{max} A$ C es irreducible si y solo si $C \cap \operatorname{Spec}_{max} A$ es irreducible.

13. Ejercicio: Prueba que el ideal de la funciones que se anulan en C coincide con el ideal de las funciones que se anulan en $C \cap \operatorname{Spec}_{max} A$.

14. Definición: Diremos que $X = \operatorname{Spec} A$ es íntegro si A es un anillo íntegro. Diremos que $X = \operatorname{Spec} A$ es reducido si A es un anillo reducido.

15. Forma fuerte del teorema 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. Si $(f)_0^{max} = \operatorname{Spec}_{max} A$, entonces $(f)_0 = \operatorname{Spec} A$, luego f es nilpotente.

□

16. De nuevo, también estamos diciendo que todo punto cerrado x de una variedad algebraica $\operatorname{Spec} A$ sobre un cuerpo algebraicamente cerrado es racional. En efecto, $\bar{1} \in A/\mathfrak{m}_x$ es nulo si es nulo en todos los puntos racionales de $\operatorname{Spec} A/\mathfrak{m}_x = \{x\}$, como $\bar{1} \neq 0$, en $\{x\}$ han de existir puntos racionales, es decir, x ha de ser racional.

3.5. Dimensión de una variedad algebraica

1. Teorema: *La dimensión de Krull de $k[x_1,\dots,x_n]$ es n.*

Demostración. Procedamos por inducción sobre n. El caso $n=1$ es obvio.
Sea

$$0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$$

una cadena de ideales primos de $k[x_1,\dots,x_n]$. Sea $p \in \mathfrak{p}_1$, no nulo e irreducible. Como $k[x_1,\dots,x_n]$ es un dominio de factorización única, el ideal (p) es un ideal primo. Si $(p) \neq \mathfrak{p}_1$, lo añadimos a la cadena anterior, con lo que podemos suponer que $(p) = \mathfrak{p}_1$. Por el lema de normalización de Noether y la observación 3.4.4, existe un morfismo finito inyectivo $k[x_1,\dots,x_r] \hookrightarrow k[x_1,\dots,x_n]/(p)$, con $r < n$. Por la hipótesis de inducción, $\dim k[x_1,\dots,x_r] = r$, luego la longitud de las cadenas de ideales primos de $k[x_1,\dots,x_n]/(p)$ es menor o igual que $r \leq n-1$. Haciendo cociente por (p), la cadena anterior define una cadena de ideales primos en $A/(p)$

$$\bar{0} = \bar{\mathfrak{p}}_1 \subset \bar{\mathfrak{p}}_2 \subset \cdots \subset \bar{\mathfrak{p}}_m$$

luego $m-1 \leq n-1$ y $\dim k[x_1,\dots,x_n] \leq n$. Por otra parte,

$$0 \subset (x_1) \subset (x_1,x_2) \subset \cdots \subset (x_1,\dots,x_n)$$

es una cadena de longitud n, luego $\dim k[x_1,\dots,x_n] \geq n$. En conclusión $k[x_1,\dots,x_n]$ tiene dimensión de Krull n. □

2. Teorema: *Sea A una k-álgebra de tipo finito íntegra. La dimensión de Krull de A coincide con el grado de trascendencia de su cuerpo de fracciones.*

Demostración. Por el lema de normalización de Noether, existe un morfismo finito inyectivo $k[x_1,\dots,x_n] \hookrightarrow A$, que induce un morfismo finito entre sus cuerpos de fracciones (pruébese)

$$k(x_1,\dots,x_n) \hookrightarrow \Sigma$$

Luego

$$\dim A \overset{3.2.23}{=} \dim k[x_1,\dots,x_n] = n = \operatorname{gr}\operatorname{tr} k(x_1,\dots,x_n) = \operatorname{gr}\operatorname{tr}\Sigma.$$

□

3. Proposición: *Sea X una variedad algebraica afín irreducible y $U \subset X$ un abierto no vacío. Entonces,* $\dim U = \dim X$.

Demostración. Si $V \subset V'$ es una inclusión de abiertos, entonces $\dim V \leq \dim V'$. Podemos suponer que $X = \operatorname{Spec} A$ es una variedad íntegra. Sea $U_a \subset U$ un abierto básico, no vacío. La dimensión de $U_a = \operatorname{Spec} A_a$ coincide con la de $X = \operatorname{Spec} A$, porque el cuerpo de fracciones de A_a es igual al de A. Como $\dim U_a \leq \dim U \leq \dim X$, todos los $\leq$ son igualdades. □

En general, toda variedad algebraica es unión de variedades algebraicas irreducibles y la dimensión de la variedad es el máximo de las dimensiones de sus componentes irreducibles. Observemos que $\dim A = \dim A_{\mathrm{red}}$. Por tanto, la dimensión de una variedad irreducible $\operatorname{Spec} A$ coincide con la dimensión de $\operatorname{Spec} A_{\mathrm{red}}$, que es una variedad algebraica íntegra.

4. Proposición: *Sean $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $X \times_k Y := \operatorname{Spec}(A \otimes_k B)$ variedades algebraicas. Se cumple que*

$$\dim(X \times_k Y) = \dim X + \dim Y$$

Demostración. Sean $f : k[x_1, \ldots, x_n] \hookrightarrow A$, $g : k[y_1, \ldots, y_m] \hookrightarrow B$ morfismos finitos inyectivos, entonces

$$\begin{array}{rcl} k[x_1, \ldots, x_n, y_1, \ldots, y_m] = k[x_1, \ldots, x_n] \otimes k[y_1, \ldots, y_m] & \to & A \otimes B \\ p(x) \otimes q(y) & \mapsto & f(p(x)) \otimes g(q(y)) \end{array}$$

es un morfismo inyectivo finito y $\dim X + \dim Y = n + m = \dim(X \times Y)$.

□

5. Proposición: *Sea $f : X \to Y$ un morfismo entre variedades algebraicas. Sea $C \subset X$ un cerrado. Se cumple que*

$$\dim C \geq \dim \overline{f(C)}.$$

Demostración. Podemos suponer que C es irreducible. Denotemos $X = \operatorname{Spec} B$, $C = (\mathfrak{p})_0 = \operatorname{Spec} B/\mathfrak{p}$, $Y = \operatorname{Spec} A$ y $\phi : A \to B$ el morfismo de k-álgebras tal que $\phi^* = f$. Entonces, el morfismo $A/\phi^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p}$ es inyectivo y $\overline{f(C)} = (\phi^{-1}(\mathfrak{p}))_0 = \operatorname{Spec} A/\phi^{-1}(\mathfrak{p})$. El cuerpo de fracciones de $A/\phi^{-1}(\mathfrak{p})$ está incluido en el cuerpo de fracciones de $B/\mathfrak{p}$, luego el grado de trascendencia del primero es menor o igual que el del segundo y $\dim \overline{f(C)} \leq \dim C$. □

3.5.1. Teorema del ideal principal de Krull

Probemos que las hipersuperficies de una variedad algebraica son de codimensión 1.

6. Teorema del ideal principal de Krull: *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra y $f \in A$, 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 $f = p_1 \cdot \ldots \cdot p_s$ 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 funciones de $k[x_1,\dots,x_n]/(p_i)$ es $n-1$, luego $\dim(p_i)_0 = n-1$.

Escribamos $(f)_0 = C_1 \cup \cdots \cup C_s$ como unión de componentes irreducibles. Sea $y \in C_1 - (C_2 \cup \cdots \cup C_s)$ un punto cerrado. Sea $U_a = \operatorname{Spec} A_a$ un abierto básico que contenga a y disjunto con los C_i, para $i > 1$. Por 3.5.2, $\dim X = \dim U_a$ y $\dim C_1 = \dim C_1 \cap U_a$. Ahora bien, $C_1 \cap U_a$ coincide con los ceros de f en U_a. En conclusión, sustituyendo X por U_a, podemos suponer que $(f)_0 = C_1$.

Por el lema de normalización de Noether sabemos que existe 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, $i^{*-1}((f)_0) = (f)_0$, por tanto la dimensión de $(f)_0$ en $\operatorname{Spec} k[x_1,\dots,x_n][f]$ es la misma que la de $(f)_0$ en $\operatorname{Spec} A$. Por tanto, podemos suponer que $A = k[x_1,\dots,x_n][f]$.

Sea $p(x_1,\dots,x_n,x_{n+1})$ un polinomio irreducible tal que $p(x_1,\dots,x_n,f) = 0$. El epimorfismo

$$k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1})) \to k[x_1,\dots,x_n][f],\ \bar{x}_{n+1} \mapsto f$$

es un isomorfismo, porque $k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}))$ es un anillo de dimensión n, íntegro y si hubiese núcleo la dimensión de $k[x_1,\dots,x_n][f]$ sería menor que n.

En conclusión $A = k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}))$ y $f = x_{n+1}$. Por tanto,

$$\begin{aligned}\dim(f)_0 &= \dim A/(f) = \dim k[x_1,\dots,x_{n+1}]/(p(x_1,\dots,x_n,x_{n+1}),x_{n+1}) \\ &= \dim k[x_1,\dots,x_n]/(p(x_1,\dots,x_n,0)) = n-1.\end{aligned}$$

□

7. Definición: Una cadena de cerrados irreducibles (resp. con extremos prefijados) diremos que es maximal si no está incluida en ninguna otra mayor (resp. con los mismos extremos).

8. Corolario: *Todas las cadenas maximales de cerrados irreducibles de una variedad algebraica irreducible tienen la misma longitud, que es la dimensión de Krull de la variedad.*

Demostración. Sea $X = \operatorname{Spec} A$ la variedad algebraica irreducible. Podemos suponer que la variedad algebraica es íntegra ya que $\operatorname{Spec} A = \operatorname{Spec} A_{\mathrm{red}}$. 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 $\dim X_1 = \dim X - 1$, luego por inducción sobre la dimensión $m - 1 = \dim X_1 = \dim X - 1$, y por tanto $m = \dim X$. □

9. Definición: Se dice que una variedad algebraica es catenaria si todas las cadenas maximales de cerrados irreducibles con extremos cualesquiera prefijados tienen la misma longitud.

10. Corolario: *Las variedades algebraicas son catenarias.*

Demostración. Sean $Y \supset Y'$ cerrados irreducibles de una variedad algebraica X. Toda cadena maximal de extremos Y 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. □

11. Proposición: *Si $X = \operatorname{Spec} A$ es una variedad algebraica irreducible y $x \in X$ un punto cerrado, entonces* $\dim X = \dim A_x$.

Demostración. La dimensión de Krull de A_x coincide con la longitud de las cadenas maximales de cerrados irreducibles de X que pasan por x. Ahora bien, todas las cadenas maximales de cerrados irreducibles tienen longitud $\dim X$.

□

12. Proposición: *Sea $X = \operatorname{Spec} A$ una variedad algebraica irreducible de dimensión n e $Y \subset X$ una subvariedad algebraica irreducible de dimensión m. El número mínimo r para el cual existen r funciones $f_1, \ldots f_r$ de X tales que una de las componentes irreducibles de $(f_1, \ldots, f_r)_0$ sea Y es $r = n - m$ (puede imponerse además que todas las componentes sean de dimensión m).*

Demostración. Es fácil probar, aplicando recurrentemente el teorema del ideal principal de Krull, que todas las componentes irreducibles de $(f_1,\dots,f_r)_0$ 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 $m=n-1$, entonces unas de los C_i ha de coincidir con Y y 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.

□

13. Corolario: *Sea X una variedad algebraica irreducible de dimensión n y $x\in X$ un punto cerrado. El número mínimo de funciones $f_1,\dots,f_r$ tales que $(f_1,\dots,f_r)_0\cap U=\{x\}$, en algún entorno abierto U de x, es $r=n$.*

14. Corolario: *Sea X una variedad algebraica irreducible, $f\colon X\to Y$ un morfismo entre variedades algebraicas. Si $y\in f(X)$ es un punto cerrado, entonces*

$$\dim f^{-1}(y)\geq \dim X-\dim \overline{f(X)}$$

Demostración. Podemos suponer que $\overline{f(X)}=Y$ y que X e Y son variedades algebraicas íntegras.. Tomando en vez de Y un abierto básico que contenga a $f(x)$, podemos suponer que existen $g_1,\dots,g_n$ funciones de Y tales que $(g_1,\dots,g_n)_0=\{f(x)\}$ y $n=\dim Y$. Entonces, $f^{-1}(y)=(g_1\circ f,\dots,g_n\circ f)_0$ y por el teorema del ideal principal de Krull $\dim f^{-1}(y)\geq \dim X-n=\dim X-\dim Y$. □

3.5.2. Variedades algebraicas de dimensión cero

15. Sea $X=\operatorname{Spec}A$ una variedad algebraica de dimensión cero. Por el lema de normalización de Noether y la proposición 3.2.23, existe un morfismo finito $k\hookrightarrow A$. Por lo tanto, $\dim_k A<\infty$. Tenemos que $\operatorname{Spec}A=\{x_1,\dots,x_n\}$, donde los x_i son puntos cerrados. El morfismo $A\to A_{x_1}\times\cdots\times A_{x_n}$, $a\mapsto(\frac{a}{1},\dots,\frac{a}{1})$ es un isomorfismo porque lo es al localizar en todo punto. Por lo tanto,

$$\dim_k A=\sum_{x\in X}\dim_k A_x.$$

Diremos que el número de puntos de X, contando grados y multiplicidades, que denotaremos (X) es

$$(X) := \dim_k A$$

Número que no varía por cambio de cuerpo base.

16. Se llama grado de x a $\dim_k A/\mathfrak{m}_x$ y lo denotaremos $\mathrm{gr}_k\, x$. Diremos que $\frac{\dim_k A_x}{\dim_k A/\mathfrak{m}_x}$[2] es la multiplicidad con la que aparece x en X y lo denotaremos $m_x(X)$. En conclusión,

$$(X) = \dim_k A = \sum_{x\in X} \dim_k A_x = \sum_{x\in X} \mathrm{gr}_k\, x \cdot m_x(X).$$

Si $X = \mathrm{Spec}\, A/I, Y = \mathrm{Spec}\, A/J$ son subvariedades cerradas de $Z = \mathrm{Spec}\, A$ y $x \in X \cap Y$ es un punto aislado de $X \cap Y$, diremos que $(X \cap Y)_x = \dim_k (A/I + J)_x$ es la multiplicidad de intersección en x de X e Y.

17. Ejemplo: $X = \mathrm{Spec}\, \mathbb{R}[x]/(x^2(x-1)(x^2+1)^2 = \{\mathfrak{m}_{z_0} := (\bar{x}), \mathfrak{m}_{z_1} := (\bar{x}-1), \mathfrak{m}_{z_{\pm i}} := (\bar{x}^2+1)\}$ tiene tres puntos. Denotemos $A = \mathbb{R}[x]/(x^2(x-1)(x^2+1)^2)$. Observemos que $\dim_{\mathbb{R}} A = 7$ y

$$\begin{array}{l} \dim_{\mathbb{R}} A_{z_0} = \dim_{\mathbb{R}} (\mathbb{R}[x]/(x^2))_{z_0} = \dim_{\mathbb{R}} (\mathbb{R}[x]/(x^2)) = 2 \text{ y } \dim_{\mathbb{R}} A/\mathfrak{m}_{z_0} = \dim_{\mathbb{R}} \mathbb{R}[x]/(x) = 1. \\ \dim_{\mathbb{R}} A_{z_1} = \dim_{\mathbb{R}} (\mathbb{R}[x]/(x-1)) = 1 \text{ y } \dim_{\mathbb{R}} A/\mathfrak{m}_{z_1} = \dim_{\mathbb{R}} \mathbb{R}[x]/(x-1) = 1. \\ \dim_{\mathbb{R}} A_{z_{\pm i}} = \dim_{\mathbb{R}} \mathbb{R}[x]/((x^2+1)^2) = 4 \text{ y } \dim_{\mathbb{R}} A/\mathfrak{m}_{z_{\pm i}} = \dim_{\mathbb{R}} \mathbb{R}[x]/(x^2+1) = 2. \end{array}$$

y $(X) = 7 = 1\cdot 2 + 1\cdot 1 + 2\cdot 2$.

18. Proposición: *Sea $\pi\colon \mathrm{Spec}\, A \to \mathrm{Spec}\, B$ un morfismo finito y supongamos A íntegro y B es un dominio de ideales principales. El número de puntos (contando grados y multiplicidades) de las fibras de π es constante.*

Demostración. Dado $z \in \mathrm{Spec}\, B$, denotaremos "el cuerpo residual de z" $k(z) := B_z/\mathfrak{p}_z B_z$. Nos piden que probemos que el número de puntos de $\pi^{-1}(z) = \mathrm{Spec}\, A_z/\mathfrak{p}_z A_z$ es constante, es decir, $\dim_{k(z)} A_z/\mathfrak{p}_z A_z$ no depende de z. A es un B-módulo finito generado sin torsión, ya que A es íntegro. Por tanto, A es un B-módulo libre, $A \simeq B \oplus \overset{n}{\cdots} \oplus B$. Sea $g \in \mathrm{Spec}\, B$ el punto genérico, entonces $A_g = B_g \oplus \overset{n}{\cdots} \oplus B_g$ y el número de puntos de $\pi^{-1}(g) = n$. Sea $z \in \mathrm{Spec}\, B$ un punto cerrado, entonces $A/\mathfrak{m}_z A = k(z) \oplus \cdots \oplus k(z)$ y y el número de puntos de $\pi^{-1}(z$ es n. □

[2] Si K es una k-extensión de cuerpos y E un K espacio vectorial de dimensión n, entonces $\dim_k E = \dim_k (K \oplus \overset{n}{\cdots} \oplus K) = \dim_k K \cdot n = \dim_k K \cdot \dim_K E$. Sea n tal que $\mathfrak{m}_x^n A_x = 0$. Consideremos la cadena de inclusiones

$$0 = \mathfrak{m}_x^n A_x \subset \mathfrak{m}_x^{n-1} A_x \subset \cdots \subset \mathfrak{m}_x A_x \subset A_x$$

Entonces, $\dim_k A_x = \sum_{i=0}^{n-1} \dim_k \mathfrak{m}_x^i A_x/\mathfrak{m}_x^{i+1} A_x = \dim_k A/\mathfrak{m}_x \cdot \sum_{i=0}^{n-1} \dim_{A/\mathfrak{m}_x} \mathfrak{m}_x^i A_x/\mathfrak{m}_x^{i+1} A_x$, luego $\dim_k A/\mathfrak{m}_x$ divide a $\dim_k A_x$.

19. Ejemplo: Sea $p(x,y) = p_n(x)y^n + p_{n-1}(x)y^{n-1} + \cdots + p_0(x)$, donde $p_n(x) \neq 0$. El morfismo de anillos $\mathbb{C}[x] \to \mathbb{C}[x,y]/(p(x,y))$, $q(x) \mapsto \overline{q(x)}$ es finito si y solo si $\operatorname{gr} p_n(x) = 0$: Si $\operatorname{gr} p_n(x) = 0$, entonces el morfismo es finito. Si $\operatorname{gr}(p(x) \neq 0$ y α es una raíz de $p(x)$ y $\mathfrak{m}_\alpha = (x-\alpha)$, entonces el número de puntos (contando multiplicidades) de $i^{*-1}(\alpha)$ es igual a $\dim_{\mathbb{C}} \mathbb{C}[y]/(p(\alpha,y)) < n$ y si α no es raíz de $p_n(x)$ el número de puntos (contando multiplicidades) de $i^{*-1}(\alpha)$ es igual a $\dim_{\mathbb{C}} \mathbb{C}[y]/(p(\alpha,y)) = n$. Luego, el morfismo no puede ser finito.

20. Intersección de curvas planas: Sean $p, q, q' \in k[x,y]$ y supongamos que $C = (p)_0$ no tiene componentes comunes con $D = (q)_0$ y $D' = (q')_0$; y sea $D \cup D' = (qq')_0$. Entonces,

$$\boxed{(C \cap [D \cup D']) = (C,D) + (C,D')}$$

Es decir, $\dim_k k[x,y]/(p,qq') = \dim_k k[x,y]/(p,q) + \dim_k k[x,y]/(p,q')$. En efecto, si $E' \subset E$ es una inclusión de espacios vectoriales, sabemos que $\dim_k E/E'$ es igual a la longitud de las cadenas de subespacios vectoriales de E/E' irrefinables, que coincide con la longitud de las cadenas de subespacios vectoriales de E irrefinables cuyo primer eslabón es E' y cuyo último eslabón es E. De la composición de los morfismos inyectivos

$$k[x,y]/(p) \xrightarrow{q\cdot} k[x,y]/(p) \xrightarrow{q'\cdot} k[x,y]/(p)$$

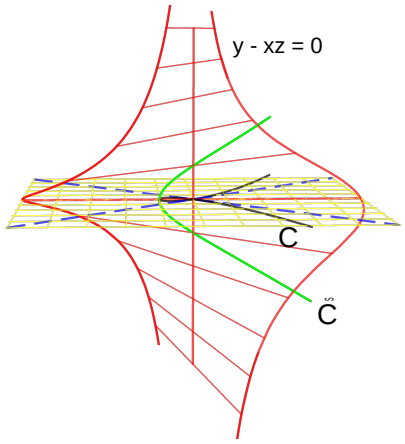
se deduce que $\dim_k k[x,y]/(p,qq') = \dim_k k[x,y]/(p,q) + \dim_k k[x,y]/(p,q')$.

Si z es un punto cerrado de C, igualmente $(C \cap [D \cup D'])_z = (C,D)_z + (C,D')_z$.

Consideremos las superficies $(y - xz)_0$ y $(z)_0$ de $\mathbb{A}^3$ y el morfismo $\pi\colon (y-xz)_0 \to (z)_0$, $(\alpha,\beta,\gamma) \mapsto (\alpha,\beta,0)$, que es el morfismo inducido por el morfismo de anillos

$$\begin{array}{ccc} k[x,y] = k[x,y,z]/(z) & \longrightarrow & k[x,y,z]/(y-xz) = k[x,y/x] \\ x \equiv\!\!= \bar{x} & \longmapsto & \bar{x} \equiv\!\!= x \\ y \equiv\!\!= \bar{y} & \longmapsto & \bar{y} \equiv\!\!= x \cdot \frac{y}{x} \end{array}$$

Observemos que $\pi^{-1}((0,0,0))$ es igual al conjunto de los puntos cerrados de la recta recta $(x,y)_0$. Además, $(y-xz)_0 - (x,y)_0 \xrightarrow{\pi} (z)_0 - \{(0,0,0)\}$ es un homeomorfismo y $\overline{\pi^{-1}((y-\lambda x)_0 - \{(0,0,0)\})}$ es igual a la recta $(y - \lambda x, z - \lambda)_0$.



Escribamos $p(x,y) = p_m(x,y) + \cdots + p_{m+r}(x,y)$ y supongamos que es un polinomio irreducible y que x no divide a $p_m(x,y)$, "$x=0$ corta transversalmente a C en el origen".
Sea $\mathfrak{m}_{or} = (\bar{x},\bar{y})$ y $A = (k[x,y]/(p(x,y))_{or}$. El morfismo $i\colon A \hookrightarrow A[y/x]$ es un morfismo finito y $\dim_k A[y/x]/A < \infty$: Escribamos $p_m(x,y) = \sum_{i=0}^{m} a_i x^{m-i} y^i$ $(a_m \neq 0)$. Entonces,

$$\frac{p_m(x,y)}{x^m} = a_m(\frac{y}{x})^m + \cdots + a_0.$$

Para $r + r' > m$,

$$\frac{y^r x^{r'}}{x^m} = \begin{cases} (\frac{y}{x})^m y^{r-m} x^{r'}, \text{ si } r \geq m. \\ (\frac{y}{x})^r x^{r+r'-m}, \text{ si } r \leq m. \end{cases}$$

$\frac{p(x,y)}{x^m} = (a_m + b_0)(\frac{y}{x})^m + b_1(\frac{y}{x})^{m-1} + \cdots + b_m$, con $b_i \in A$ y $b_0 \in (\bar{x},\bar{y})$. Por tanto, $a_m + b_0 \in A$ es invertible y $A[y/x]$ es un A-módulo generado por $\{1, y/x, \ldots, (y/x)^{m-1}\}$. Además, $x^m \cdot A[y/x] \subset A$, por lo tanto, $A[y/x]/A$ es un $A/(x^m)$-módulo finito, y como $\dim_k A/(x^m) < \infty$ entonces $\dim_k A[y/x]/A < \infty$.

Sea $p_m = f_1^{n_1} \cdots f_s^{n_s}$ la descomposición de p_m en producto de potencias de irreducibles. Diremos que $f_i = 0$ son las tangentes a C en or. Observemos que $\frac{p(x,y)}{x^m} = p_m(1,y/x) + x p_{m+1}(x,y/x) + \cdots + x p_{m+n}(x,y/x) x^n$, entonces

$$i^{*-1}(or) = \operatorname{Spec} A[y/x]/(x,y) = \operatorname{Spec} A[y/x]/(x) = \operatorname{Spec} k[y/x]/(p_m(1,y/x))$$
$$= \{\mathfrak{m}_{t_1} = (x, f_1(1,\frac{y}{x})), \ldots, \mathfrak{m}_{t_s} = (x, f_s(1,\frac{y}{x}))\}$$

Además, $(C \cap \{x=0\})_{or} = \dim_k(k[x,y]/(p,x))_{or} = \dim_k(k[y]/(p_m(0,y) + \cdots + p_{m+r}(0,y))_{or} = m$.

Sea $\tilde{p}(x,y/x) := p(x,y)/x^n$, entonces $A[y/x]$ es isomorfo a $k[x,y/x]/(\tilde{p}(x,y/x))$ localizado en $\{t_1,\ldots,t_s\}$. Escribiremos $\tilde{C} = \operatorname{Spec} k[x,y/x]/(\tilde{p}(x,y/x))$.

Sea $q(x,y) = q_n(x,y) + \cdots + p_{n+u}(x,y) \in k[x,y]$. Probemos que

$$\boxed{(C \cap D)_{or} = mn + \sum_i (\tilde{C} \cap \tilde{D})_{t_i}}$$

Probemos primero que $\dim_k A/(q) = \dim_k A[y/x]/(q)$: Del diagrama conmutativo

$$\begin{array}{ccc} A & \hookrightarrow & A[y/x] \\ {\scriptstyle q\cdot}\downarrow & & \downarrow{\scriptstyle q\cdot} \\ A & \hookrightarrow & A[y/x] \end{array}$$

se deduce que $\dim_k A[y/x]/A + \dim_k A[y/x]/(q) = \dim_k A/(q) + \dim_k A[y/x]/A$, y se concluye. Entonces,

$$\begin{aligned}(C \cap D)_{or} &= \dim_k A/(q) = \dim_k A[y/x]/(q) = \dim_k A[y/x]/(x^n \tilde{q}) \\ &= n \cdot A[y/x]/x + \dim_k A[y/x]/(x^n \tilde{q}) = nm + \sum_i (\tilde{C} \cap \tilde{D})_{t_i}\end{aligned}$$

Observemos que $(C \cap D)_{t_i} \neq 0$, si $t_i \in C \cap D$, es decir, $f_i = 0$ es una tangente común a C y D.

3.6. Apéndice: Variedades algebraicas lisas

En esta sección queremos mostrar que el concepto de diferencial en un punto y más en general el concepto de diferencial de una función son conceptos algebraicos. Dada una variedad algebraica $X = \operatorname{Spec} A$, se cumple que el módulo dual del A-módulo generado por todas las diferenciales de las funciones de X es el módulo de derivaciones, luego derivar es también un concepto algebraico (dicho de otro modo, es una aplicación lineal que cumple la regla de Leibnitz). En Geometría Algebraica las variedades lisas se corresponden con las variedades diferenciables (algebraicas), y son aquellas variedades cuyo módulo de diferenciales es libre (de rango la dimensión de la variedad). Desarrollaremos el cálculo diferencial en las variedades algebraicas y daremos criterios diferenciales que caracterizan a las variedades lisas.

3.6.1. Módulo de las diferenciales de Kähler y módulo de derivaciones

Justifiquemos o introduzcamos la definición de diferencial de Kähler, a partir de la definición conocida de diferencial en Análisis o Geometría Diferencial.

Como es bien conocido, el incremento en un punto $\alpha \in \mathbb{R}$, de una función real f, se define $\Delta_\alpha f := f - f(\alpha)$. Esta definición es ampliable a las funciones algebraicas sobre la recta afín, es decir, para $k[x]$: Dado $p(x) \in k[x]$ y $\alpha \in k$ (equivalentemente, el punto "racional" $\alpha \in \operatorname{Spec} k[x]$, donde $\mathfrak{m}_\alpha = (x - \alpha)$), se define el incremento de $p(x)$ en α como $\Delta_\alpha p(x) := p(x) - p(\alpha)$. Más en general, dada una k-álgebra A y un punto racional $\alpha \in \operatorname{Spec} A$ (es decir, $A/\mathfrak{m}_\alpha = k$), se define el incremento de una función $f \in A$ en el punto α como $\Delta_\alpha f := f - f(\alpha)$ (donde $f(\alpha) := \bar{f} \in A/\mathfrak{m}_\alpha = k$).

La diferencial de una función real infinitamente diferenciable f, en un punto $\alpha \in \mathbb{R}$, se define como $d_\alpha f = f - f(\alpha) \mod (x - \alpha)^2$. Es decir, si $\mathfrak{m}_\alpha$ es el ideal de las funciones diferenciables que se anulan en α, entonces

$$d_\alpha f := \overline{\Delta_\alpha f} = \overline{f - f(\alpha)} \in \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

En general, dada una k-álgebra A y un punto racional $\alpha \in \operatorname{Spec} A$, se define la diferencial de la función $f \in A$ en el punto α como $d_\alpha f := \overline{\Delta_\alpha f} = \overline{f - f(\alpha)} \in \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$. El k-espacio vectorial $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, se le denomina espacio cotangente en α de $\operatorname{Spec} A$.

El siguiente paso es abstraernos del punto concreto $\alpha \in \mathbb{R}$. El incremento de una función diferenciable $f(x)$, en un punto $\bar{x}$, cualquiera, lo podemos definir como $\Delta f(x) := f(x) - f(\bar{x})$ (con precisión, $\Delta f(x)$ es la función definida en $\mathbb{R} \times \mathbb{R}$, cuyo valor en cada punto $(x, \bar{x})$ es $f(x) - f(\bar{x})$). Obviamente, $\Delta f(x)$ se anula sobre la diagonal de $\mathbb{R} \times \mathbb{R}$ y su restricción a $\mathbb{R} \times \alpha$ es $\Delta_\alpha f$. Además, si Δ es el ideal de las funciones diferenciales de $\mathbb{R} \times \mathbb{R}$ que se anulan en la diagonal, entonces la restricción de Δ a $\mathbb{R} \times \alpha$ es $\mathfrak{m}_\alpha$. Puede demostrarse que la definición de diferencial de una función, en Geometría Diferencial o Análisis, es $df := \overline{\Delta f} = \overline{f(x) - f(\bar{x})} \in \Delta/\Delta^2$. Se dice que Δ/Δ^2 es el $\mathscr{C}^\infty(\mathbb{R})$-módulo de las diferenciales de las funciones diferenciales de $\mathbb{R}$.

Consideremos el anillo $k[x]$ de las funciones algebraicas de la recta afín $\mathbb{A}^1$ y el anillo $k[x] \otimes_k k[x]$ de funciones algebraicas de $\mathbb{A}_1 \times_k \mathbb{A}_1 = \mathbb{A}_2$. Los morfismos

$$k[x] \rightrightarrows k[x, \bar{x}],\ p(x) \mapsto p(x),\ p(x) \mapsto p(\bar{x})$$

son obviamente los morfismos $k[x] \rightrightarrows k[x] \otimes_k k[x]$, $p(x) \mapsto p(x) \otimes 1$ y $p(x) \mapsto 1 \otimes p(x)$, que inducen por tomas de espectros las dos proyecciones naturales de $\mathbb{A}_1 \times_k \mathbb{A}_1$ en $\mathbb{A}_1$. La inmersión diagonal $\mathbb{A}_1 \to \mathbb{A}_1 \times_k \mathbb{A}_1$, $\alpha \mapsto (\alpha, \alpha)$ es el morfismo inducido por el morfismo de anillos $k[x] \otimes_k k[x] \xrightarrow{\phi} k[x]$, $p(x) \otimes q(x) \mapsto p(x) \cdot q(x)$. El ideal de las funciones algebraicas que se anulan en la diagonal es $\operatorname{Ker} \phi$.

Más en general, sea k un anillo y A una k-álgebra. Si definimos $\operatorname{Spec} A \times_k \operatorname{Spec} A := \operatorname{Spec}(A \otimes_k A)$, 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 cumple que*

$$\Delta \otimes_A A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha.$$

Es decir, "la restricción a $\mathrm{Spec} A \times \alpha$ *del ideal de las funciones que se anulan en la diagonal es el ideal de las funciones que se anulan en α"*

Demostración. Dado que la sucesión exacta

$$0 \to \Delta \to A \otimes_k A \to A \to 0$$

escinde, si tensamos por $\otimes_A A/\mathfrak{m}_\alpha$ obtenemos la sucesión exacta

$$0 \to \Delta \otimes_A A/\mathfrak{m}_\alpha \to A \to A/\mathfrak{m}_\alpha \to 0$$

y se concluye que $\Delta \otimes_A A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha$. □

5. Corolario: *Sea $\mathfrak{m}_\alpha$ un ideal de A tal que $A/\mathfrak{m}_\alpha = k$. Entonces*

$$\Omega_{A/k} \underset{A}{\otimes} A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

Demostración. Es inmediato de la definición de módulo de diferenciales de Kähler y de la proposición anterior. □

6. Observación: Si $\mathfrak{m}_\alpha$ es un ideal de A tal que $A/\mathfrak{m}_\alpha = k$, entonces la composición de la diferencial $d\colon A \to \Omega_{A/k}$ con el paso al cociente $\Omega_{A/k} \to \Omega_{A/k} \underset{A}{\otimes} A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, define un morfismo

$$d_\alpha\colon A \to \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$$

que se denomina diferencial en α, y que vale $d_\alpha(f) = \overline{f - f(\alpha)}$, donde $f(\alpha)$ es la clase de f en $A/\mathfrak{m}_\alpha = k$.

7. Proposición: *Si $k \to k'$ es un morfismo de anillos, entonces que*

$$\Omega_{A/k} \underset{k}{\otimes} k' = \Omega_{A \underset{k}{\otimes} k'/k'}$$

Demostración. Denotemos Δ_A el ideal de la diagonal definido a partir de A. Denotemos $A_{k'} = A \otimes_k k'$.

Si tensamos la sucesión exacta

$$0 \to \Delta_A \to A \otimes_k A \to A \to 0$$

por $\otimes_k k'$, obtenemos la sucesión exacta

$$0 \to \Delta_A \otimes_k k' \to A_{k'} \otimes_{k'} A_{k'} \to A_{k'} \to 0$$

Luego, $\Delta_A \otimes_k k' = \Delta_{A_{k'}}$. Por tanto, $\Omega_{A/k} \otimes_k k' = (\Delta_A/\Delta_A^2) \otimes_k k' = (\Delta_A \otimes_k k')/(\Delta^2 \otimes_k k') = \Delta_{A_{k'}}/\Delta^2_{A_{k'}} = \Omega_{A_{k'}/k'}$.

□

Derivaciones

8. Definición: Sea A una k-álgebra y M un A-módulo. Diremos que una aplicación $D\colon A \to M$ es una k-derivación si verifica las siguientes condiciones:

1. D es un morfismo de k-módulos.
2. $D(ab) = bD(a) + aD(b)$ para todo $a, b \in A$.

Observemos que $D(1) = D(1\cdot 1) = 1D(1) + 1D(1) = 2D(1)$, luego $D(1) = 0$. Además, dado $\lambda \in k$, $D(\lambda) = \lambda D(1) = 0$.

El conjunto de todas las k-derivaciones de A en M se denota por $\mathrm{Der}_k(A,M)$. Si definimos

$$(D+D')(a) := D(a) + D'(a) \quad \text{y} \quad (aD)(b) := a \cdot Db$$

tenemos que el conjunto de todas las k-derivaciones de A en M tiene estructura de A-módulo.

9. Proposición: *La diferencial $d\colon A \to \Omega_{A/k}$ es una k-derivación.*

Demostración. Si denotamos $\delta a = a \otimes 1 - 1 \otimes a$, es una comprobación inmediata que $\delta(ab) = (a\otimes 1)\cdot \delta b + (\delta a)\cdot(1\otimes b)$. Haciendo módulo Δ^2 obtenemos $d(ab) = adb + bda$. □

10. Corolario: *Si $\mathfrak{m}_\alpha$ es un ideal tal que $A/\mathfrak{m}_\alpha = k$, entonces $d_\alpha\colon A \to \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$ es una k-derivación.*

Demostración. Inmediato. □

11. Proposición: *Sea $\mathfrak{m}$ un ideal de A tal que $A/\mathfrak{m} = k$. Sea M un k-módulo, luego A-módulo a través del cociente $A \to A/\mathfrak{m} = k$. Se cumple que*

$$\mathrm{Der}_k(A,M) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, M).$$

En particular,

$$\mathrm{Der}_k(A,k) = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k) \underset{Not}{=} (\mathfrak{m}/\mathfrak{m}^2)^*$$

Demostración. Dada una k-derivación $D\colon A \to M$, define por restricción un morfismo $D_{|\mathfrak{m}}\colon \mathfrak{m} \to M$, 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 $\bar{D}_{|\mathfrak{m}}\colon \mathfrak{m}/\mathfrak{m}^2 \to M$. Recíprocamente, cada morfismo de espacios vectoriales $w\colon \mathfrak{m}/\mathfrak{m}^2 \to M$, define, componiendo con $A \to \mathfrak{m}/\mathfrak{m}^2$, una k-derivación $A \to M$. Dejamos al lector que compruebe que estas asignaciones son inversas entre sí.

□

12. Teorema: *Tenemos el isomorfismo canónico*

$$\mathrm{Hom}_A(\Omega_{A/k}, M) = \mathrm{Der}_k(A,M),\ w \mapsto w \circ d.$$

Demostración. Por la proposición anterior, para todo A-módulo M se cumple que

$$\mathrm{Der}_A(A \otimes_k A, M) = \mathrm{Hom}_A(\Delta/\Delta^2, M).$$

Por tanto, basta probar que para todo morfismo de anillos $k \to k'$ y todo $A \otimes_k k'$-módulo M, se tiene un isomorfismo

$$\mathrm{Der}_k(A, M) \simeq \mathrm{Der}_{k'}(A \otimes_k k', M)$$

Dada una k-derivación $D\colon A \to M$, tenemos la k'-derivación $D'\colon A \otimes_k k' \to M$, definida por $D'(a \otimes \lambda) = (1 \otimes \lambda) \cdot D(a)$. Recíprocamente, toda k'-derivación $D'\colon A \otimes_k k' \to M$, define, componiendo con $A \to A \otimes_k k'$, una k-derivación de A en M. Una asignación es la inversa de la otra. □

13. Proposición: *Sea S un sistema multiplicativamente cerrado de A. Se verifica*

$$(\Omega_{A/k})_S = \Omega_{A_S/k},\ \frac{da}{s} \mapsto \frac{1}{s} \cdot da$$

Demostración. Empecemos probando que si M es un A_S-módulo entonces $\mathrm{Der}_k(A, M) = \mathrm{Der}_k(A_S, M)$. Basta ver para ello, que toda derivación $D \in \mathrm{Der}_k(A, M)$ extiende de modo único a una derivación de A_S. La única derivación D' que puede coincidir con D en A es:

$$D'(a/s) := (sDa - aDs)/s^2.$$

Ahora ya, tenemos

$$\begin{aligned}\mathrm{Hom}_{A_S}(\Omega_{A_S/k}, M) = \mathrm{Der}_k(A_S, M) = \mathrm{Der}_k(A, M) = \mathrm{Hom}_A(\Omega_{A/k}, M)\\ = \mathrm{Hom}_{A_S}((\Omega_{A/k})_S, M).\end{aligned}$$

Luego $(\Omega_{A/k})_S = \Omega_{A_S/k}$.

□

Dejamos al lector que demuestre con el mismo método

14. Proposición: $\Omega_{(A \otimes_k B)/k} = (\Omega_{A/k} \otimes_k B) \oplus (A \otimes_k \Omega_{B/k})$, $d(a \otimes b) \mapsto da \otimes b + a \otimes db$.

15. Proposición: $\Omega_{(A \times B)/k} = \Omega_{A/k} \oplus \Omega_{B/k}$, $d((a, b)) = (da, db)$.

Para terminar estudiemos las sucesiones exactas de diferenciales. Comencemos para ello con las sucesiones exactas de derivaciones.

16. Proposición: *Si B es una A-álgebra y N un B-módulo, la siguiente sucesión es exacta:*

$$\begin{array}{ccccccc} 0 & \to & \mathrm{Der}_A(B,N) & \to & \mathrm{Der}_k(B,N) & \to & \mathrm{Der}_k(A,N) \\ & & D & \mapsto & D & & \\ & & & & D & \mapsto & D_{|A} \end{array}$$

Demostración. Es evidente. □

Si B es una A-álgebra, el morfismo $A \to \Omega_{B/k}, a \mapsto da$ induce por 3.6.12, un morfismo $\Omega_{A/k} \to \Omega_{B/k}$, $da \mapsto da$. De otro modo, con las notaciones obvias, tenemos que Δ_A está "incluido" en Δ_B, luego tenemos un morfismo $\Omega_{A/k} = \Delta_A/\Delta_A^2 \to \Delta_B/\Delta_B^2 = \Omega_{B/k}$. Por tanto, tenemos un morfismo natural

$$\Omega_{A/k} \otimes_A B \to \Omega_{B/k}, da \otimes b \mapsto bda$$

El morfismo $B \to \Omega_{B/A}$, $d \mapsto db$, es una k-derivación, porque es una A-derivación. De nuevo, por 3.6.12, tenemos el morfismo de B-módulos $\Omega_{B/k} \to \Omega_{B/A}$, $db \mapsto db$, que es claramente epiyectivo.

17. Proposición: *Si B es una A-álgebra, la siguiente sucesión es exacta:*

$$\Omega_{A/k} \otimes_A B \to \Omega_{B/k} \to \Omega_{B/A} \to 0$$

Demostración. Basta probar que para todo B-módulo N, la sucesión

$$0 \to \underset{\mathrm{Der}_A(B,N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{B/A},N)}} \to \underset{\mathrm{Der}_k(B,N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{B/k},N)}} \to \underset{\mathrm{Der}_k(A,N)}{\underset{\|}{\underset{\mathrm{Hom}_A(\Omega_{A/k},N)}{\underset{\|}{\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B,N)}}}}$$

es exacta. Lo es por la proposición anterior.

□

18. Proposición: *Si I es un ideal de A y N es un A/I-módulo, la restricción a I de cualquier k-derivación $D\colon A \to N$ es un morfismo de A-módulos. La siguiente sucesión es exacta*

$$0 \to \mathrm{Der}_k(A/I,N) \to \mathrm{Der}_k(A,N) \to \mathrm{Hom}_A(I,N)$$

Demostración. Es evidente. □

19. Proposición: *Sea $I \subset A$ un ideal y consideremos el morfismo $I/I^2 \to \Omega_{A/k} \otimes A/I$, $\bar{i} \mapsto di \otimes 1$. La siguiente sucesión es exacta*

$$I/I^2 \to \Omega_{A/k} \otimes_A A/I \to \Omega_{(A/I)/k} \to 0$$

Demostración. Basta probar que para todo A/I-módulo N, la sucesión

$$0 \to \underset{\underset{\mathrm{Der}_k(A/I,N)}{\|}}{\mathrm{Hom}_{A/I}(\Omega_{(A/I)/k},N)} \to \underset{\underset{\underset{\mathrm{Der}_k(A,N)}{\|}}{\mathrm{Hom}_A(\Omega_{A/k},N)}}{\mathrm{Hom}_{A/I}(\Omega_{A/k}\otimes_A(A/I),N)} \to \underset{\underset{\mathrm{Hom}_A(I,N)}{\|}}{\mathrm{Hom}_{A/I}(I/I^2,N)}$$

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

$$D\colon k[x_1,\ldots,x_n] \to M$$

se anula sobre los x_i entonces $D = 0$: Por linealidad basta probar que es nula sobre los monomios x^α y para ello procedamos por inducción sobre $|\alpha| = \alpha_1+\ldots+\alpha_n$. Supongamos $\alpha_1 \neq 0$, sea β, tal que $\beta_1 = \alpha_1 - 1$ y $\beta_i = \alpha_i$, para $i > 1$ (luego $|\beta| < |\alpha|$), entonces $D(x^\alpha) = D(x_1\cdot x^\beta) = x^\beta \cdot Dx_1 + x_1 \cdot Dx^\beta = 0+0 = 0$.

Dado $m \in M$, sea $m\frac{\partial}{\partial x_i}$ la derivación definida por $m\frac{\partial}{\partial x_i}(p(x)) := \frac{\partial p(x)}{\partial x_i}\cdot m$. Dada una derivación D entonces $D = \sum_i (Dx_i)\cdot\frac{\partial}{\partial x_i}$, pues la diferencia entre los dos términos de la igualdad es una derivación que se anula en todos los x_i. Ahora ya, es clara la siguiente proposición.

20. Proposición: $\mathrm{Der}_k(k[x_1,\ldots,x_n],M) = M\frac{\partial}{\partial x_1}\oplus\cdots\oplus M\frac{\partial}{\partial x_n}$.

21. Proposición: $\Omega_{k[x_1,\ldots,x_n]/k} = k[x_1,\ldots,x_n]dx_1\oplus\cdots\oplus k[x_1,\ldots,x_n]dx_n$, $df \mapsto \sum_i \frac{\partial f}{\partial x_i}dx_i$.

Demostración. Se deduce de las igualdades

$$\begin{aligned} Hom_{k[x_1,\ldots,x_n]}(\Omega_{k[x_1,\ldots,x_n]/k},M) &= \mathrm{Der}_k(k[x_1,\ldots,x_n],M) = M\frac{\partial}{\partial x_1}\oplus\cdots\oplus M\frac{\partial}{\partial x_n} \\ &= \mathrm{Hom}_{k[x_1,\ldots,x_n]}(k[x_1,\ldots,x_n]dx_1\oplus\cdots\oplus k[x_1,\ldots,x_n]dx_n,M) \end{aligned}$$

□

22. Proposición: *Sea* $A = k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$. *Entonces*

$$\Omega_{A/k} = (Adx_1\oplus\cdots\oplus Adx_n)/(dp_1,\ldots,dp_r)$$

donde $dp_i = \sum_j \frac{\partial p_i}{\partial x_j}dx_j$.

Demostración. Considérese la sucesión exacta $0 \to (p_1,\ldots,p_r) \to k[x_1,\ldots,x_n] \to A \to 0$ y aplíquese la sucesión exacta de diferenciales 3.6.19. □

23. Teorema: *Sea k un cuerpo. Una k-álgebra finita A es separable si y solo $\Omega_{A/k} = 0$.*

Demostración. Por cambio de cuerpo base podemos suponer que A es racional. Podemos suponer que A es racional y local, de ideal maximal $\mathfrak{m}$.

Por el lema de Nakayama, $\Omega_{A/k} = 0$ si y solo si $\mathfrak{m}/\mathfrak{m}^2 = \Omega_{A/k} \otimes_A A/\mathfrak{m} = 0$, que equivale a decir que $\mathfrak{m} = 0$, es decir, que A es separable. □

24. Ejercicios:

1. Sea $A = k[x](p(x))$. Prueba que $\Omega_{A/k} = k[x]/(p, p')dx$. Prueba que $\Omega_{A/k} = 0 \Leftrightarrow p(x)$ tiene raíces dobles.

2. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcula $\Omega_{A/k}$, $\Omega_{A/K}$ y $\Omega_{K/k}$.

3. Sea A una k-álgebra finita y racional. Prueba que $\Omega_{A/k} = 0 \Leftrightarrow A = k \times \overset{n}{\cdots} \times k$.

4. 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 $M = k[x, y]/(x, y)$.

5. Si B es una A-álgebra finita y A es una k-álgebra finita, prueba que: B es separable sobre $k \Leftrightarrow A$ es separable y $\Omega_{B/A} = 0$.

6. Sea A una k-álgebra finita local y racional. Prueba: A tiene un elemento primitivo $\Leftrightarrow \Omega_{A/k}$ tiene un generador.

7. Sea A un anillo íntegro y local y sea B una A-álgebra, que como A-módulo es finito generada y libre. Prueba que $B \to \mathrm{Hom}_A(B, A)$, $b \mapsto \mathrm{tr}(b \cdot -)$ es isomorfismo si y solo si $\Omega_{B/A} = 0$.

8. Sea $A = k[x]/(p(x))$, siendo k de característica cero. Prueba la exactitud de la sucesión
$$0 \to \pi_0^k(A) \to A \xrightarrow{d} \Omega_{A/k}$$
Donde $\pi_0^k(A)$ es el conjunto de los elementos separables de A. ¿Es cierto este resultado si k es de característica p?

9. Sea $K \to \overline{K} = K(\alpha)$ una extensión finita. Prueba:

   a) Si $\overline{K}$ es separable, entonces $\Omega_{\overline{K}[x]/K} = \overline{K}[x]$.

   b) Si $\overline{K}$ no es separable, entonces $\Omega_{\overline{K}[x]/K} = \overline{K}[x] \oplus \overline{K}[x]$.

3.6.2. Variedades lisas

25. Definición: Sea $X = \operatorname{Spec} A$ una variedad algebraica. Diremos que X es lisa en un punto cerrado $x \in X$ si $\Omega_{A_x/k}$ es un A_x-módulo libre de rango $\dim A_x$. Diremos que X es lisa si es lisa en todos sus puntos cerrados.

26. Ejemplos: El espacio afín $\mathbb{A}^n = \operatorname{Spec} k[x_1, \ldots, x_n]$ es liso.

La cúspide $y^2 - x^3 = 0$ es lisa en todos los puntos cerrados salvo en el origen: Escribamos $A = \mathbb{C}[x,y]/(y^2 - x^3)$. Para todo punto cerrado $\alpha \in \operatorname{Spec} A$, $\dim A_\alpha = 1$. Consideremos la sucesión exacta

$$0 \to \langle 3x^2 dx \oplus 2y dy \rangle \to A dx \oplus A dy \to \Omega_{A/k} \to 0$$

Para $\alpha = (0,0)$, $\Omega_{A/k} \otimes_A A/\mathfrak{m}_\alpha$ es un $A/\mathfrak{m}_\alpha$-espacio vectorial de dimensión 2, luego $(\Omega_{A/k})_\alpha$ no es libre de rango 1. Por el lema 3.6.29, para todo $\alpha \neq (0,0)$, $(\Omega_{A/k})_\alpha$ es un módulo libre de rango 1.

El nodo es $y^2 - x^2 + x^3 = 0$ es liso en todos los puntos salvo el origen.

27. Proposición: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica. Si $x \in X$ es un punto racional liso, entonces $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x$.*

Demostración. Es consecuencia inmediata de la igualdad $\Omega_{A/k} \otimes_A A/\mathfrak{m}_x = \mathfrak{m}_x/\mathfrak{m}_x^2$. □

Observemos que en general $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 \geq \dim A_x$, porque si $\{\bar{f}_1, \ldots, \bar{f}_n\}$ es una base de $\mathfrak{m}_x/\mathfrak{m}_x^2$, entonces $\mathfrak{m}_x = (f_1 \ldots, f_n)$ y $0 = \dim(A_x/(f_1, \ldots, f_n)) \geq \dim A_x - n$.

28. Proposición: *Sea $X = \operatorname{Spec} A$ una variedad algebraica y $x \in X$ un punto cerrado. Si $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim A_x$ entonces A_x es íntegra.*

En particular, si $x \in X$ es un punto racional liso, entonces A_x es íntegra.

Demostración. Procedemos por inducción sobre $n = \dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2$. Si $n = 0$ entonces A_x es un cuerpo. Supongamos $n > 0$. Dado $f \in \mathfrak{m}_x$, tal que $d_x f \neq 0$, sea $\bar{A}_x := A_x/(f)$ y $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en $\bar{A}_x$. Entonces, $\dim \bar{A}_x \geq n-1$ y $\dim_{\bar{A}/\bar{\mathfrak{m}}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \leq n-1$. Luego, $\dim_{\bar{A}/\bar{\mathfrak{m}}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim \bar{A}_x = n-1$. Por hipótesis de inducción $\bar{A}_x$ es íntegro. Por tanto, $(f)_0 \subset \operatorname{Spec} A_x$ es una hipersuperficie irreducible (que pasa por x), incluida en todas las componentes irreducibles de dimensión n y no contiene, pues, ninguna componente irreducible de $\operatorname{Spec} A_x$. Sean $g_1, g_2 \in A_x$. Por noetherianidad tendremos que $g_1 = f_1^{n_1} \cdots f_r^{n_r} \cdot g_1'$, $g_2 = f_1^{m_1} \cdots f_r^{m_r} \cdot g_2'$, con $n_i, m_i \geq 0$, $d_x f_i \neq 0$ y g_1', g_2' no divisibles por ninguna $f \in \mathfrak{m}_x$, tal que $d_x f \neq 0$. Si $g_1 \cdot g_2 = 0$, entonces $(g_1' \cdot g_2')_0 = \operatorname{Spec} A_x$. Dada $f \in \mathfrak{m}_x$ con $d_x f \neq 0$, como (f) es primo se cumple que f divide a g_1' o g_2' y hemos llegado a contradicción.

□

29. Lema: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, M un $\mathcal{O}$-módulo finito generado y $f: M \to L$ un morfismo en un libre finito generado. Si $\bar{f}: M/\mathfrak{m}M \to L/\mathfrak{m}L$ es inyectivo, entonces f es inyectivo y los módulos M y $M/\operatorname{Im} f$ son libres.*

Demostración. Sea $m_1,\dots,m_r \in M$ tales que $\bar{m}_1,\dots,\bar{m}_r \in M/\mathfrak{m}M$ sean 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 $L/\mathfrak{m}L$. Entonces, $\{f(m_1),\dots,f(m_r),l_1,\dots,l_s\}$ es una base de L. Luego, $\{m_1,\dots,m_r\}$ es una base de M, f es inyectivo y $M/\operatorname{Im} f$ 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 3.6.29, $(\Omega_{(A/I)/k})_x$ es libre de rango $n-r$. Además, $\dim_k \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = n-r$ y $\dim(A/I)_x \geq n-r$. Luego, $\dim(A/I)_x = n-r$ e Y es lisa en x.

$\Rightarrow$) Consideremos la sucesión exacta

$$I_x/I_x^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Sean $f_1,\dots,f_r \in I$ tales que $d_x f_1,\dots,d_x f_r$ sean una base de la imagen de I en $\mathfrak{m}_x/\mathfrak{m}_x^2$. Observemos que $n-r = \dim_k \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim(A/I)_x$. Sea $J := (f_1,\dots,f_r) \subseteq I$. Por la implicación $\Leftarrow$), $(A/J)_x$ es lisa de dimensión de Krull $n-r$. Tenemos que $\dim(A/J)_x = \dim(A/I)_x$ y $(A/J)_x$ es íntegra. El morfismo de paso al cociente $\pi\colon (A/J)_x \to (A/I)_x$ es isomorfismo: Si $\operatorname{Ker}\pi \neq 0$, entonces la dimensión de Krull de $(A/I)_x = (A/J)_x/\operatorname{Ker}\pi$ sería menor que la de $(A/J)_x$ y llegaríamos a contradicción. Luego $(A/J)_x = (A/I)_x$ y $I_x = J_x = (f_1,\dots,f_r)$. □

En bien conocido en Geometría Diferencial que si X es una variedad diferenciable e Y el cerrado definido por r funciones diferenciables $f_1,\dots,f_r \in \mathscr{C}^\infty(X)$, tales que $d_y f_1,\dots,d_y f_r$ son linealmente independientes para todo $y \in Y$, entonces Y es una subvariedad diferenciable de X.

31. Ejercicio: Sea $X = \operatorname{Spec} k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ y $\alpha = (\alpha_1,\dots,\alpha_n)$ un punto racional de X. Supongamos que $\dim X = n-r$. Prueba que X es liso en x si y solo si la matriz $(\frac{\partial p_i}{\partial x_j}(0))_{i,j\le n}$ tiene rango r.

32. Proposición: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica y k' el cierre algebraico de k. Entonces, X es lisa $\iff$ $X_{k'} := \operatorname{Spec}(A \otimes_k k')$ es lisa.*

Demostración. El morfismo $A \hookrightarrow A \otimes_k k'$ es inyectivo, entero y plano. Sea $\pi\colon X_{k'} \to X$ el morfismo inducido en espectros. Para todo punto cerrado $x' \in X_{k'}$, $\dim(A \otimes_k k')_{x'} = \dim A_{\pi(x')}$. Además la imagen por π de un punto cerrado es un punto cerrado y las fibras de puntos cerrados son puntos cerrados (y no son vacías).

$\Omega_{A/k}$ es un A-módulo plano si y solo si $\Omega_{A_K/K} = \Omega_{A/k} \otimes_k K = \Omega_{A/k} \otimes_A A_K$ es un A_K-módulo plano, porque $A \to A_K$ es un morfismo fielmente plano. Luego, $\Omega_{A/k}$ es un A-módulo localmente libre de rango n si y solo si $\Omega_{A_K/K} = \Omega_{A/k} \otimes_k K = \Omega_{A/k} \otimes_A A_K$ es un A_K-módulo localmente libre de rango n.

□

33. Criterio jacobiano de lisitud: *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica lisa. Sea $Y = \operatorname{Spec}(A/I) \subset X$ una subvariedad. Entonces, Y es lisa si y solo si*

1. *$\Omega_{(A/I)/k}$ es localmente libre.*
2. *La sucesión $0 \to I/I^2 \to \Omega_{A/k} \otimes_A A/I \to \Omega_{(A/I)/k} \to 0$ es exacta.*

Demostración. Por cambio de cuerpo base podemos suponer que k es algebraicamente cerrado. La cuestión es local, luego podemos suponer que A es local de ideal maximal $\mathfrak{m}_x$. Denotemos por $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en A/I.

$\Leftarrow$) Por ser $\Omega_{(A/I)/k}$ un módulo libre, la sucesión de 2. escinde. Por tanto, al tensar por $\otimes_A A/\mathfrak{m}_x$ obtenemos la sucesión exacta

$$0 \to I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0,$$

luego I está generado por un sistema de parámetros cuyas diferenciales en x son linealmente independientes. Por 3.6.30, A/I es lisa.

$\Rightarrow$) Si Y es lisa, ya sabemos que satisface la condición 1. Sólo queda probar que la sucesión de 2. es exacta por la izquierda. Por el lema anterior, basta ver que

$$I/\mathfrak{m}_x I \xrightarrow{\bar{\imath}} \mathfrak{m}_x/\mathfrak{m}_x^2$$

es inyectivo, que lo es por 3.6.30. □

3.6.3. Módulo de diferenciales de una variedad en el punto genérico

Queremos probar que las variedades algebraicas íntegras (sobre un cuerpo algebraicamente cerrado) son lisas en un abierto no vacío. Para ello probaremos que el rango del módulo de diferenciales de Kahler coincide con la dimensión de la variedad.

34. Proposición: *Sea $k \to K = k(\xi_1, \ldots, \xi_m)$ una extensión de tipo finito. Se verifica*

$$\dim_K \Omega_{K/k} \geq \operatorname{gr\,tr}_k K$$

Además, la desigualdad es una igualdad si y solo si existe una base de trascendencia $\{x_1, \ldots, x_n\}$ tal que $k(x_1, \ldots, x_n) \hookrightarrow K$ sea una extensión separable.

Demostración. Sea $\Sigma \to \Sigma(\xi)$ una extensión. Se cumple que

$$\dim_{\Sigma(\xi)} \Omega_{\Sigma(\xi)/k} = \begin{cases} \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es trascendente.} \\ \dim_\Sigma \Omega_{\Sigma/k} \text{ ó } \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es algebraico.} \end{cases}$$

En efecto: Consideremos $\Sigma[x]$. Tenemos que

$$\Omega_{\Sigma[x]/k} = \Omega_{\Sigma \otimes_k k[x]/k} = (\Omega_{\Sigma/k} \otimes_k k[x]) \oplus (\Sigma \otimes_k \Omega_{k[x]/k}) = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma[x]) \oplus \Sigma[x]dx$$

Localizando en el punto genérico de $\Sigma[x]$,

$$\Omega_{\Sigma(x)/k} = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma(x)) \oplus \Sigma(x)dx$$

y se concluye la primera parte. Supongamos ahora que ξ es algebraico. Así pues, $\Sigma(\xi) = \Sigma[x]/(p(x))$. De la sucesión exacta $0 \to (p(x)) \to \Sigma[x] \to \Sigma(\xi) \to 0$, se obtiene la sucesión exacta de diferenciales

$$\begin{array}{ccc} (p(x))/(p(x)^2) & \to & \Omega_{\Sigma[x]/k} \underset{\Sigma[x]}{\otimes} \Sigma(\xi) \to \Omega_{\Sigma(\xi)/k} \to 0 \\ p(x) & \mapsto & dp(x) \end{array}$$

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 $\dim_K \Omega_{K/k} \le \dim_{K'} \Omega_{K'/k} = n = \mathrm{gr\,tr}_k K$, luego $\dim_K \Omega_{K/k} = \mathrm{gr\,tr}_k K$.

Recíprocamente, si $\dim_K \Omega_{K/k} = \mathrm{gr\,tr}_k K = n$, sean $x_1,\dots,x_n \in K$ tales que las diferenciales $dx_1,\dots,dx_n$ sean una base de $\Omega_{K/k}$. De la sucesión $(**)$ obtenemos que i^* es epiyectiva, luego $\Omega_{K/K'} = 0$. Por tanto, $K' \hookrightarrow K$ es finita y separable y $\{x_1,\dots,x_n\}$ es una base de trascendencia. □

35. Teorema: *Sea k un cuerpo perfecto y K una extensión de tipo finito de k. Entonces,*

1. $\dim_K \Omega_{K/k} = \mathrm{gr\,tr}_k K$.

2. *Dados $\xi_1,\dots,\xi_n \in K$, $\{d\xi_1,\dots,d\xi_n\}$ es una base del K-espacio vectorial $\Omega_{K/k}$ $\iff$ $\{\xi_1,\dots,\xi_n\}$ es una base de trascendencia de la k-extensión K y $k(\xi_1,\dots,\xi_n) \hookrightarrow K$ es un morfismo finito separable.*

Demostración. Basta demostrar 2.

$\Rightarrow$) El morfismo $k(\xi_1,\dots,\xi_n) \hookrightarrow K$ es separable, por la sucesión exacta $(**)$ de la proposición anterior. Sólo tenemos que ver que $\xi_1,\dots,\xi_n$ son algebraicamente independientes. Sea $p(x_1,\dots,x_n) \neq 0$ un polinomio de grado mínimo tal que $p(\xi_1,\dots,\xi_n) = 0$. Entonces, $dp(\xi_1,\dots,\xi_n) = \sum_i \frac{\partial p}{\partial x_i}(\xi_1,\dots,\xi_n)d\xi_i = 0$, luego $\frac{\partial p}{\partial x_i}(\xi_1,\dots,\xi_n) = 0$ para todo i, de donde se deduce que $\frac{\partial p}{\partial x_i}(x_1,\dots,x_n) = 0$ y $p(x_1,\dots,x_n) = q(x_1^p,\dots,x_n^p)$. Tenemos $\sqrt[p]{p(x_1,\dots,x_n)} = \sqrt[p]{q(x_1^p,\dots,x_n^p)} \in k[x_1,\dots,x_n]$ por ser k perfecto. Además, $\sqrt[p]{p(x_1,\dots,x_n)}$ es un polinomio de grado menor que el de $p(x_1,\dots,x_n)$, que anula a $\xi_1,\dots,\xi_n$. Contradicción, no existe $p(x_1,\dots,x_n) \neq 0$ tal que $p(\xi_1,\dots,\xi_n) = 0$.

$\Leftarrow$) Por la sucesión exacta $(**)$ de la demostración de la proposición anterior, el morfismo $\Omega_{k(\xi_1,\dots,\xi_n)/k}\otimes_{k(\xi_1,\dots,\xi_n)}K \to \Omega_{K/k}$ es epiyectivo, luego $\{d\xi_1,\dots,d\xi_n\}$ generan el K-espacio vectorial $\Omega_{K/k}$. Además, como $\dim_K \Omega_{K/k} \ge \mathrm{gr\,tr}_k K = \mathrm{gr\,tr}_k k(\xi_1,\dots,\xi_n) = n$, $\{d\xi_1,\dots,d\xi_n\}$ es una base del K-espacio vectorial $\Omega_{K/k}$. □

36. Corolario: *Sea k un cuerpo perfecto y K, K' dos k-extensiones de cuerpos. Entonces, la k-álgebra $K\otimes_k K'$ es reducida.*

Demostración. K es unión de k-subextensiones K_i de tipo finito y la unión de subanillos reducidos $K_i \otimes_k K'$ es reducido. Podemos suponer que K es una extensión de tipo finito y, por el teorema 3.6.35, que K es una extensión finita separable de $k(x_1,\dots,x_n)$. $k(x_1,\dots,x_n)\otimes_k K'$ es una localización de $k[x_1,\dots,x_n]\otimes_k K' = K'[x_1,\dots,x_n]$, luego es íntegro. Sea Σ el cuerpo de fracciones de $k(x_1,\dots,x_n)\otimes_k K'$. Entonces,

$$K\otimes_k K' = K\otimes_{k(x_1,\dots,x_n)}(k(x_1,\dots,x_n)\otimes_k K') \subseteq K\otimes_{k(x_1,\dots,x_n)}\Sigma$$

ésta última es reducida, luego $K\otimes_k K'$ luego es reducida.

□

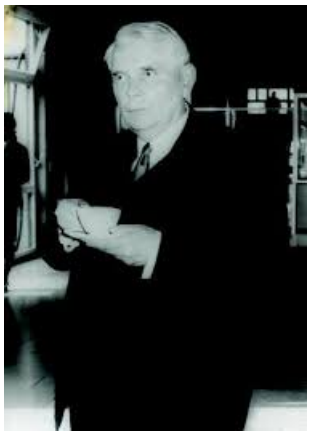
37. Corolario : *Sea k un cuerpo algebraicamente cerrado y X, Y dos k-variedades íntegras. Entonces, $X\times_k Y$ es una variedad íntegra.*

Demostración. $X\times_k Y$ es irreducible por la problema 14 Escribamos $X = \operatorname{Spec} A$ e $Y = \operatorname{Spec} A'$, y sean Σ y Σ' los cuerpos de fracciones de A y A' respectivamente. Como el morfismo $A\otimes_k A' \hookrightarrow \Sigma\otimes_k\Sigma'$ es inyectivo, entonces $A\otimes_k A'$ es reducida. Por tanto, $X\times_k Y$ es una variedad íntegra. □

38. Proposición : *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra sobre un cuerpo perfecto. El conjunto de puntos cerrados lisos de X es un abierto no vacío (del conjunto de puntos cerrados de X).*

Demostración. Sea Σ el cuerpo de fracciones de A. Sabemos que $\dim_\Sigma \Omega_{\Sigma/k} = \operatorname{gr\,tr}\Sigma = \dim X$. 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. □

3.7. Biografía de Krull



KRULL BIOGRAPHY

Wolfgang Krull's father was Helmuth Krull and his mother was Adele Siefert Krull. Helmuth Krull had a dentist's practice in Baden-Baden and it was in that town that Krull attended school.

After graduating from secondary school in 1919 he entered the University of Freiburg. It was the custom in those days for students in Germany to move around various universities during their period of study and Krull was no exception. He spent time at the University of Rostock before moving to Göttingen in 1920.

From 1920 to 1921 he studied at Göttingen with Klein but was most influenced by Emmy Noether. He attended Klein's seminar in the session 1920-21 and he then returned to Freiburg and presented his doctoral thesis on the theory of elementary divisors in 1922. Ring theory results from this thesis have recently been found important in the area of coding theory.

Appointed as an instructor at Freiburg on 1 October 1922 he was promoted to extraordinary professor in 1926. He remained there until 1928 when he moved to Erlangen. His inaugural address on becoming a full professor at Erlangen was one which says much of how Krull saw mathematics. He saw the role of a mathematician as

"*... not merely ... finding theorems and proving them. He wants to arrange and group these theorems together in such a way that they appear not only as correct but also as imperative and self-evident. To my mind such an aspiration is an aesthetic one and not one based on theoretical cognition*"

If Emmy Noether had the greatest influence on the topics which Krull would spend his life researching, it can be seen from this inaugural address that it was Klein who had the greatest influence on Krull's large scale view of mathematics. In 1929 he married Gret Meyer and they would have two daughters.

The ten years Krull spent in Erlangen were the most productive period of his career. As Schoeneborn wrote:

"*The years Krull spent as a full professor in Erlangen were the high point of his creative life. About thirty-five publications of fundamental importance for the development of commutative algebra and algebraic geometry date from this period.*"

At Erlangen he was involved in university life as well as concentrating on his research, being elected Head of the Faculty of Science.

In 1939 Krull left Erlangen to take up a chair at Bonn. However, his career was

disrupted by the Second World War which began shortly after Krull was appointed to the University of Bonn. During the war he undertook war duties, working in the naval meteorological service. When his war service had ended in 1946, Krull took up again his post at the University of Bonn and he would remain there for the rest of his life. In this final period of his career Krull continued his high level of productivity (he wrote 50 papers in his post-war years in Bonn) and also broadened his mathematical interests. Schoeneborn wrote:

"*... his earlier studies, but also dealt with other fields of mathematics: group theory, calculus of variations, differential equations, Hilbert spaces.*"

Krull's first publications were on rings and algebraic extension fields. In 1925 he proved the Krull-Schmidt theorem for decomposing abelian groups of operators. He then studied Galois theory and extended the classical results on Galois theory of finite field extensions to infinite field extensions. In passing from the finite to the infinite case Krull introduced topological ideas.

In 1928 he defined the Krull dimension of a commutative Noetherian ring and brought ring theory into in new setting in which he was able to show that the principal ideal theorem held. Perhaps the reason that the idea of the Krull dimension is such a natural concept is that it encapsulates in an abstract setting the analogues of geometric dimensions. The principal ideal theorem was quickly recognised as a decisive advance in Noether's programme of emancipating abstract ring theory from the theory of polynomial rings. Krull carried his work forward, defining further concepts which are today central to modern research in ring theory. In 1932 he defined valuations which are today known as Krull valuations. He then wrote the remarkable treatise Ideal Theory which remains a beautiful introduction to ring theory but is simply a theory built from the results that Krull had himself proved. One could say that Krull had achieved the goal he had in some sense set himself in his Erlangen address and arranged his theory to be self-evident.

Another major topic in ring theory is the study of local rings, that is rings having a unique maximal ideal, and they are used in the study of local properties of algebraic varieties. The concept was introduced by Krull in 1938 and his fundamental results were developed into a major theory by mathematicians such as Chevalley and Zariski.

He supervised 35 doctoral students, and rather remarkably, 32 of these were students whom he supervised after the end of World War II. Gray wrote that Krull's papers are

"*... marked by the profundity of his ideas, the rigour of his proofs, and also by a strong aesthetic sense.*"

Indeed much of modern ring theory is still following the path which Krull took, building on the foundations which Emmy Noether had laid.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/

Biographies/).

3.8. Cuestionario

1. ¿Es $k \to k[x]$ un morfismo de anillos finito?
2. Si $\alpha \in \mathbb{C}$ es una raíz n-ésima de la unidad, prueba que $\mathbb{Q} \hookrightarrow \mathbb{Q}[\alpha]$ es un morfismo finito.
3. Sea $A \to B$ un morfismo de anillos y $b_1, b_2 \in B$. Prueba que $A[b_1][b_2] = A[b_1, b_2]$.
4. ¿Es $\mathbb{Z} \to \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ un morfismo de anillos finito?
5. ¿Es $\mathbb{Q}[x] \to \mathbb{Q}[x,y]/(x^2+y^2-1)$, $p(x) \mapsto \overline{p(x)}$ un morfismo de anillos finito?
6. ¿Es lo mismo A-álgebra finita que A-álgebra de tipo finito?
7. Prueba que un morfismo de anillos $A \to B \times C$ es finito si y solo si $A \to B$ y $A \to C$ lo son.
8. Prueba que $k[x]$ es íntegramente cerrado en su cuerpo de fracciones.
9. ¿Cuál es la dimensión de Krull de $k[x,y,z,t]/(x^2+y^2+z^2+t^2-1)$?
10. Pon un ejemplo de variedad algebraica que sea la unión de dos componentes irreducibles no disjuntas, una de dimensión 2 y la otra de dimensión 1.
11. Sean U, V dos abiertos de una variedad algebraica X. Prueba que si el conjunto de puntos cerrados de U es igual al conjunto de puntos cerrados V, entonces $U = V$.
12. Sea X una variedad algebraica y C, C' dos cerrados. Prueba que si todo punto cerrado de C es un punto (cerrado) de C', entonces $C \subseteq C'$.
13. Sea $\operatorname{Spec} A$ una variedad algebraica. Prueba que $\operatorname{Spec} A$ es irreducible si y solo si $\operatorname{Spec}_{max} A$ es irreducible.
14. Sea X una variedad algebraica sobre un cuerpo algebraicamente cerrado. Prueba que X es irreducible si y solo si X_{rac} es irreducible.
15. Sea $\operatorname{Spec} A$ una variedad algebraica. Prueba que $\dim \operatorname{Spec}_{max} A = \dim A$.
16. Sea $X = \operatorname{Spec} A$ una variedad algebraica irreducible. Prueba que si $f \in A$ ni es invertible ni nilpotente, entonces $\dim(f)_0 = \dim X - 1$.

17. ¿Todas las cadenas de inclusiones de cerrados irreducibles maximales de una variedad algebraica irreducible tienen la misma longitud? Y si la variedad no es irreducible ¿también?

3.9. Problemas

1. Sean $f: A \to B$ y $f': A' \to B'$ dos morfismos de k-álgebras finitos. Prueba que el morfismo de k-álgebras $f \otimes f': A \otimes_k A' \to B \otimes_k B'$, $(f \otimes f')(a \otimes a') := f(a) \otimes f'(a')$ es finito.

2. Sea A un anillo íntegro y $a \in A$ ni invertible, ni nula. Prueba que el morfismo de localización $A \to A_a$ no es finito.

3. Sea $f: A \hookrightarrow B$ un morfismo de anillos entero y $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido en espectros.

   a) Si f es inyectivo, entonces f^* es epiyectivo.

   b) f^* es cerrado de fibras de dimensión cero.

4. Prueba que un morfismo de anillos $A \to B$ es finito si y solo si es entero y de tipo finito.

5. Sea $k \hookrightarrow K$ una extensión finita de cuerpos y $X = \operatorname{Spec} A$ una k-variedad algebraica. Prueba que el morfismo natural $X_K = \operatorname{Spec} A \otimes_k K \to X = \operatorname{Spec} A$ de cambio de base es epiyectivo y cerrado.

6. Contraejemplo de Nagata: Sea $A = k[x_1, x_2, \ldots, x_n, \ldots]$ el anillo de polinomios en infinitas variables. Sean $\mathfrak{p}_{y_i} = (x_{2^i}, \ldots, x_{2^{i+1}-1})$ y $S = A - \bigcup_{i \in \mathbb{N}} \mathfrak{p}_{y_i}$. Prueba:

   a) Si un ideal $I \subset \bigcup_{i \in \mathbb{N}} \mathfrak{p}_{y_i}$, entonces existe $m \in \mathbb{N}$ tal que $I \subseteq \mathfrak{p}_{y_m}$. Dado un ideal J no nulo existe solo un número finito de $i \in \mathbb{N}$ tal que $J \subseteq \mathfrak{p}_{y_i}$.

   b) $\operatorname{Spec} A_S = \bigcup_{i \in \mathbb{N}} \operatorname{Spec} A_{y_i}$.

   c) A_S es un anillo noetheriano.

   d) $\dim A_S = \infty$.

7. Sea $X = \operatorname{Spec} A$ una k-variedad algebraica. Prueba que $\dim X = 0 \iff \dim_k A < \infty$.

8. Calcula los ideales maximales de $\mathbb{C}[x_1, \ldots, x_n]$, de $\mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - 1)$ y de $\mathbb{C}[x, y]/(x^2 + y^2 - 1.x^3 + y^3 - 1)$.

9. Prueba que todo ideal maximal de $k[x_1,\dots,x_n]$ está generado por n polinomios ¿Puede estar generado por $n-1$ polinomios?

10. Calcula la multiplicidad de intersección en el origen de la curva $y^2 = x^2 + y^3$ con la curva $y^3 + x^2 = 0$. Es decir, calcula $\dim_{\mathbb{C}}(\mathbb{C}[x,y]/(y^2 - x^2 - y^3, y^3 + x^2))_{or}$, donde $\mathfrak{m}_{or} = (\bar{x}, \bar{y})$.

11. Sea $X = \operatorname{Spec} B$ una variedad algebraica íntegra sobre un cuerpo algebraicamente cerrado e $Y = \operatorname{Spec} A$ otra variedad algebraica. Sean $f, g\colon A \to B$ dos morfismos de k-álgebras y f^*, g^* los morfimos inducidos en espectros y f^*_{rac}, g^*_{rac} los morfismos inducidos en los espectros racionales. Prueba:

    a) Si $C = \{x \in X_{rac}$ tales que $f^*(x) = g^*(x)\}$, entonces C es un cerrado de X_{rac} y $\bar{C}$ es el mayor cerrado de X sobre el que coinciden f^* y g^*

    b) Si $f^*_{rac} = g^*_{rac}$ entonces $f = g$. .

12. Sea $k \hookrightarrow K$ una extensión de cuerpos. Si $X = \operatorname{Spec} A$ es una variedad k-algebraica irreducible de dimensión n, prueba que todas las componentes irreducibles de $X \times_k K := \operatorname{Spec}(A \otimes_k K)$ son de dimensión n.

13. Sean A y B k-álgebras de tipo finito, $f : A \to B$ un morfismo de k-álgebras plano y $f^* :\ \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación inducida. Supongamos que $\operatorname{Spec} B$ es irreducible, $x \in \operatorname{Spec} B$ un punto cerrado e $y = f^*(x)$. Prueba que

$$\dim f^{*-1}(y) = \dim \operatorname{Spec} B - \dim \operatorname{Spec} A.$$

14. Prueba que si X e Y son variedades algebraicas irreducibles sobre un cuerpo k algebraicamente cerrado, entonces $X \times_k Y$ es irreducible. (Indicación: Usa el teorema de los ceros de Hilbert).

15. Sean X e Y variedades algebraicas irreducibles. Prueba que todas las componentes irreducibles de $X \times Y$ son de dimensión $\dim X + \dim Y$.

16. Prueba que si X e Y son variedades algebraicas íntegras sobre un cuerpo k algebraicamente cerrado de característica cero, entonces $X \times_k Y$ es íntegra[3].

17. Sea $X = \operatorname{Spec} A$ una variedad íntegra sobre un cuerpo k algebraicamente cerrado de característica cero. Prueba que para toda extensión de cuerpos $k \to K$, la variedad $X_K = \operatorname{Spec}(A \otimes_k K)$ es íntegra. (Pista: K es unión de álgebras de tipo finito).

[3] Si $\operatorname{car} k = p > 0$, entonces $X \times_k Y$ también es íntegra

18. En la curva plana compleja de ecuación $x^2+y^2=9$, determina si la función $f(x,y)=(y-3)(x-5)$ divide a la función $g(x,y)=x(y^2+16)$ ¿divide $f(x,y)$ a alguna potencia de $g(x,y)$? ¿y si sustituimos el cuerpo de los números complejos por el de los números racionales?

19. 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 $Y\cap Y'\neq\emptyset$ y sea Z una componente irreducible de $Y\cap Y'$. Demuéstrese que

$$\operatorname{codim} Z \leq \operatorname{codim} Y + \operatorname{codim} Y'.$$

20. Sea $\bar{k}$ el cierre algebraico de k. Prueba que dos ideales radicales $I=(f_i)_{i\in I}$, $J=(g_j)_{j\in J}$ de $k[x_1,\dots,x_n]$ son iguales si y sólo si las soluciones en $\bar{k}$ de los dos sistemas de ecuaciones $\{f_i=0\}_{i\in I}$, $\{g_j=0\}_{j\in J}$ son las mismas.

21. Sea $A=k[x_1,\dots,x_n]/I$ y sea el mayor $r\in\mathbb{N}$ para el que existe un subconjunto $\{j_1,\dots,j_r\}\subseteq\{1,\dots,n\}$ de modo que el morfismo de k-álgebras $k[x_{j_1},\dots,x_{j_r}]\to A$, $p(x_{j_1},\dots,x_{j_r})\mapsto \overline{p(x_{j_1},\dots,x_{j_r})}$ es inyectivo. Prueba que $\dim A=r$.

22. Diremos que $\alpha=(\alpha_1,\dots,\alpha_n)\in \operatorname{Spec}_{rac} k[x_1,\dots,x_n]/(p(x_1,\dots,x_n))$ es no singular si $(\frac{\partial p}{\partial x_1}(\alpha),\dots,\frac{\partial p}{\partial x_n}(\alpha))\neq 0$. Prueba que α es un punto no singular $\iff \dim_k \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 = n-1 \iff$ existen $f_1,\dots,f_{n-1}\in A_X$ tales que $\mathfrak{m}_\alpha\cdot A_{X,\alpha}=(f_1,\dots,f_{n-1})$, donde $A_X=k[x_1,\dots,x_n]/(p(x_1,\dots,x_n))$.

23. Se dice que en general los puntos racionales de una variedad algebraica irreducible cumplen una propiedad si existe un abierto de la variedad cuyos puntos racionales cumplen la propiedad. Demuestra que en general las matrices cuadradas son invertibles. Sean A y B dos matrices cuadradas de orden n, prueba que $c_{A\cdot B}(x)=c_{B\cdot A}(x)$.

24. Demuestra el teorema de Cayley-Hamilton siguiendo el siguiente esquema: 1. Podemos suponer que el cuerpo es algebraicamente cerrado. 2. En general, las matrices cuadradas son diagonalizables. 3. Como $c_A(A)=0$ para toda matriz cuadrada invertible, en general, entonces $c_A(A)=0$ siempre.

25. Sean X, Y variedades algebraicas íntegras sobre un cuerpo k y sean Σ_X, Σ_Y sus respectivos cuerpos de funciones racionales. Si $\phi\colon Y\to X$ es un morfismo que transforma el punto genérico de Y en el punto genérico de X (lo que equivale a que tenga imagen densa), induce un morfismo de k-álgebras $\Sigma_X\to\Sigma_Y$. Diremos que ϕ es un morfismo de *grado* n cuando Σ_Y sea una extensión finita de

grado n de Σ_X. Los morfismos de grado 1 se llaman morfismos birracionales. Diremos que X e Y son birracionalmente equivalentes si sus cuerpos de funciones racionales son extensiones de k isomorfas: $\Sigma_X \simeq \Sigma_Y$. Las variedades algebraicas birracionalmente equivalentes al espacio afín se llaman racionales. Es decir, una variedad algebraica sobre k es racional si su cuerpo de funciones racionales es isomorfo a un cuerpo de fracciones racionales $k(x_1,\dots,x_n)$ con coeficientes en k.

a) Sea C la cúbica plana $y^2 = x^2 + x^3$. Consideremos la aplicación de C_{rac} en el haz de rectas que que pasa por el origen, que asigna a cada punto racional de C la recta que pasa por el origen y el punto racional. Define un morfismo de variedades algebraicas de un abierto de C en un abierto de $\mathbb{P}^1$, de modo que en los puntos racionales coincide con la aplicación definida.

El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcula la longitud del "ojo del lazo" definido por la curva $y^2 = x^2 + x^3$.

b) Sea C la cúbica plana $y^2 = x^3$. Prueba que el haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2$, $y = t^3$.

Capítulo 4

Variedades algebraicas proyectivas

4.1. Introducción

En Geometría Lineal el marco "afín" pronto se muestra excesivamente estrecho y es necesario la introducción de los espacios proyectivos. Lo mismo sucede en Geometría Algebraica, donde habrá que introducir el concepto de variedad proyectiva. Por poner un ejemplo de esta necesidad, digamos que el teorema de Bézout, que afirma que dos curvas planas de grados n y m, se cortan en $n \cdot m$ puntos, es un enunciado en el plano proyectivo, pues es necesario para la validez de este teorema considerar los puntos del infinito.

En Geometría Proyectiva el espacio proyectivo $\mathbb{P}(E)$ asociado a un espacio vectorial E se define como el conjunto de rectas (que pasan por el origen) de E. Así las rectas de E (que pasan por el origen) se corresponden biunívocamente con los puntos de $\mathbb{P}(E)$. En Geometría Algebraica vamos a definir de modo equivalente, a partir de $\mathbb{A}^{n+1} = \operatorname{Spec}\mathbb{C}[x_0,\dots,x_n]$, el espacio proyectivo n-dimensional. Las subvariedades V que vamos a considerar en $\mathbb{A}^{n+1}$ son las variedades homogéneas, es decir, las que contengan para todo punto cerrado $p \in V$ la recta que pasa por p y el origen, y tales que $V \neq \{\text{origen}\}$. Así, las subvariedades irreducibles homogéneas de dimensión mínima serán las rectas que pasan por el origen, que se corresponderán con los puntos cerrados del espacio proyectivo que queremos asociarle a $\mathbb{A}^{n+1}$.

Sea $p(x_0,\dots,x_n) \in \mathbb{C}[x_0,\dots,x_n]$ una función que se anula en una variedad homogénea V, escribamos $p(x_0,\dots,x_n) = p_s(x_0,\dots,x_n)+\cdots+p_m(x_0,\dots,x_n)$ como suma de polinomios homogéneos. Si $(a_0,\dots,a_n)$ es un punto de V, entonces también lo es $(\lambda a_0,\dots,\lambda a_n)$, luego

$$0 = p(\lambda a_0,\dots,\lambda a_n) = \lambda^s p_s(a_0,\dots,a_n)+\cdots+\lambda^m p_m(a_0,\dots,a_n), \quad \text{para todo } \lambda.$$

Por tanto, $p_i(a_0,\dots,a_n)$ se anula en V, para todo i. En conclusión, $V = (I)_0$, donde I

159

es un ideal generado por polinomios homogéneos. Es fácil ver el recíproco, es decir, si $V = (I)_0$ donde I es un ideal generado por polinomios homogéneos, entonces V es una variedad homogénea.

Sea $\mathbb{P}^n = \mathrm{Proj}\,\mathbb{C}[x_0,\ldots,x_n]$ el conjunto de los ideales primos homogéneos (es decir, generados por polinomios homogéneos) de $\mathbb{C}[x_0,\ldots,x_n]$, distintos de $(x_0,\ldots,x_n)$. Si consideramos en $\mathbb{P}^n$ la topología inducida por $\mathbb{A}^{n+1}$, entonces los puntos cerrados de $\mathbb{P}^n$ se corresponden con las variedades homogéneas de $\mathbb{A}^{n+1}$ de dimensión mínima, que son justamente las rectas de $\mathbb{A}^{n+1}$ que pasan por el origen.

En Geometría Proyectiva se demuestra que $\mathbb{P}^n$ está recubierto por los subconjuntos $U_i^h := \{\text{rectas de } \mathbb{C}^{n+1} \text{ que pasan por el origen y no yacen en el hiperplano } x_i = 0\}$ y que éstos se corresponden con los puntos del espacio afín $\mathbb{A}^n$, del modo siguiente: El morfismo

$$\mathbb{A}^{n+1}\setminus\{x_i = 0\} \to \mathbb{A}^n,\ (\alpha_0,\ldots,\alpha_n) \mapsto (\frac{\alpha_0}{\alpha_i},\ldots,\frac{\alpha_n}{\alpha_i})$$

tiene por fibras las rectas que pasan por el origen y no yacen en el hiperplano $x_i = 0$, es decir, induce la igualdad

$$U_i^h = \{\text{rectas } \langle(\alpha_0,\ldots,\alpha_n)\rangle \mid \alpha_i \neq 0\} \longrightarrow\!\!\!\!\!\!= \mathbb{A}^n$$

$$\langle(\alpha_0,\ldots,\alpha_n)\rangle \longmapsto (\tfrac{\alpha_0}{\alpha_i},\ldots,\tfrac{\alpha_n}{\alpha_i})$$

En Geometría Algebraica, si $U_{x_i}^h := \{x \in \mathrm{Proj}\,\mathbb{C}[x_0,\ldots,x_n],\ x \notin (x_i)_0\}$ probaremos que la composición de los morfismos

$$U_{x_i}^h \hookrightarrow \mathbb{A}^{n+1} - (x_i)_0 \longrightarrow \mathbb{A}^n$$

$$(\alpha_0,\ldots,\alpha_n) \longmapsto (\tfrac{\alpha_0}{\alpha_i},\ldots,\tfrac{\alpha_n}{\alpha_i})$$

$$\mathbb{C}[x_0,\ldots,x_n]_{x_i} \hookleftarrow \mathbb{C}[\tfrac{x_0}{x_i},\ldots,\tfrac{x_n}{x_i}]$$

induce un homeomorfismo $U_{x_i}^h \simeq \mathrm{Spec}\,\mathbb{C}[\frac{x_0}{x_i},\ldots,\frac{x_n}{x_i}]$. Además probaremos que $\mathbb{P}^n = \bigcup_i U_{x_i}^h$ y que $\mathbb{A}^{n+1} - (x_i)_0 = \mathbb{A}^n \times (\mathbb{A}^1 - \{0\})$.

Las variedades proyectivas son un buen ejemplo de variedad algebraica no afín. No es difícil proceder en Geometría Algebraica como se procede en Geometría Diferencial, y definir el concepto de variedad algebraica general mediante el uso de un atlas o cartas de abiertos (que sean variedades algebraicas afines). Por ejemplo, ¿cómo definiríamos $\mathbb{P}^1 \times \mathbb{P}^1$? Diríamos

$$\mathbb{P}^1 \times \mathbb{P}^1 := U_{x_0}^h \times U_{x_0}^h \cup U_{x_0}^h \times U_{x_0}^h \cup U_{x_1}^h \times U_{x_1}^h \cup U_{x_1}^h \times U_{x_1}^h$$

donde $(U^h_{x_i} \times U^h_{x_j}) \cap (U^h_{x_r} \times U^h_{x_s}) = (U^h_{x_i} \cap U^h_{x_r}) \times (U^h_{x_j} \cap U^h_{x_s})$. De modo inmediato surgirá la necesidad de definir para cada abierto U de la variedad algebraica el anillo de las funciones algebraicas del abierto. Necesitaremos hablar de los haces de funciones algebraicas, teoría que no abordaremos en esta asignatura.

4.2. Álgebras graduadas

Procedamos ahora con todo rigor y generalidad.

1. Definición: Sea R un anillo y supongamos que como grupo, con la operación $+$, es suma directa de subgrupos R_i, con $i \in \mathbb{Z}$. Diremos que el anillo $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ es un álgebra graduada, si para cada $r_i \in R_i$ y $r_j \in R_j$, se cumple que $r_i \cdot r_j \in R_{i+j}$. Diremos que $r_i \in R_i$ es un elemento homogéneo de grado i.

2. Ejemplo: $k[x_1,\dots,x_m]$ es álgebra graduada como sigue: Para $n \geq 0$,

$$k[x_1,\dots,x_m]_n := \langle x^\alpha;\ \forall\, \alpha \in \mathbb{N}^m \text{ tal que } |\alpha| := \alpha_1 + \cdots + \alpha_m = n\rangle_k.$$

y $k[x_1,\dots,x_m]_n := 0$, para $n < 0$.

3. Si R es un álgebra graduada, entonces $1 \in R$ es un elemento homogéneo de grado cero: Escribamos $1 = \sum_{i=-n}^{n} f_n$, con $n \in \mathbb{N}$ y $f_i \in R_i$. Multiplicando en la igualdad por cualquier $g_m \in R_m$, obtenemos $g_m = \sum_{i=-n}^{n} g_m \cdot f_n$, luego $g_m \cdot f_i = 0$ para todo $i \neq 0$ y todo g_m, luego $f_i = 0$, para todo $i \neq 0$ y $1 = f_0 \in R_0$.

4. Definición: Sea $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo, si está generado por elementos homogéneos.

5. Proposición: *Sea R un álgebra graduada e $I \subset R$ un ideal. Las siguientes afirmaciones sin equivalentes:*

1. *I es un ideal homogéneo.*
2. *$I = \oplus I_n$, siendo $I_n := I \cap R_n$ los elementos homogéneos de I de grado n.*
3. *Si $f = f_n + f_{n+1} + \cdots + f_{n+m} \in I$, entonces $f_n,\dots,f_{n+m} \in I$.*

Demostración. $\oplus I_n \subset I$ y es un ideal homogéneo de R. Dejamos la demostración como ejercicio al lector.

□

6. Ejercicio: Prueba que la intersección de un número arbitrario de ideales homogéneos es un ideal homogéneo.

7. Ejercicio: Prueba que un ideal homogéneo $\mathfrak{p} \subseteq R$ es primo si y solo si cumple que si el producto de dos elementos homogéneos pertenece a $\mathfrak{p}$ entonces uno de los dos pertenece a $\mathfrak{p}$.

8. Proposición: *Sea R una álgebra graduada y $\mathfrak{p} \subset R$ un ideal primo. El ideal homogéneo $\mathfrak{q} = \bigoplus_{n\in\mathbb{Z}} (\mathfrak{p} \cap R_n)$ es primo. Por lo tanto, los ideales primos minimales de R son homogéneos.*

Demostración. Si $f_n \cdot f_m \in \mathfrak{q}$, entonces $f_n \cdot f_m \in \mathfrak{p}$, luego $f_n \in \mathfrak{p}$ o $f_m \in \mathfrak{p}$, por tanto, $f_n \in \mathfrak{q}$ o $f_m \in \mathfrak{q}$. □

9. Definición: Diremos que un morfismo de álgebras $\phi\colon R \to R'$ entre álgebras graduadas es graduado (de grado r) si transforma funciones homogéneas de grado n en funciones homogéneas de grado nr, para todo $n \in \mathbb{Z}$.

10. Si $I = \bigoplus_{n\in\mathbb{Z}} I_n$ es un ideal homogéneo de R, entonces R/I es un álgebra graduada de modo natural: $[R/I]_n := \{\bar{r}_n, \forall r_n \in R_n\}$.

En efecto, , $R/I = \bigoplus_{n\in\mathbb{Z}} R_n/I_n = \bigoplus_{n\in\mathbb{Z}} [R/I]_n$. Además, si $\bar{r}_n \in [R/I]_n$ y $\bar{r}_m \in [R/I]_m$, entonces $\bar{r}_n \cdot \bar{r}_m = \overline{r_n \cdot r_m} \in [R/I]_{n+m}$.

El morfismo de paso al cociente $R \to R/I$ es un morfismo graduado (de grado 1).

11. Ejemplo: Sea $\alpha \in k^{n+1}$ no nulo y $p(x_0,\dots,x_n) \in k[x_0,\dots,x_n]$ homogéneo. Para cierto i se cumple que $\alpha_i \neq 0$ y $p = \sum_{j\neq i} h_j \cdot (x_j - \frac{\alpha_j}{\alpha_i} x_i) + q(x_i)$. Por tanto, $p(\alpha) = 0$ si y solo si $q = 0$, es decir, si y solo si $p(x_0,\dots,x_n) \in \mathfrak{p}_{[\alpha]} := (\alpha_j x_k - \alpha_k x_j)_{0\leq j,k\leq n} = (\alpha_j x_i - \alpha_i x_j)_{0\leq j\leq n}$. Por tanto, el morfismo $k[x_0,\dots,x_n]/\mathfrak{p}_{[\alpha]} \to k[x_i]$, $\bar{x}_j \mapsto \frac{\alpha_j}{\alpha_i} x_i$ es isomorfismo. Luego, $\mathfrak{p}_{[\alpha]}$ es un ideal primo homogéneo. El único ideal primo homogéneo que contiene estrictamente a $\mathfrak{p}_{[\alpha]}$ es el ideal $(x_0,\dots,x_n)$, ya que el único ideal primo homogéneo de $k[x_i]$ que contiene estrictamente a (0) es (x_i).

Observemos que $(\mathfrak{p}_{[\alpha]})_0^{rac}$ se identifica con los puntos de las recta que pasa por α y el origen, cuyas ecuaciones son $x_j - \frac{\alpha_j}{\alpha_i} x_i = 0$, para todo $j \neq i$. Si $0 \neq \alpha' \in k^{n+1}$ está en esta recta, es decir, existe $\lambda \in k$ tal que $\alpha' = \lambda \cdot \alpha$, entonces $\mathfrak{p}_{[\alpha']} = \mathfrak{p}_{[\alpha]}$. Si $0 \neq \beta \in k^{n+1}$, no está en esta recta, entonces $(\mathfrak{p}_{[\beta]})_0^{rac} \neq (\mathfrak{p}_{[\alpha]})_0^{rac}$ y $\mathfrak{p}_{[\beta]} \neq \mathfrak{p}_{[\alpha]}$.

12. Sea R un álgebra graduada y $S \subset R$ un sistema multiplicativo formado por elementos homogéneos. R_S es un álgebra graduada de modo natural:

$$[R_S]_n := \{\frac{r_{n+m}}{s_m} \in R_S, \forall\, r_{n+m} \in R_{n+m}, \forall\, s_m \in S \cap R_m\}.$$

En efecto, dados $\frac{f_{n+m}}{s_m}, \frac{g_{n+m'}}{t_{m'}} \in [R_S]_n$, entonces $\frac{f_{n+m}}{s_m} + \frac{g_{n+m'}}{t_{m'}} = \frac{t_{m'} f_{n+m} + s_m g_{n+m'}}{s_m t_{m'}} \in [R_S]_n$. Dado $\frac{f}{s_m} \in R_S$, $\frac{f}{s_m} = \frac{f_r + f_{r+1} + \cdots + f_s}{s_m} = \frac{f_r}{s_m} + \frac{f_{r+1}}{s_m} + \cdots + \frac{f_s}{s_m} \in \sum_n [R_S]_n$. Si $\sum_n \frac{f_{n+m_n}}{s_{m_n}} = 0$, entonces $\frac{\sum_n s_n \cdot f_{n+m_n}}{1} = 0$, con $s_n = \prod_{r \neq n} s_{m_r}$ y existe $t \in S$ tal que $\sum_n t \cdot s_n \cdot f_{n+m_n} = 0$. Sea $s = \operatorname{gr} \prod_m s_{m_n}$, entonces $\operatorname{gr}(t \cdot s_n \cdot f_{n+m_n}) = \operatorname{gr} t + s + n$. Por tanto, $t \cdot s_n \cdot f_{n+m_n} = 0$, para todo n y $\frac{f_{n+m_n}}{s_{m_n}} = 0$, para todo n. En conclusión, $R_S = \oplus_n [R_S]_n$.

El morfismo de localización $R \to R_S$ es un morfismo graduado (de grado 1).

4.3. Espectro proyectivo

1. Definición: Llamaremos ideal irrelevante de R al ideal $(\oplus_{n \neq 0} R_n) \subseteq R$.

2. Ejemplo: El ideal irrelevante de $k[x_0, x_1, \ldots, n]$ es $(x_0, x_1, \ldots, x_n)$.

Si $f_n \in R_n$, con $n \neq 0$, es invertible entonces el ideal irrelevante de R es R.

3. Definición: Llamaremos espectro proyectivo de R, y lo denotaremos $\operatorname{Proj} R$, al conjunto de ideales primos homogéneos de R que no contienen al ideal irrelevante.

Si R_0 es un cuerpo, entonces todo ideal primo homogéneo está incluido en $\oplus_{n \neq 0} R_n$, luego $\operatorname{Proj} R = \{x \in \operatorname{Spec} R : \mathfrak{p}_x \text{ homogéneo y } \mathfrak{p}_x \subsetneq \oplus_{n \neq 0} R_n\}$.

4. Definición: Llamaremos espacio proyectivo de dimensión n (sobre k) a

$$\mathbb{P}_k^n := \operatorname{Proj} k[x_0, \ldots, x_n] = \{\text{Ideales primos homogéneos } \mathfrak{p} \subsetneq (x_0, \ldots, x_n)\}.$$

5. Ejemplo: $\mathbb{P}_k^0 = \operatorname{Proj} k[x_0] = \{(0)\}$, es decir, es un único punto.

6. Ejemplo: $\mathbb{P}_{\mathbb{C}}^1 = \operatorname{Proj} k\mathbb{C}[x_0, x_1] = \{(0), (p_n(x,y)) \text{ con } p_n(x,y) \text{ irreducible y homogéneo}\}$. Como

$$p_n(x_0, x_1) = x_0^n p_n(1, \frac{x_1}{x_0}) = x_0^n \prod_{i=1}^n (a_i \frac{x_1}{x_0} + b_i) = \prod_{i=1}^n (a_i x_1 + b_i x_0)$$

es irreducible, entonces $n = 1$ y

$$\mathbb{P}_{\mathbb{C}}^1 = \begin{cases} (0) \\ (ax_1 + bx_0), \ \forall (a,b) \in \mathbb{C}^2 - \{(0,0)\} \end{cases}$$

7. Evidentemente $\operatorname{Proj} R \subset \operatorname{Spec} R$. Consideraremos $\operatorname{Proj} R$ como espacio topológico con la topología inicial heredada de la topología de Zariski de $\operatorname{Spec} R$. Por tanto, los cerrados de $\operatorname{Proj} R$ son $(I)_0^h := (I)_0 \cap \operatorname{Proj} R := \{x \in \operatorname{Proj} R : I \subseteq \mathfrak{p}_x\}$. Si I' es el ideal homogéneo mínimo conteniendo a I, entonces $(I)_0^h = (I')_0^h$. Además, $(I')_0^h = \bigcap_{f \in I', \text{homog}} (f)_0^h$. Por tanto, una base de cerrados de $\operatorname{Proj} R$ son los cerrados $(f)_0^h$, con f homogéneo; y una base de abiertos de la topología de $\operatorname{Proj} R$ son los abiertos

$$U_f^h := \operatorname{Proj} R \setminus (f)_0^h = \{x \in \operatorname{Proj} R, f \notin \mathfrak{p}_x\}, \qquad (f \text{ homogéneo}).$$

8. Si $C \subset \operatorname{Proj} R$ es un cerrado, entonces $I_C = \{f \in R : f \in \mathfrak{p}_x, \forall x \in C\}$ es un ideal homogéno y $C = (I_C)_0^h$. Si C es irreducible, entonces $I_C = \mathfrak{p}_x$ es un ideal primo homogéneo y $C = \bar{x} \subset \operatorname{Proj} R$. Todo subespacio de un espacio noetheriano es noetheriano. Si R es noetheriano, entonces $\operatorname{Proj} R \subseteq \operatorname{Spec} R$, es un espacio noetheriano. En particular, $\operatorname{Proj} R$ es unión de un número finito de cerrados irreducibles, luego $\operatorname{Proj} R = \bar{x}_1 \cup \cdots \cup \bar{x}_r$, siendo $\mathfrak{p}_{x_1}, \ldots, \mathfrak{p}_{x_r}$ los ideales primos homogéneos minimales de R (que no contengan al irrelevante).

Un punto $x \in \operatorname{Proj} R \subset \operatorname{Spec} R$ es cerrado si y solo si $\mathfrak{p}_x$ es un ideal primo homogéneo maximal (entre los ideales primos homogéneos que no contienen al ideal irrelevante).

9. Ejemplo: Consideremos en $\mathbb{C}^{n+1} - \{(0,\ldots,0)\}$ la siguiente relación de equivalencia: $\alpha \sim \beta$ si y solo existe $\lambda \in \mathbb{C}$ tal que $\alpha = \lambda\beta$. La aplicación

$$\begin{array}{rcl} \mathbb{C}^{n+1} - \{(0,\ldots,0)\}/\sim & \longrightarrow & \{\text{Puntos cerrados de } \mathbb{P}^n_{\mathbb{C}}\} \\ [(\alpha_0,\ldots,\alpha_n)] & \longmapsto & \mathfrak{p}_{[\alpha]} := (\alpha_i x_j - \alpha_j x_i)_{ij} \end{array}$$

es biyectiva: Por el ejemplo 4.2.11, nos falta probar que si $z \in \mathbb{P}^n_{\mathbb{C}}$ es un punto cerrado de $\mathbb{P}^n_{\mathbb{C}}$ entonces $\mathfrak{p}_z = \mathfrak{p}_{[\alpha]}$ para algún α. Sea $0 \neq \alpha \in \mathbb{C}^{n+1}$ un punto cerrado de $\bar{z} = (\mathfrak{p}_z)_0 \in \operatorname{Spec} \mathbb{C}[x_0,\ldots,x_n]$. El ideal generado por todas las funciones homogéneas que se anulan en α, contiene a $\mathfrak{p}_{[\alpha]}$, luego ha de coincidir con éste; y $\mathfrak{p}_z$, que lo contiene, ha de coincidir con $\mathfrak{p}_{[\alpha]}$.

10. Si $\phi\colon R \to R'$ es un morfismo graduado entonces el morfismo $\phi^*\colon \operatorname{Spec} R' \to \operatorname{Spec} R$ inducido, aplica ideales primos homogéneos en ideales primos homogéneos. Sea $C = (\bigoplus_{n \neq 0} \phi(R_n))_0$, tenemos definido un morfismo

$$\begin{array}{rcll} \phi^*\colon \operatorname{Proj} R' \setminus C & \to & \operatorname{Proj} R & \\ x & \mapsto & \phi^*(x), & \text{donde } \mathfrak{p}_{\phi^*(x)} = \phi^{-1}(\mathfrak{p}_x). \end{array}$$

11. Ejemplo: Sea $\phi\colon k[x_0,x_1,x_2] \to k[x_0,x_1,x_2]$, $\phi(x_i) = \sum_j \lambda_{ij}x_j$ un morfismo de k-algebras tal que $\det(\lambda_{ij}) \neq 0$. Entonces, ϕ es un isomorfismo graduado, que induce un isomorfismo $\phi^*\colon \mathbb{P}^2_k \to \mathbb{P}^2_k$.

12. Proposición: *Sea I un ideal homogéneo de R. El morfismo de paso al cociente $R \to R/I$ es un morfismo graduado que induce un homeomorfismo*

$$\operatorname{Proj}(R/I) = (I)_0^h.$$

Demostración. En la igualdad $\operatorname{Spec}(R/I) = (I)_0$, los ideales primos homogéneos de R/I se corresponden con los ideales primos homogéneos de R que contienen a I. □

13. Ejemplo: Sea $X = \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]/(p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n))$. Establezcamos en $\mathbb{C}^{n+1}-\{0\}$ la relación de equivalencia: $\alpha \sim \alpha'$ si existe $\lambda \in k$ tal que $\alpha' = \lambda\cdot\alpha$. La aplicación

$$\begin{array}{ccc} \left\{\alpha \in \mathbb{C}^{n+1}-\{0\}\colon \begin{array}{c} p_1(\alpha)=0 \\ \cdots \\ p_r(\alpha)=0 \end{array}\right\}/\sim & \longrightarrow & \{\text{Puntos cerrados de } X\} \\ [(\alpha_0,\dots,\alpha_n)] & \longmapsto & (\alpha_j\bar{x}_i - \alpha_i\bar{x}_j)_{ij} \end{array}$$

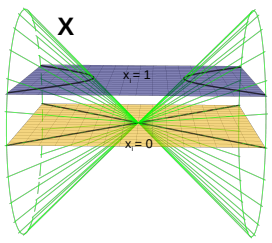
es biyectiva: Sabemos que un polinomio homogéneo $p \in \mathbb{C}[x_0,\dots,x_n]$ cumple que $p(\alpha) = 0$ si y solo si $p \in \mathfrak{p}_{[\alpha]} := (\alpha_i x_j - \alpha_j x_i)_{ij}$. Denotemos $I = (p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n))$. Tenemos que

$$\begin{aligned} \{\text{Puntos cerrados de } X\} &= \{\text{Puntos cerrados de } (I)_0^h\} = \{\mathfrak{p}_{[\alpha]} \in \operatorname{Proj}\mathbb{C}[x_0,\dots,x_n]\colon I \subseteq \mathfrak{p}_{[\alpha]}\} \\ &= \{\alpha \in \mathbb{C}^{n+1}-\{0\}\colon p_i(\alpha) = 0,\ \forall i\}/\sim. \end{aligned}$$

14. Proposición: *Sea $f \in R$ un elemento homogéneo. El morfismo de localización $R \to R_f$ es un morfismo graduado que induce un homeomorfismo*

$$\operatorname{Proj} R_f = U_f^h.$$

Demostración. En la igualdad $\operatorname{Spec} R_f = U_f$, los ideales primos homogéneos de R_f se corresponden con los ideales primos homogéneos de R que no contiene a f. □



El conjunto de rectas que pasan por el origen de una variedad homogénea X, que no yacen en el plano $x_i = 0$, se identifica el conjunto de los puntos de corte del plano $x_i - 1 = 0$ con la variedad homogénea. Además,

$$X - \{x_i = 0\} = (X \cap \{x_i - 1 = 0\}) \times (\mathbb{A}^1 - \{0\}).$$

Con rigor y detalle:

15. Sea R una álgebra graduada. La aplicación

$$\begin{array}{ccc} \operatorname{Spec} R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \operatorname{Proj} R \\ \mathfrak{p} & \longmapsto & \underset{n\in\mathbb{N}}{\oplus} [\mathfrak{p}]_n \end{array}$$

es continua, ya que para cada $f \in R_n$, $\pi_R^{-1}((f)_0^h) = (f)_0 \cap (\operatorname{Spec} R - (\underset{n\neq 0}{\oplus} R_n)_0)$. En particular, para toda $f \in R_n$, con $n \neq 0$, $\pi_R^{-1}(U_f^h) = U_f$. Evidentemente, el diagrama

$$\begin{array}{ccc} \operatorname{Spec} R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \operatorname{Proj} R \\ \uparrow & & \uparrow \\ \operatorname{Spec} R_f & \xrightarrow{\pi_{R_f}} & \operatorname{Proj} R_f \end{array}$$

es conmutativo. Si $\varphi\colon R \simeq S$ es un isomorfismo de álgebras graduadas, el diagrama

$$\begin{array}{ccc} \operatorname{Spec} R - (\underset{n\neq 0}{\oplus} R_n)_0 & \xrightarrow{\pi_R} & \operatorname{Proj} R \\ \varphi^* \uparrow \wr & & \wr \uparrow \varphi^* \\ \operatorname{Spec} S - (\underset{n\neq 0}{\oplus} S_n)_0 & \xrightarrow[\pi_S]{} & \operatorname{Proj} S \end{array}$$

es conmutativo.

Si R es una álgebra graduada, entonces R_0 es un subanillo.

16. Proposición: *Sea $f \in R$ homogénea de grado 1, entonces*

1. $\varphi\colon \operatorname{Proj} R_f \to \operatorname{Spec}[R_f]_0$, $\mathfrak{p} \mapsto [\mathfrak{p}]_0$ *es un homeomorfismo.*
2. *El morfismo de $[R_f]_0$-álgebras $\phi\colon [R_f]_0 \otimes_{\mathbb{Z}} \mathbb{Z}[x, 1/x] \to R_f$, $x \mapsto f$ es un isomorfismo y tenemos el diagrama conmutativo*

$$\begin{array}{ccc} \operatorname{Spec} R_f & \xrightarrow{\pi_{R_f}} & \operatorname{Proj} R_f \\ \phi^* \| & & \| \varphi \\ \operatorname{Spec}[R_f]_0 \times_{\mathbb{Z}} (\mathbb{A}^1_{\mathbb{Z}} - \{0\}) & \xrightarrow[\pi_1]{} & \operatorname{Spec}[R_f]_0 \end{array}$$

donde π_1 es la proyección en el primer factor.

3. $[R_f]_0 \simeq R/(f-1)$*, luego* $\operatorname{Proj} R_f = \operatorname{Spec}[R_f]_0 \simeq \operatorname{Spec} R/(f-1) = (f-1)_0$.

Demostración. Denotemos $S = R_f$.

1. y 2. El morfismo $S_0[x,1/x] \to S$, $x \mapsto f$ es un isomorfismo graduado, porque el morfismo inverso es $\frac{r_n}{f^m} \mapsto \frac{r_n}{f^n} \cdot x^{n-m}$. Podemos suponer que $S = S_0[x,1/x]$ y $f = x$.

La composición φ de las aplicaciones continuas naturales

$$\operatorname{Proj} S_0[x,1/x] \hookrightarrow \operatorname{Spec} S_0[x,1/x] \to \operatorname{Spec} S_0,$$

que asigna a cada ideal primo homogéneo $\mathfrak{q} \subset S_0[x,1/x]$ el ideal primo $[\mathfrak{q}]_0 := \mathfrak{q} \cap S_0$ es un homeomorfismo: Si $\mathfrak{q}$ es un ideal primo homogéneo de $S_0[x,1/x]$, entonces $\mathfrak{q} = \bigoplus_n [\mathfrak{q}]_0 \cdot x^n$. Si $\mathfrak{q}_0$ es un ideal primo de S_0 entonces $\mathfrak{q} := \bigoplus_n \mathfrak{q}_0 \cdot x^n$ es un ideal primo de $S_0[x,1/x]$ y $[\mathfrak{q}]_0 = \mathfrak{q}_0$. Por tanto, φ es biyectiva. Es un homeomorfismo porque aplica cerrados en cerrados. En efecto, $\varphi((s_0 \cdot x^n)_0^h) = \varphi((s_0)_0^h = (s_0)_0$ (para todo $s_0 \in S_0$ y $n \in \mathbb{N}$). Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \operatorname{Spec} S_0[x,1/x]) & \xrightarrow{\pi_{S_0[x,1/x]}} & \operatorname{Proj} S_0[x,1/x] \\ \| & & \| \varphi \\ \operatorname{Spec} S_0 \times_{\mathbb{Z}} (\mathbb{A}^1 - \{0\}) & \xrightarrow[\pi_1]{} & \operatorname{Spec} S_0 \end{array} \qquad \begin{array}{ccc} \mathfrak{q} & \longmapsto & \bigoplus_n [\mathfrak{q}]_n \\ & \searrow & \downarrow \\ & & [\mathfrak{q}]_0 \end{array}$$

3. $R/(f-1) = S/(f-1) = S_0[x,1/x]/(x-1) = S_0$. □

Si A es una k-álgebra, entonces $A \otimes_{\mathbb{Z}} \mathbb{Z}[x,1/x] = A \otimes_k k \otimes_{\mathbb{Z}} \mathbb{Z}[x,1/x] = A \otimes_k k[x,1/x]$, luego $\operatorname{Spec} A \times_{\mathbb{Z}} (\mathbb{A}^1_{\mathbb{Z}} - \{0\}) = \operatorname{Spec} A \times_k (\mathbb{A}^1_k - \{0\})$.

4.3.1. Variedades algebraicas proyectivas

17. Definición: Llamaremos variedad algebraica proyectiva (sobre k) al espectro proyectivo de un álgebra graduada del tipo $k[\xi_0,\dots,\xi_n] = k[x_0,\dots,x_n]/I$, siendo I un ideal homogéneo. Es decir, una variedad proyectiva es un cerrado del espacio proyectivo $\mathbb{P}^n_k$.

Por sencillez, siempre que escribamos $k[\xi_0,\dots,\xi_n]$ supondremos que cada ξ_i es de grado 1.

Se cumple que $[k[\xi_0,\dots,\xi_n]_{\xi_i}]_0 = k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, donde $k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$ es la k-subálgebra de $R_0[\xi_0,\dots,\xi_n]_{\xi_i}$ generada por $\xi_0/\xi_i,\dots,\xi_n/\xi_i$.

Denotaremos el ideal irrelevante $\mathfrak{m}_{or} = (\xi_0,\dots,\xi_n) \subset k[\xi_0,\dots,\xi_n]$.

18. Teorema: *Se cumple que*

1. $\operatorname{Proj} k[\xi_0,\dots,\xi_n] = \bigcup_{i=0}^n U^h_{\xi_i}$.

2. $U^h_{\xi_i} = \operatorname{Spec} k[\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}] = \operatorname{Spec} k[\xi_0, \ldots, \xi_n]/(\xi_i - 1)$.

3. *Sea* $\pi\colon \operatorname{Spec} k[\xi_0, \ldots, \xi_n] - \{or\} \longrightarrow \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$, $\mathfrak{p} \mapsto \bigoplus_{m \in \mathbb{N}} [\mathfrak{p}]_m$. *Entonces,*

$$\pi^{-1}(U^h_{\xi_i}) = U_{\xi_i} = U^h_{\xi_i} \times (\mathbb{A}^1 - \{0\}).$$

Demostración. 1. $\operatorname{Proj} k[\xi_0, \ldots, \xi_n] = \bigcup_{i=0}^{n} U^h_{\xi_i}$, ya que $\bigcap_{i=0}^{n} (\xi_i)^h_0 = (\xi_0, \ldots, \xi_n)^h_0 = \emptyset$.

2. y 3. son consecuencia de la proposición 4.3.16.

□

19. Observación: Vía las iguald. $U^h_{\xi_i} = \operatorname{Spec} R_0[\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}] = \operatorname{Spec} R_0[\xi_0, \ldots, \xi_n]/(\xi_i - 1)$, tenemos

$$\begin{aligned}(q_1(\xi_0, \ldots, \xi_n), \ldots, q_r(\xi_0, \ldots, \xi_n))^h_0 \cap U^h_{\xi_i} &= (q_1(\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}), \ldots, q_r(\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}))_0 \\ &= (q_1(\xi_0, \ldots, \overset{i}{1}, \ldots, \xi_n), \ldots, q_r(\xi_0, \ldots, \overset{i}{1}, \ldots, \xi_n))_0.\end{aligned}$$

20. Un subconjunto C de un espacio topológico X es cerrado si y solo si dada un recubrimiento $\{U_i\}$ por abiertos de X, se cumple que $U_i \cap C$ es un cerrado de U_i, para todo i. Sea $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ una variedad proyectiva. Si $U \subset X$ es un abierto y $x \in U$ es un punto cerrado de U, entonces x es un punto cerrado de X: Sea $\{U^h_{\xi_i}\}$ un recubrimiento de X, entonces x es un punto cerrado de $x \in U^h_{\xi_i} \cap U$ (para todo i, tal que $x \in U^h_{\xi_i}$), luego es un punto cerrado de $U^h_{\xi_i}$. Por tanto, $\{x\} \cap U^h_{\xi_i}$ es un cerrado para todo i, luego x es un punto cerrado de X.

21. Proposición: *Dos cerrados* C, C' *de una variedad proyectiva* $\operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ *son iguales si y solo si tienen los mismos puntos cerrados.*

Demostración. Si C tiene los mismos puntos cerrados que C', entonces $C \cap U^h_{\xi_i}$ tiene los mismos puntos cerrados que $C' \cap U^h_{\xi_i}$, luego $C \cap U^h_{\xi_i} = C' \cap U^h_{\xi_i}$, para todo i, luego $C = C'$. □

22. Proposición: *Si* $f_m \in k[\xi_0, \ldots, \xi_n]$ *es una función homogénea tal que para todo punto cerrado* $z \in \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$, $f_m(z) = 0$ *(es decir,* $f_m \in \mathfrak{p}_z$*), entonces* f_m *es nilpotente.*

Demostración. Como {Conjunto de puntos cerrados de $(f_m)^h_0$} = {Conjunto de puntos cerrados de $\operatorname{Proj} k[\xi_0, \ldots, \xi_n]$}, entonces $(f_m)^h_0 = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$, luego f_m pertenece a todos los ideales primos minimales de $k[\xi_0, \ldots, \xi_n]$, luego es nilpotente. □

23. Si $z \in Z = \operatorname{Spec} A$, denotaremos $\mathcal{O}_{Z,z} = A_z$. Si $z \in U_a \subset \operatorname{Spec} A = Z$, entonces $\mathcal{O}_{U_a,z} = A_z = \mathcal{O}_{Z,z}$. Sea $x \in \operatorname{Spec} k[\frac{\xi_0}{\xi_i}, \dots, \frac{\xi_n}{\xi_i}] = U^h_{\xi_i} \subset X = \operatorname{Proj} k[\xi_0, \dots, \xi_n]$, denotaremos $\mathcal{O}_{X,x} := \mathcal{O}_{U^h_{\xi_i},x}$. Si $x \in U^h_{\xi_j}$, entonces $U^h_{\xi_i} \cap U^h_{\xi_j} = \operatorname{Spec} k[\frac{\xi_0}{\xi_i}, \dots, \frac{\xi_n}{\xi_i}]_{\frac{\xi_j}{\xi_i}} = \operatorname{Spec} k[\frac{\xi_0}{\xi_j}, \dots, \frac{\xi_n}{\xi_j}]_{\frac{\xi_i}{\xi_j}}$, luego $\mathcal{O}_{U^h_{\xi_i},x} = \mathcal{O}_{U^h_{\xi_i} \cap U^h_{\xi_j},x} = \mathcal{O}_{U^h_{\xi_j},x}$.

Diremos que $x \in U^h_{\xi_i} \subset X = \operatorname{Proj} k[\xi_0, \dots, \xi_n]$ es un punto racional de X, si el ideal maximal de $\mathcal{O}_{X,x}$ es racional, es decir, si x es un punto racional de $U^h_{\xi_i}$. Si k es algebraicamente cerrado, los puntos cerrados de X coinciden con los puntos racionales.

24. Ejemplo: Sea $X = \operatorname{Proj} k[x_0, \dots, x_n]/(p_1(x_0, \dots, x_n), \dots, p_r(x_0, \dots, x_n))$ y denotemos por X_{rac} el conjunto de los puntos racionales de X. Probemos que

$$X_{rac} = \left\{ \alpha \in k^{n+1}, \text{ no nulo} : \begin{array}{c} p_1(\alpha) = 0 \\ \cdots \\ p_r(\alpha) = 0 \end{array} \right\} / \sim$$

donde $\alpha \sim \alpha'$ si existe $\lambda \in k$ tal que $\alpha' = \lambda \cdot \alpha$. Denotemos al término de la derecha de la igualdad por S. Sea $S_i := \{[\alpha] \in S : \alpha_i \neq 0\}$. La aplicación $S \to X_{rac}$, $[\alpha] \mapsto \alpha$, donde $\mathfrak{p}_\alpha = (\alpha_i \bar{x}_j - \alpha_j \bar{x}_i)_{i,j}$, restringida a cada S_i es la aplicación biyectiva

$$\begin{array}{rcl} S_i & \to & \left\{ (\alpha_0, \dots, \overset{i}{1}, \dots, \alpha_n) \in k^{n+1} : \begin{array}{c} p_1(\alpha_0, \dots, \overset{i}{1}, \dots, \alpha_n) = 0 \\ \cdots \\ p_r(\alpha_0, \dots, \overset{i}{1}, \dots, \alpha_n) = 0 \end{array} \right\} = (U^h_{\xi_i})_{rac} \\ [(\alpha_0, \dots, \alpha_n)] & \mapsto & (\frac{\alpha_0}{\alpha_i}, \dots, \overset{i}{1}, \dots, \frac{\alpha_n}{\alpha_i}) \end{array}$$

Además, $\alpha_i = 0$ si y solo si $[(\alpha_0, \dots, \alpha_n)]$ se aplica en un punto (racional) de $(\xi_i)^h_0$.

4.4. Dimensión de una variedad proyectiva

1. La dimensión del espacio topológico $\operatorname{Proj} R$ coincide con con el máximo de las longitudes de las cadenas de inclusiones de ideales primos homogéneos de R que no contengan al ideal irrelevante.

2. Sea $\bar{x}_1 \subset \cdots \subset \bar{x}_m$ una cadena de cerrados irreducibles de longitud máxima de $\operatorname{Proj} R$ y U un abierto que contiene a x_1. Entonces, $x_2 \in U$, porque si $x_2 \in U^c$, entonces $\bar{x}_2 \subseteq U^c$ y $x_1 \in U^c$. Luego, $x_i \in U$, para todo i. Entonces, $\bar{x}_1 \cap U \subset \cdots \subset \bar{x}_m \cap U$ es una cadena de cerrados irreducibles en U. Como la dimensión de un abierto es siempre menor o igual que la del espacio, entonces $\dim \operatorname{Proj} R = \dim U$. Por lo tanto,

$$\dim \operatorname{Proj} k[\xi_0, \dots, \xi_n] = \operatorname{máx}\{\dim U^h_{\xi_i}, \forall i\}.$$

3. Proposición: *Sea X una variedad proyectiva irreducible y $U \subset X$ un abierto no vacío. Entonces,* $\dim X = \dim U$.

Demostración. Para toda pareja de abiertos V y V' no vacíos, $V \cap V' \neq \emptyset$ porque X es irreducible. Si $V \subset V'$ entonces $\dim V \leq \dim V'$. Existe un abierto afín V tal que $\dim X = \dim V$. Por la proposición 3.5.3, $\dim(U \cap V) = \dim V = \dim X$ y $\dim(U \cap V) \leq \dim U \leq \dim X$. Por tanto, $\dim U = \dim X$. □

4. Proposición: *Sea $\mathfrak{m}_{or} = (\xi_0, \ldots, \xi_n) \subset k[\xi_0, \ldots, \xi_n]$ el ideal irrelevante. Entonces,*

$$\dim \operatorname{Proj} k[\xi_0, \ldots, \xi_n] = \dim k[\xi_0, \ldots, \xi_n]_{or} - 1 = (\dim \operatorname{Spec} k[\xi_0, \ldots, \xi_n]) - 1.$$

Demostración. Los ideales primos minimales de $k[\xi_0, \ldots, \xi_n]$ son homogéneos y están incluidos en $\mathfrak{m}_{or}$. Haciendo cociente en cada uno de estos ideales primos, podemos suponer que $k[\xi_0, \ldots, \xi_n]$ es un anillo íntegro. Sabemos que $\dim k[\xi_0, \ldots, \xi_n] = \dim k[\xi_0, \ldots, \xi_n]_{or}$. Todos los abiertos no vacíos de $\operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ (igualmente los de $\operatorname{Spec} k[\xi_0, \ldots, \xi_n]$) tienen la misma dimensión. Por el proposición 4.3.16, se concluye. □

5. Proposición: *Sea $f \in k[\xi_0, \ldots, \xi_n]$ una función homogénea de grado mayor que cero. Entonces,*

$$\dim(f)_0^h \geq \dim \operatorname{Proj} k[\xi_0, \ldots, \xi_n] - 1$$

Demostración. En efecto,

$$\dim(f)_0^h \overset{4.4.4}{=} \dim(f)_0 - 1 \overset{*}{\geq} \dim \operatorname{Spec} k[\xi_0, \ldots, \xi_n] - 2 \overset{4.4.4}{=} \dim \operatorname{Proj} k[\xi_0, \ldots, \xi_n] - 1,$$

donde $\overset{*}{\geq}$ es consecuencia del teorema del ideal principal de Krull, teniendo en cuenta que todas las componentes irreducibles de $\operatorname{Spec} k[\xi_1, \ldots, \xi_n]$ pasan por or y que f se anula en or (donde $\mathfrak{m}_{or} = (\xi_0, \ldots, \xi_n)$). □

6. Proposición: *Las variedades proyectivas son catenarias.*

Demostración. Dados dos cerrados irreducibles $\bar{x}_1 \subset \bar{x}_2$, sea U un abierto, que sea una variedad algebraica afín y que contenga a x_1. Toda cadena maximal de inclusiones de cerrados irreducibles de extremos $\bar{x}_1$ y $\bar{x}_2$ induce, cortando con U, una cadena maximal de inclusiones de cerrados dee U (de extremos $\bar{x}_1 \cap U$ y $\bar{x}_2 \cap U$). Se concluye por 3.5.10. □

4.5. Teoremas de Bézout y Max Noether

1. Sea X una variedad proyectiva de dimensión cero. Llamaremos número de puntos de X contando grados y multiplicidades, que denotaremos (X), a

$$(X) = \sum_{x \in X} \dim_k \mathcal{O}_{X,x}.$$

Dado un punto cerrado $x \in X$, llamaremos grado de x sobre k a $\dim_k \mathcal{O}_{X,x}/\mathfrak{m}_x$, donde $\mathfrak{m}_x$ es el ideal maximal de $\mathcal{O}_{X,x}$; y multiplicidad con la que aparece $x \in X$, que denotaremos $m_x(X)$, a $m_x(X) = \frac{\dim_k \mathcal{O}_{X,x}}{\mathrm{gr}_k\, x}$. Luego, $(X) = \sum_{x \in X} \mathrm{gr}_k\, x \cdot m_x(X)$.

Diremos que $C \subset \mathbb{P}^n$ es una curva proyectiva si es de dimensión 1. Diremos que $H \subset \mathbb{P}^n$ es una hipersuperficie si $H = (f_n)_0^h$ y diremos que n es el grado de la hipersuperficie. Sea C una curva proyectiva del espacio proyectivo $\mathbb{P}_k^n$ y H una hipersuperficie que no contiene ninguna componente irreducible de C. Entonces, $C \cap H = \{y_1, \ldots, y_m\}$ es un número finito de puntos cerrados. Diremos que el número de puntos de corte (contando multiplicidades y grados) de C con H es $(C \cap H)$. Este número es estable por cambios de cuerpo base.

2. Teorema de Bézout: *Sean C, C' dos curvas proyectivas planas sin componentes comunes 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 $C = \mathrm{Proj}\, k[x_0, x_1, x_2]/(p_r(x_0, x_1, x_2))$, $C' = \mathrm{Proj}\, k[x_0, x_1, x_2]/(p'_{r'}(x_0, x_1, x_2))$. 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

$$B' = [B_{\bar{x}_0}]_0 = \bigcup_i \frac{B_i}{\bar{x}_0^i}$$

Como $\emptyset = (\bar{x}_0)_0^h = \mathrm{Proj} B/(\bar{x}_0)$, entonces $\dim B/(\bar{x}_0) = 0$ y $\dim_k B/(\bar{x}_0) < \infty$. Existe m, tal que $(B/(\bar{x}_0))_n = 0$, para todo $n \geq m$. La sucesión $B \xrightarrow{\bar{x}_0 \cdot} B \to B/(x_0) \to 0$ es exacta, luego la

sucesión $B_n \xrightarrow{\bar{x}_0\cdot} B_{n+1} \to 0$ es exacta, para todo $n \geq m$. Por lo tanto, $\dim_k B_{n+1} \leq \dim_k B_n$, para todo $n \geq m$. Existe $m' > m$, tal que $\dim_k B_{n+1} = \dim_k B_n$, para todo $n \geq m'$. Por lo tanto, $B_n \xrightarrow{\bar{x}_0\cdot} B_{n+1}$ es un isomorfismo, para todo para todo $n \geq m'$. Como $\frac{B_i}{\bar{x}_0^i} \subseteq \frac{B_{i+1}}{\bar{x}_0^{i+1}}$, se concluye que $B' = \frac{B_n}{\bar{x}_0^n} \simeq B_n$, para $n > m'$.

Denotemos $A = k[x_0, x_1, x_2]$. La sucesión

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \oplus A & \longrightarrow & A & \longrightarrow & B \longrightarrow 0 \\ & & q & \longmapsto & (p'_{r'} \cdot q, -p_r \cdot q) & & q & \longmapsto & \bar{q} \\ & & & & & & (q, q') & \longmapsto & p_r \cdot q + p'_{r'} \cdot q' \end{array}$$

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

$$\dim_k B_n = \binom{n+2}{2} + \binom{n+2-r-r'}{2} - \binom{n+2-r}{2} - \binom{n+2-r'}{2} = r \cdot r'$$

para $n \geq r + r'$.

□

Dada una curva proyectiva plana $C = (p_n(x_0, x_1, x_2))_0^h$, un punto cerrado $x \in C$ y un abierto afín que lo contiene, digamos $U_{x_0}^h \subset \mathbb{P}^2$, tenemos que $C \cap U_{x_0}^h$ es la curva del plano afín de ecuación $p_n(x_0, x_1, x_2)/x_0^n = p_n(1, x_1/x_0, x_2/x_0) = 0$. Denotaremos $\mathfrak{p}_{C,x} = (p_n(1, x_1/x_0, x_2/x_0)) \subset k[x_1/x_0, x_2/x_0]_x$ y diremos que es el ideal de gérmenes en x de funciones del plano que se anulan en C, ideal que no depende del abierto afín considerado.

3. Teorema de Max Noether : *Sean $p_i \in k[x_0, x_1, x_2]$ polinomios homogéneos ($i = 1, 2, 3$) y consideremos las curvas proyectivas planas $C_i = (p_i)_0^h$. Supongamos que C_1, C_2 no tienen componentes comunes. Existe una ecuación*

$$p_3 = a \cdot p_1 + b \cdot p_2$$

con a, b polinomios homogéneos de grados $\operatorname{gr} a = \operatorname{gr} p_3 - \operatorname{gr} p_1, \operatorname{gr} b = \operatorname{gr} p_3 - \operatorname{gr} p_2$, si y solo si para todo $x \in C_1 \cap C_2$ se verifica que $\mathfrak{p}_{C_3,x} \subseteq \mathfrak{p}_{C_1,x} + \mathfrak{p}_{C_2,x}$.

Demostración. La necesidad es obvia, veamos la suficiencia.

La hipótesis equivale a que $(\frac{p_3}{x_i^{n_3}}) \subseteq (\frac{p_1}{x_i^{n_1}}) + (\frac{p_2}{x_i^{n_2}})$, para todo i, porque localmente es así. Luego la hipótesis se mantiene por cambio de cuerpo base. La tesis es cierta si lo es por cambio de cuerpo base. Podemos suponer que el cuerpo es algebraicamente cerrado.

Haciendo un cambio de coordenadas homogéneo, podemos suponer que x_0 no se anula en ningún punto de $C_1 \cap C_2$, es decir, $p_1(0,x_1,x_2)$ es primo con $p_2(0,x_1,x_2)$. Sabemos que

$$\frac{p_3}{x_0^{n_3}} = a \cdot \frac{p_1}{x_0^{n_1}} + b \cdot \frac{p_2}{x_0^{n_2}}$$

porque $(\frac{p_3}{x_0^{n_3}}) \subseteq (\frac{p_1}{x_0^{n_1}}) + (\frac{p_2}{x_0^{n_2}})$. Homogeneizando tenemos que

$$x_0^r \cdot p_3 = a' p_1 + b' p_2.$$

Sea r mínimo en las igualdades de esta forma. Si $r > 0$, entonces

$$0 = a'(0,x_1,x_2)p_1(0,x_1,x_2) + b'(0,x_1,x_2)p_2(0,x_1,x_2).$$

Por tanto, $a'(0,x_1,x_2) = h \cdot p_2(0,x_1,x_2)$ y $b'(0,x_1,x_2) = -h \cdot p_1(0,x_1,x_2)$. Observemos que $a'' := a' - h \cdot p_2$ y $b'' := b' + h \cdot p_1$ son divisibles por x_0; y que $x_0^r \cdot p_3 = a'' p_1 + b'' p_2$. Dividiendo esta igualdad por x_0 llegamos a contradicción, porque $r - 1 < r$. En conclusión,

$$p_3 = a \cdot p_1 + b \cdot p_2.$$

□

La siguiente proposición será de utilidad para poder aplicar el teorema de Max Noether en los problemas.

4. Proposición: *Sea* $C = \operatorname{Spec} k[x,y]/(p(x,y))$ *una curva plana y* $\alpha \in C$ *un punto racional no singular (ver el problema 22 del capítulo 3). Sean* $C_1 = \operatorname{Spec} k[x,y]/(q_1(x,y))$ *y* $C_2 = \operatorname{Spec} k[x,y]/(q_2(x,y))$ *dos curvas planas que pasan por* α*. Entonces,*

$$(p,q_2)_\alpha \subseteq (p,q_1)_\alpha \iff (C,C_2)_\alpha \geq (C,C_1)_\alpha.$$

Demostración. Por el problema 22 del capítulo 3, $\mathfrak{m}_\alpha \cdot (k[x,y]/(p(x,y)))_\alpha = (t)$ es principal. Luego, $\bar{q}_i = t^{m_i} \cdot inv$ y tendremos que $(\bar{q}_1) \subseteq (\bar{q}_2)$ o $(\bar{q}_2) \subseteq (\bar{q}_1)$. Es decir, $(p,q_1)_\alpha \subseteq (p,q_2)_\alpha$ o $(p,q_2)_\alpha \subseteq (p,q_1)_\alpha$. La primera inclusión se cumple cuando $(C,C_2)_\alpha \geq (C,C_1)_\alpha$, la segunda cuando $(C,C_1)_\alpha \geq (C,C_2)_\alpha$. □

4.6. Biografía de Bézout

BÉZOUT BIOGRAPHY

Étienne Bézout's father was Pierre Bézout who was a magistrate in the town of Nemours. One might have expected Étienne to follow the same career, for his grandfather had also been a magistrate in Nemours. Étienne's mother was Hélène-Jeanne Filz.

As we have already indicated the family tradition almost demanded that Étienne follow in his father and grandfather's footsteps. However the remarkable mathematics of Leonard Euler proved stronger than his parents wishes, for once Bézout had read Euler's works he wished to devote himself to mathematics. In 1756 he published a memoir Dynamique. In the following year he published Quantités différentielles and in 1758 Rectification des courbes. These latter two papers were investigations of integration.

In 1758 Bézout was appointed an adjoint in mechanics of the Académie des Sciences and, in the same year, as royal censor. He was appointed examiner of the Gardes de la Marine in 1763, the post being offered to him by the Duke of Choiseul. One important task that he was given in this role was to compose a textbook specially designed for teaching mathematics to the students.

Bézout is famed for the texbooks which came out of this assignment. The first was *Cours de mathématiques à l'usage des Gardes du Pavillon et de la Marine*, a four volume work which appeared in 1764-67.

In 1768 Camus, who was the examiner for the artillery, died. Bézout was appointed to succeed him becoming examiner of the Corps d'Artillerie. He began work on another mathematics textbook and as a result he produced *Cours complet de mathématiques à l'usage de la marine et de l'artillerie*, a six volume work which appeared between 1770 and 1782. This was a very successful textbook and for many years it was the book which students hoping to enter the École Polytechnique studied. Grabiner wrote:

"The experience of teaching non-mathematicians shaped the style of the works: Bézout treated geometry before algebra, observing that beginners were not yet familiar enough with mathematical reasoning to understand the force of algebraic demonstrations, although they did appreciate proofs in geometry. He eschewed the frightening terms «axiom» «theorem»,«scholium« and tried to avoid arguments that were too close and detailed".

As might be expected given this approach aimong at the readership for whom Bézout intended his texts, his books came in for a certain amount of criticism for lacking rigour. However, despite this they were books which could be understood by those who needed to use mathematics and as a result were very popular and widely used. Their

use spread beyond France for they were translated into English and used in North America. In particular Harvard University adopted them as calculus textbooks.

Returning to give more information about Bézout's career, we should note that he was promoted to associé in mechanics at the Académie des Sciences in 1768 and then further promoted to pensionnaire in 1770.

As we have indicated Bézout is famed for being a writer of textbooks but he is famed also for his work on algebra, in particular on equations. He was much occupied with his teaching duties after his 1763 appointments and he took these very seriously indeed. As a consequence he could devote relatively little time to research and he made a conscience decision to restrict the range of his work so that he could produce worthwhile results in a narrow order.

The way Bézout went about his research is interesting since still today it is a good approach for obtaining results. He attacked quite general problems, but since an attack was usually beyond what could be achieved with the mathematical knowledge then available, he attacked special cases of the general problems which he could solve. This approach often leads slowly to more and more understanding of the general case which may eventually become soluble. Bézout had a name for this approach to mathematics, namely the "method of simplifying assumptions".

His first paper on the theory of equations *Sur plusieurs classes d'équations de tous les degrés qui admettent une solution algébrique* examined how a single equation in a single unknown could be attacked by writing it as two equations in two unknowns. He wrote in this paper:

"It is known that a determinate equation can always be viewed as the result of two equations in two unknowns, when one of the unknowns is eliminated."

Of course on the face of it this does not help solve the equation but Bézout made the simplifying assumption that one of the two equations was of a particularly simple form. For example he considered the case when one of the two equations had only two terms, the term of degree n and a constant term. Already this paper had introduced the topic to which Bézout would make his most important contributions, namely methods of elimination to produce from a set of simultaneous equations, a single resultant equation in one of the unknowns.

He also did important work on the use of determinants in solving equations. This appears in a paper *Sur le degré des équations résultantes de l'évanouissement des inconnues* which he published in 1764. As a result of the ideas in this paper for solving systems of simultaneous equations, Sylvester, in 1853, called the determinant of the matrix of coefficients of the equations the Bézoutiant.

These and further papers published by Bézout in the theory of equations were gathered together in *Théorie générale des équations algébraiques* which was published in 1779. This work includes a result known as Bézout's theorem:

The degree of the final equation resulting from any number of complete equations in the same number of unknowns, and of any degrees, is equal to the product of the degrees of the equations.

By a complete equation Bézout meant one defined by a polynomial which contains terms of all possible products of the unknowns whose degree does not exceed that of the polynomial. One has to understand the problems that faced Bézout for he did not have our simple suffix notation to denote the unknowns by $x_1, x_2, x_3, \ldots$, nor could he even label his equations with a suffix notation. Despite this Bézout, who was prepared to enter long and difficult algebraic manipulations, proved his theorem with just a little hand waving over an inductive argument.

In this work Bézout also gave the first satisfactory proof of a result of Maclaurin on the intersection of two algebraic curves.

Grabiner told us that:

"[Bézout] married early and happily; although he was reserved and somewhat sombre in society, those who knew him spoke of his great kindness and warm heart. By [1763] Bézout had become a father ..."

After his death in 1783 a statue was erected in Nemours, the town of his birth, to commemorate his great achievements.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

4.7. Cuestionario

1. Prueba que $p(x_0,\ldots,x_n) \in k[x_0,\ldots,x_n]$ es un polinomio homogéneo de grado m si y solo si $p(tx_0,\ldots,tx_n) = t^m \cdot p(x_0,\ldots,x_n) \in k[t,x_0,\ldots,x_n]$.

2. ¿Cuál es el ideal homogéneo mínimo de $k[x,y]$ que contiene al ideal $(y+7x^2+xy)$?

3. Descompón el polinomio homogéneo $x^3+y^3 \in \mathbb{C}[x,y]$ en producto de irreducibles.

4. Sean $I_1, I_2 \subset R$ dos ideales homogéneos. Prueba que $(I_1 \cap I_2)_0^h = (I_1)_0^h \cup (I_2)_0^h$.

5. Calcula $(-x_0^2+x_1^2+x_2^2)_0^h \cap (-x_0^2+x_1^2+2x_2^2)_0^h \subset \mathbb{P}^2_{\mathbb{C}}$.

6. Sea R una álgebra graduada y supongamos que $\operatorname{Proj} R \neq \emptyset$. Prueba que $\operatorname{Proj} R$ es irreducible si y solo si $\operatorname{Spec} R$ es irreducible.

7. Prueba que toda variedad proyectiva es compacta. Prueba que si R es un anillo graduado noetheriano, entonces $\operatorname{Proj} R$ es un espacio topológico noetheriano.

8. Sea $f \in R_0[\xi_0,\dots,\xi_n]$ un elemento homogéneo de grado 1 (y $\mathrm{gr}(\xi_i)=1$, $\forall i$). Prueba que
$$[R_0[\xi_0,\dots,\xi_n]_f]_0 = R_0[\frac{\xi_0}{f},\dots,\frac{\xi_n}{f}].$$

9. Sea $f \in R_0[\xi_0,\dots,\xi_n]$ un elemento homogéneo de grado m. Prueba que $U^h_{\xi_i} \cap U^h_f = \mathrm{Spec}\, k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]_{\frac{f}{\xi_i^m}}$.

10. Da una variedad proyectiva cuyos puntos racionales sean la unión de un cono (proyectivo) con un plano (proyectivo) que pasa por el vértice del cono.

11. Da una variedad proyectiva con dos componentes irreducibles, una de dimensión 2 y otra de dimensión 0.

12. ¿Pueden ser un hiperplano y una recta de $\mathbb{P}^n$ disjuntos?¿Y un hiperplano y una recta de $\mathbb{A}^n$?

4.8. Problemas

1. Sea R un álgebra graduada y $f \in R_r$ con $r \neq 0$. Prueba

   a) Si f es invertible, entonces $\mathrm{Proj}\, R \to \mathrm{Spec} R_0$, $\mathfrak{p} \mapsto [\mathfrak{p}]_0$ es un homeorfismo.

   b) $U^h_f = \mathrm{Spec}[R_f]_0$.

   c) Si $(f)^h_0 = \mathrm{Proj}\, R$, entonces f es nilpotente.

2. Sea R un álgebra graduada. Prueba que $\mathrm{Proj}\, R = \emptyset$ si y solo si todo $f_n \in R_n$ es nilpotente, para todo $n \neq 0$.

3. a) Escribe las ecuaciones "afines" de la curva proyectiva plana
$$C = \mathrm{Proj}\, \mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2) \subset \mathbb{P}^2_{\mathbb{C}}$$
en cada uno de los abiertos afines $U^h_{\bar{x}_i}$ ("deshomogeneizar").

   b) Define una curva proyectiva plana que en uno de los abiertos afines sea la curva plana "afín" $y+x^2=0$. ¿Corta la recta $x=0$, a la curva $y+x^2=0$, en algún punto del "infinito"?

4. Prueba que el morfismo $\mathbb{C}[x] \hookrightarrow \mathbb{C}[x,y]/(p(x,y))$ es finito si y sólo si la curva $p(x,y)=0$ no tiene asíntotas verticales.

5. Calcula las asíntotas imaginarias de la circunferencia $x^2+y^2=1$.

6. Demuestra que la recta tangente a una curva de $\mathbb{P}^2$ de ecuaciones homogéneas $p(x_0,x_1,x_2)=0$ en un punto $\alpha=(\alpha_0,\alpha_1,\alpha_2)$ no singular es

$$\frac{\partial p}{\partial x_0}(\alpha)\cdot x_0+\frac{\partial p}{\partial x_1}(\alpha)\cdot x_1+\frac{\partial p}{\partial x_2}(\alpha)\cdot x_2=0$$

7. Sea

$$\begin{gathered} p_1(x_0,\dots,x_n)=0\\ \dots\\ p_r(x_0,\dots,x_n)=0 \end{gathered}$$

un sistema de ecuaciones homogéneas k-algebraicas y Σ el cierre algebraico de $k(y_1,\dots,y_n)$. En el conjunto X de todas las soluciones sobre Σ no nulas establezcamos la relación de equivalencia $\sim$: $(\lambda_0,\dots,\lambda_n)\sim(\mu_0,\dots,\mu_n)$ si existe $a\in\Sigma$ y $\tau\in \mathrm{Aut}_{k-alg}(\Sigma)$ tal que $(\lambda_0,\dots,\lambda_n)=a\cdot(\tau(\mu_0),\dots,\tau(\mu_n))$. Prueba que la aplicación

$$X/\sim \longrightarrow \mathrm{Proj}\, k[x_0,\dots,x_n]/(p_1,\dots,p_r)$$

que asigna a cada clase de equivalencia $[(\lambda_0,\dots,\lambda_n)]$ el ideal de funciones que se anulan en $t\cdot(\lambda_0,\dots,\lambda_n)$, para todo t, es biyectiva.

8. Consideremos la $k[x,y]$-álgebra graduada

$$A=\bigoplus_{n\in\mathbb{N}}(x,y)^n=k[x,y]\oplus(x,y)\oplus\cdots\oplus(x,y)^n\oplus\cdots.$$

Sea $\pi\colon \mathrm{Proj}\,A\to \mathrm{Spec}\,k[x,y]$ el morfismo natural. Prueba

   a) $\pi^{-1}(or)=\mathbb{P}^1$.
   b) $\pi^{-1}(\mathbb{A}^2-or)\xrightarrow{\pi}\mathbb{A}^2-or$ es un homeomorfismo.
   c) $\mathrm{Proj}\,A_{\tilde{x}}=\mathrm{Spec}\,k[x,y/x]$ donde $\tilde{x}\in A$ es el elemento $x\in(x,y)=A_1$, y por tanto $\mathrm{Proj}\,A=\mathrm{Spec}\,k[x,y/x]\cup\mathrm{Spec}\,k[y,x/y]$.

9. Sean X e Y dos subvariedades proyectivas irreducibles de $\mathbb{P}^n$, y supongamos que $\mathrm{codim}\,X+\mathrm{codim}\,Y\le n$[1]. Prueba que $X\cap Y\neq\emptyset$. Si Z es una componente irreducible de $X\cap Y$ prueba que

$$\mathrm{codim}\,Z\le\mathrm{codim}\,X+\mathrm{codim}\,Y.$$

[1] Se define $\mathrm{codim}\,X:=\dim\mathbb{P}^n-\dim X$

10. Prueba que el conjunto de rectas que pasan por un punto ("haz de rectas") del plano afín se corresponde con el conjunto de puntos racionales de una recta proyectiva.

11. Prueba que el conjunto de cónicas que pasan por cuatro puntos no alineados del plano afín se corresponden con los puntos racionales de una recta proyectiva.

12. Prueba que el conjunto de cónicas que pasan tres puntos no alineados del plano afín y es tangente en uno de ellos a una recta fijada que pasa por el punto se corresponden con los puntos racionales de una recta proyectiva.

13. Prueba que el conjunto de curvas de grado n de $\mathbb{P}^2$ se corresponden con los puntos racionales de un espacio proyectivo.

14. Prueba que el conjunto de curvas afines de grado menor o igual que n de $\mathbb{A}^2$ se corresponden con los puntos racionales de un abierto de un espacio proyectivo.

15. Prueba que en general las curvas planas afines de grado n son irreducibles.

16. Diremos que $\binom{n}{2}$ puntos del plano proyectivo están en posición general si no existe una curva de grado $n-2$ que pase por ellos. Prueba:

    a) Dados $\binom{n}{2}-1$ puntos cualesquiera existe una curva de grado $n-2$ que pasa por ellos.

    b) En general, dados $\binom{n}{2}-1$ puntos cualesquiera existe una única curva de grado $n-2$ que pasa por ellos.

    c) En general, $\binom{n}{2}$ puntos están en posición general.

17. Parametriza la curva $x^6 - x^2y^3 - y^5 = 0$. Calcula sus soluciones racionales.

18. Suponemos las curvas sobre un cuerpo algebraicamente cerrado. Prueba:

    a) Si una cónica tiene un punto singular, entonces no es irreducible.

    b) Si una cúbica plana tiene exactamente dos puntos singulares no es irreducible.

    c) Si una cuártica plana tiene cuatro puntos singulares entonces no es irreducible.

19. Prueba que los puntos $(0,0),(2,0),(0,2)$ 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).

20. Justifica 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.

21. Teorema de Pascal: Si un hexágono está inscrito en una cónica irreducible, entonces los lados opuestos se cortan en puntos alineados.

22. Teorema de Pappus: Sean R_1, R_2 dos rectas; $p_1, p_2, p_3 \in R_1$ y $q_1, q_2, q_3 \in R_2$ (ninguno de ellos se encuentran sobre $R_1 \cap R_2$). Sea R_{ij} la recta que une p_i y q_j. Prueba que los puntos $\{a,b,c\} = \{R_{ij} \cap R_{ji}\}_{i<j}\}$ están alineados.

23. Ley de grupo en las cúbicas: Sea C los puntos cerrados de una cúbica plana sobre un cuerpo algebraicamente cerrado no singular en todo punto. 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.

24. 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. Prueba que los tres restantes están alineados.

25. Demuestra que las tangentes a una cúbica irreducible plana en 3 puntos alineados cortan a la cúbica en otros 3 puntos alineados.

26. Demuestra que si un triángulo está inscrito en una cónica irreducible, entonces los puntos de corte de cada lado del triángulo con la tangente a la cónica en el vértice opuesto, están alineados.

27. Prueba que una recta que pase por dos puntos de inflexión[2] de una cúbica plana irreducible pasa por un tercer punto de inflexión.

28. Teorema de Chasles: Prueba que si una cúbica pasa por ocho de los nueve puntos distintos de corte de otras dos cúbicas, entonces también pasa por el noveno.

29. Teorema de Cayley-Bacharach: Sean C_d y $C_{d'}$ dos curvas proyectivas planas de grados d y d' que se cortan en dd' puntos distintos. Sea C_k una curva de grado k, con $d, d' \leq k \leq d+d'-3$ que pasa por $dd' - \binom{d+d'-k-1}{2}$ puntos de $C_d \cap C_{d'}$. Si el resto de los puntos están en posición general, es decir, no existe una curva plana de grado $d+d'-k-3$ que pase por los $\binom{d+d'-k-1}{2}$ puntos, entonces C_k pasa por todos los puntos de $C_d \cap C_{d'}$.

[2] Es decir, las rectas tangentes a la cúbica en los dos puntos cortan a la cúbica con multiplicidad 3

Capítulo 5

Desomposición primaria

5.1. Introducción

Dado un ideal I, puede parecernos que es siempre mejor considerar su radical $r(I)$ en vez de I. Pongamos un ejemplo sencillo en el que nos interese el ideal I: Consideremos el ideal $(x, y^2 - x) \subset \mathbb{C}[x, y]$ o el sistema de ecuaciones algebraicas

$$\begin{aligned} x &= 0 \\ y^2 - x &= 0 \end{aligned}$$

la variedad de soluciones de este sistema de ecuaciones 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 $r(I)$, con precisión $\dim_{\mathbb{C}} \mathbb{C}[x, y]/I = 2$, pero $\dim_{\mathbb{C}} \mathbb{C}[x, y]/r(I) = 1 \neq 2$. En conclusión, cuando estudiamos el sistema de ecuaciones definido por I, si consideramos solo el conjunto de soluciones del sistema de ecuaciones (o equivalentemente, consideramos solo $r(I)$) perdemos información que puede ser esencial, sobre todo en una teoría fina de intersección de variedades.

El ideal $(x, y^2 - x)$ es el ideal de polinomios $p(x, y)$ tales que $p(0, 0) = 0$ y $\frac{\partial p}{\partial y}(0, 0) = 0$, que hemos expresado de modo más impreciso como ideal de funciones que se anulan dos veces en el origen. En general, demostraremos que todo ideal $I \subset k[x_1, \ldots, x_n]$ es el ideal de polinomios que se anulan en ciertas variedades algebraicas 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

181

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 ciertas condiciones infinitesimales a lo largo de ellas.

Demos ahora un punto de vista aritmético. El teorema de Euclides afirma que todo número natural n es producto de potencias de números primos distintos de modo único salvo ordenación de los factores, $n = p_1^{n_1} \cdots p_r^{n_r}$. En términos de ideales, estamos diciendo que $(n) = (p_1)^{n_1} \cap \cdots \cap (p_r)^{n_r}$. Puede probarse que un anillo íntegro es localmente dominio de ideales principales si y solo si todo ideal es producto de modo único (salvo ordenación de los factores) de ideales primos.

Sea ahora A un anillo noetheriano. Dado un ideal primo $\mathfrak{p}_x \subset A$ denotemos $\mathfrak{p}_x^{(n)}$ el núcleo del morfismo natural $\pi\colon A \to A_x/\mathfrak{p}_x^n \cdot A_x$. Puede probarse que A es un anillo normal si y solo si A es íntegro y para todo $a \in A$ se cumple que

$$(a) = \mathfrak{p}_{x_1}^{(n_1)} \cap \cdots \cap \mathfrak{p}_{x_r}^{(n_r)}$$

para ciertos $n_1, \ldots, n_r > 0$ y $x_1, \ldots, x_r$ únicos, donde $\mathfrak{p}_{x_i} \nsubseteq \mathfrak{p}_{x_j}$ para todo $i \neq j$. Se dice que un ideal $\mathfrak{q}$ es $\mathfrak{p}_x$-primario si es la antimagen por π de un ideal (distinto del ideal (1)) de $A_x/\mathfrak{p}_x^n \cdot A_x$. El teorema central de este capítulo afirma que todo ideal de un anillo noetheriano es intersección de ideales primarios y veremos en qué sentido esta descomposición es única.

5.2. Ideales primarios

Queremos demostrar que todo ideal de un anillo noetheriano viene definido por condiciones infinitesimales en un número finito de puntos del espectro. Comencemos con los ideales primarios que serán los definidos por condiciones infinitesimales en un punto.

1. Definición: Sea A un anillo. Un ideal $\mathfrak{q} \subsetneq A$ es *primario* si todo divisor de cero de $A/\mathfrak{q}$ es nilpotente; es decir:

$$ab \in \mathfrak{q},\ a \notin \mathfrak{q} \ \Rightarrow\ b^n \in \mathfrak{q} \text{ para algún } n \geq 1.$$

2. Ejemplos:

1. Los ideales primos son primarios.
2. Si $p \in \mathbb{Z}$ es un número primo entonces (p^n) es un ideal primario de $\mathbb{Z}$. Igualmente si $p(x) \in k[x]$ es un polinomio irreducible entonces $(p(x)^n)$ es un ideal primario de $k[x]$

3. Proposición: *El radical de un ideal primario es un ideal primo.*

Demostración. En efecto, sea $\mathfrak{p}$ el radical de un ideal primario $\mathfrak{q}$. Si $ab \in \mathfrak{p}$ y $a \notin \mathfrak{p}$, entonces $(ab)^n \in \mathfrak{q}$ para algún $n \geq 1$ y $a^r \notin \mathfrak{q}$ para ningún r. Como $\mathfrak{q}$ es primario, alguna potencia de b^n ha de estar en $\mathfrak{q}$, luego $b \in \mathfrak{p}$. □

4. Definición: Sea $\mathfrak{q}$ un ideal primario y $\mathfrak{p} = r(\mathfrak{q})$ el radical de $\mathfrak{q}$. Diremos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario ó que $\mathfrak{p}$ es el *ideal primo asociado* a $\mathfrak{q}$.

En tal caso, si $A' \to A$ es un morfismo de anillos, es sencillo comprobar que $A' \cap \mathfrak{q}$ es un ideal $(A' \cap \mathfrak{p})$-primario de A'.

5. Proposición: *Sea $\mathfrak{m} \subset A$ un ideal maximal. Entonces, un ideal $I \subset A$ es $\mathfrak{m}$-primario si y solo si $r(I) = \mathfrak{m}$.*

En particular, todas las potencias $\mathfrak{m}^n$, con $n > 0$, son ideales $\mathfrak{m}$-primarios.

Demostración. Si I es un ideal de radical $\mathfrak{m}$, entonces $\mathfrak{m}$ es el único ideal primo que contiene a I. Por tanto, A/I tiene un único ideal primo, luego todo elemento de A/I es invertible o nilpotente; en particular, todo divisor de cero es nilpotente. □

Si el anillo A es noetheriano, cada ideal contiene una potencia de su radical, así que todo ideal $\mathfrak{m}$-primario es de la forma $\pi^{-1}(\bar{\mathfrak{q}})$ para algún ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}^r$ (donde $\pi\colon A \to A/\mathfrak{m}^r$ es el morfismo de paso al cociente). En el caso del anillo $A = \mathbb{C}[x_1,\ldots,x_n]$, si consideramos el ideal maximal $\mathfrak{m}_\alpha = (x_1 - \alpha_1,\ldots,x_n - \alpha_n)$ y escribimos $t_i = x_i - \alpha_i$, entonces $\mathfrak{m}_\alpha = (t_1,\ldots,t_n)$,

$$A/\mathfrak{m}_\alpha^r = \mathbb{C}[t_1,\ldots,t_n]/(t_1,\ldots,t_n)^r = \begin{bmatrix}\text{Polinomios de grado}\\ < r \text{ en } t_1,\ldots,t_n\end{bmatrix}$$

y la reducción módulo $\mathfrak{m}_\alpha^r$ de cualquier polinomio coincide con el clásico desarrollo de Taylor hasta el orden $r-1$ en el punto $(\alpha_1,\ldots,\alpha_n)$. Por tanto, el ideal $\mathfrak{m}_\alpha$-primario $\mathfrak{q}$ está formado por todas las funciones $f \in A$ cuyo desarrollo de Taylor $\bar{f} \in A/\mathfrak{m}_\alpha^r$ hasta el orden $r-1$ en el punto α, pertenece al subespacio vectorial $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}_\alpha^r$.

Una base del $\mathbb{C}$-espacio vectorial dual de $A/\mathfrak{m}_\alpha^r$, la constituyen las formas lineales

$$D_\beta = \left(\frac{\partial^{|\beta|}}{\partial^{\beta_1}x_1\cdots\partial^{\beta_n}x_n}\right)_{|\alpha}$$

con $\beta = (\beta_1,\ldots,\beta_n)$ y $|\beta| = \beta_1 + \cdots + \beta_n < r$, definidas por $D_\beta(\bar{f}) = \frac{\partial^{|\beta|} f}{\partial^{\beta_1}x_1\cdots\partial^{\beta_n}x_n}(\alpha_1,\ldots,\alpha_n)$. Por tanto, todo ideal de $A/\mathfrak{m}_\alpha^r$ está definido por un sistema de s-ecuaciones

$$\sum_{|\beta|<r} \lambda_{i,\beta} D_\beta(\bar{f}) = 0, \quad 1 \leq i \leq s.$$

Añadamos la ecuación redundante $f(\alpha_1,\dots,\alpha_n)=0$. Los ideales $\mathfrak{m}$-primarios son ideales generados por las funciones f que verifican un sistema de s-ecuaciones

$$\begin{array}{l}\sum\limits_{0<|\beta|<r}\lambda_{i,\beta}\frac{\partial^{|\beta|}f}{\partial^{\beta_1}x_1\cdots\partial^{\beta_n}x_n}(\alpha_1,\dots,\alpha_n)=0,\ \ 1\le i\le s\\ f(\alpha_1,\dots,\alpha_n)=0\end{array}$$

(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. Ejemplo: El ideal primario $(x^2,y)\subset\mathbb{C}[x,y]$ es igual al ideal

$$I=\{f\in\mathbb{C}[x,y]\colon f(0,0)=0,\frac{\partial f}{\partial x}(0,0)=0\}.$$

7. Proposición: *Sea S un sistema multiplicativo de un anillo A y sea $\mathfrak{q}$ un ideal $\mathfrak{p}_x$-primario.*

1. *Si $\mathfrak{p}_x$ corta a S, entonces $\mathfrak{q}A_S=A_S$.*
2. *Si $\mathfrak{p}_x$ no corta a S, entonces $\mathfrak{q}A_S$ es un ideal $\mathfrak{p}_xA_S$-primario y $\mathfrak{q}=A\cap(\mathfrak{q}A_S)$. En particular:*
$$\mathfrak{q}=A\cap(\mathfrak{q}A_x).$$

Por tanto, dos ideales $\mathfrak{p}_x$-primarios son iguales si son iguales al localizar en x.

Demostración. 1. Si $s\in S\cap\mathfrak{p}_x$, entonces $\mathfrak{q}$ contiene alguna s^n, que es invertible en A_S; luego $\mathfrak{q}A_S=A_S$.

2. Si $S\cap\mathfrak{p}_x=\emptyset$, entonces $\mathfrak{p}_xA_S$ es un ideal primo de A_S y es fácil comprobar que $\mathfrak{q}A_S$ es un ideal $\mathfrak{p}_xA_S$-primario. Por último, veamos que $\mathfrak{q}=A\cap(\mathfrak{q}A_S)$. Si $f\in A\cap(\mathfrak{q}A_S)$, entonces $sf\in\mathfrak{q}$ para algún $s\in S$. Ninguna potencia de s está en $\mathfrak{q}$, luego $f\in\mathfrak{q}$. Por tanto, $A\cap(\mathfrak{q}A_S)\subseteq\mathfrak{q}$. La inclusión contraria es evidente. □

8. Ejercicio: Prueba la igualdad

$$\{\text{Ideales primarios de } A_S\}=\{\text{Ideales primarios } \mathfrak{q}\subset A \text{ tales que } \mathfrak{q}\cap S=\emptyset\}.$$

9. Sea A un anillo noetheriano y $\mathfrak{p}_x \subset A$ un ideal primo. Un ideal $\mathfrak{q} \subset A$ es $\mathfrak{p}_x$-primario si y solo $\mathfrak{q}\cdot A_x$ es un ideal $\mathfrak{p}_x\cdot A_x$-primario, que equivale a que exista un número natural r, tal que $\mathfrak{p}_x^r A_x \subseteq \mathfrak{q}\cdot A_x \subsetneq A_x$. En conclusión, $\mathfrak{q}$ es un ideal $\mathfrak{p}_x$-primario si y solo si existe un número natural r y un ideal $\bar{\mathfrak{q}} \subsetneq A_x/\mathfrak{p}_x^r A_x$ 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. Por tanto, "los ideales $\mathfrak{p}_x$-primarios son los ideales determinados por condiciones infinitesimales a lo largo de x".

10. Ejemplos: Si un ideal primo $\mathfrak{p}$ no es maximal, pueden existir ideales de radical $\mathfrak{p}$ que no son primarios. Fijemos en un plano afín un punto racional p y una recta r que pase por él. Sea $\mathfrak{m}_p$ el ideal de funciones del plano que se anulen en p y $\mathfrak{p}_r$ el ideal de funciones del plano que se anulen en r. Consideremos ahora el ideal $I = \mathfrak{m}_p^2 \cap \mathfrak{p}_r$, que son los polinomios que se anulan en la recta r y sus derivadas parciales se anulan en el punto fijado p. El radical de I es

$$r(I) = r(\mathfrak{m}_p^2) \cap r(\mathfrak{p}_r) = \mathfrak{m}_p \cap \mathfrak{p}_r = \mathfrak{p}_r$$

pero el ideal I no es primario: si fuese primario sería $\mathfrak{p}_r$-primario. Al localizarlo en r, coincide con la localización de $\mathfrak{p}_r$ en r, por tanto I coincidiría con $\mathfrak{p}_r$, lo cual es falso.

Puede incluso darse el caso de que una potencia de un ideal primo no sea un ideal primario. Por ejemplo, sea $A = k[x,y,z]/(x^2+y^2-z^2)$ el anillo de las funciones algebraicas de un cono de $\mathbb{A}^3$ y sea $\mathfrak{p}_{gt} = (x, y-z)$ el ideal primo de A definido por una generatriz. El ideal $\mathfrak{p}_{gt}^2$ no viene definido por condiciones infinitesimales en el punto genérico de tal generatriz; es decir, $\mathfrak{p}_{gt}^2$ no coincide con $A \cap \mathfrak{p}_{gt}^2 A_{gt}$ sino que involucra además condiciones en el vértice del cono, pues las funciones de $\mathfrak{p}_{gt}^2$ deben cumplir además la condición de estar en $\mathfrak{m}^2$, donde $\mathfrak{m} = (x,y,z)$ denota el ideal maximal del vértice del cono. En efecto, $y - z \in A \cap \mathfrak{p}_{gt}^2 A_{gt}$ (porque $(y-z)\cdot(y+z) \in \mathfrak{p}_{gt}^2 A_{gt}$) pero $y - z \notin \mathfrak{p}_{gt}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal $\mathfrak{p}_{gt}^2$ no es primario.

5.3. Descomposición primaria de ideales

1. 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.

2. Lema fundamental: *Sea A un anillo noetheriano. Todo ideal irreducible $\mathfrak{q} \neq A$ es primario.*

Demostración. Sea $\mathfrak{q}$ irreducible y sea $b \in A/\mathfrak{q}$ un divisor de cero. Sea $b\colon A/\mathfrak{q} \to A/\mathfrak{q}$ la homotecia de razón b. Se tiene que

$$0 \neq \operatorname{Ker} b \subseteq \operatorname{Ker} b^2 \subseteq \cdots \subseteq \operatorname{Ker} b^n \subseteq \cdots$$

Como $A/\mathfrak{q}$ es un anillo noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún n. Por lo tanto, $(\operatorname{Ker} b) \cap (\operatorname{Im} b^n) = 0$. Como $\mathfrak{q}$ es irreducible, debe ser $\operatorname{Ker} b = 0$ ó $\operatorname{Im} b^n = 0$. Por hipótesis $\operatorname{Ker} b \neq 0$, luego $\operatorname{Im} b^n = 0$ y por tanto b es nilpotente. En conclusión, los divisores de cero de $A/\mathfrak{q}$ son nilpotentes y $\mathfrak{q}$ es primario. □

3. Existencia de descomposiciones primarias: *Sea A un anillo noetheriano. Todo ideal $I \subsetneq A$ es intersección finita de ideales irreducibles de A. Por tanto, todo ideal $I \subsetneq A$ es intersección finita de ideales primarios de A.*

Demostración. Basta ver que si I no es irreducible entonces $I = I_1 \cap I'$ con I_1 irreducible e $I \subsetneq I'$ (pues con I' se repite el argumento y así sucesivamente y se concluye por noetherianidad). Si I no es irreducible, entonces es intersección de ideales estrictamente mayores: $I = I_1 \cap J_1$. Si I_1 es irreducible hemos terminado; si no, $I_1 = I_{11} \cap I_{12}$, luego $I = I_{11} \cap I_{12} \cap J_1$. Si la inclusión $I \subset I_{12} \cap J_1$ es estricta, tomamos $I_2 = I_{11}, J_2 = I_{12} \cap J_1$; si no, tomamos $I_2 = I_{12}$, $J_2 = J_1$. En ambos casos obtenemos de nuevo que $I = I_2 \cap J_2$, con $I \subsetneq J_2$, además $I_1 \subsetneq I_2$. Así sucesivamente, el proceso es finito por noetherianidad, luego para cierto n, $I = I_n \cap J_n$ con I_n irreducible e $I \subsetneq J_n$ por construcción. □

4. 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) y $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ cuando $i \neq j$.

5. 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.*

6. 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 primaria $\mathfrak{q}_i$ y*

$$\mathfrak{q}_i = A \cap (IA_x)$$

Por tanto, las componentes primarias $\mathfrak{q}_i$ 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 5.2.7, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_x) = A \cap (IA_x)$. □

7. Definición : Si $I = \cap_i \mathfrak{q}_i$ es una descomposición primaria reducida, las componentes primarias $\mathfrak{q}_i$ cuyos radicales son mínimos se denominan componentes primarias *no sumergidas*. Una componente primaria $\mathfrak{q}_j$ se dice que está *sumergida* cuando sus ceros están contenidos estrictamente en los ceros de alguna otra componente: $(\mathfrak{q}_j)_0 \subset (\mathfrak{q}_i)_0$.

Los ceros de las componentes primarias no sumergidas corresponden biunívocamente con las componentes irreducibles de $(I)_0$, el radical de una componente primaria se corresponde el punto genérico de una componente irreducible de $(I)_0$.

8. 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 de los ideales primarios.*

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

$$(I : a) = \{b \in A : a \cdot b \in I\}.$$

9. 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. □

10. Definición: Diremos que un ideal $\mathfrak{p}$ es un *ideal primo asociado* a un ideal I, si existe una descomposición primaria reducida $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ tal que $\mathfrak{p} = r(\mathfrak{q}_i)$, para algún i.

11. Unicidad de los primos asociados a un ideal: *Los radicales de los ideales primarios de las descomposiciones primarias reducidas de I no dependen de la descomposición primaria reducida considerada.*

Demostración. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida. y sea $\mathfrak{p}_i = r(\mathfrak{q}_i)$, para todo i.

Sea $a \in \bigcap_{i\neq j}^{n} \mathfrak{q}_i$ y $a \notin \mathfrak{q}_j$. Entonces, $(I : a) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : a) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a) = (\mathfrak{q}_j : a)$ es un ideal $\mathfrak{p}_j$-primario por la proposición anterior. Por tanto, $\mathfrak{p}_j = r((I : a))$.

Dado $b \in A$, $(I : b) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : b) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : b)$. Por la proposición anterior, $r(I : b)$ es intersección de algunos de los primos $\mathfrak{p}_i$, luego si $r((I : b)) = \mathfrak{p}$ es un ideal primo entonces $\mathfrak{p} = \mathfrak{p}_i$, para algún i (ya que el cerrado irreducible $(\mathfrak{p})_0$ es igual a la unión de unos cuantos cerrados irreducibles $(\mathfrak{p}_i)_0$).

□

12. Proposición: *Sea A un anillo noetheriano y $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos asociados al ideal* (0)*. Entonces,*

$$\{\textit{Divisores de cero de } A\} = \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Demostración. Sea $(0) = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una descomposición primaria reducida. Si a es divisor de cero, entonces existe b no nulo tal que $ab = 0$, luego $b \notin \mathfrak{q}_i$ para algún i y $a \in r(\mathfrak{q}_i) = \mathfrak{p}_i$.

Sea $a \in \mathfrak{p}_i$. Sea $n \in \mathbb{N}$ tal que $a^n \in \mathfrak{q}_i$ y $b \in \cap_{j\neq i} \mathfrak{q}_j$ no nulo. Entonces, $a^n b \in \bigcap_{i=1}^{n} \mathfrak{q}_i = 0$ y a es divisor de cero. □

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.

13. Proposición: *Sea A un anillo noetheriano. Un ideal primo $\mathfrak{p} \subset A$ es un ideal primo asociado al ideal $I \subset A$ si y solo si existe $a \in A$ tal que $(I : a) = \mathfrak{p}$.*

Demostración. Sea $= \mathfrak{q}_1 \cap \cdots\cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida y $\mathfrak{p}_i = r(\mathfrak{q}_i)$, para todo i. Observemos que $(I : a) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : a) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a)$. 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 $(\mathfrak{p}_i)_0$).

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 **??** $(I : a) = (\mathfrak{q}_1 : a)$ 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 $(I : ab) = (\mathfrak{q}_1 : ab) = \mathfrak{p}$. □

14. 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.

□

5.4. Descomposición primaria de submódulos

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.

1. 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).

2. Definición: Un submódulo $M' \subseteq M$ diremos que es irreducible si no es intersección de dos submódulos estrictamente mayores de M.

3. Proposición: *Los submódulos irreducibles de un módulo noetheriano son primarios.*

4. Teorema: *Todo submódulo de un módulo noetheriano es intersección de un número finito de submódulos primarios.*

5. 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'.

6. 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 $(M' : m) = \{a \in A : am \in M'\}$.

7. 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*

$$(M' : m) = \begin{cases} A & \text{si } m \in M'. \\ \mathfrak{q}' & \text{si } m \notin M', \text{ siendo } \mathfrak{q}' \text{ un ideal } \mathfrak{p}\text{-primario, que contiene a } \mathfrak{q}. \end{cases}$$

8. Proposición: *Sea M' un submódulo de un módulo noetheriano M y consideremos una descomposición primaria reducida $M' = M_1 \cap \cdots \cap M_n$ de M'. Un ideal primo $\mathfrak{p}$ es un ideal primo asociado a alguno de los M_i si y solo si existe $m \in M$ tal que $(M' : m) = \mathfrak{p}$.*

9. Teorema de unicidad de las componentes no sumergidas: *Sea M' un submódulo de un módulo noetheriano M y $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida. Sea $\mathfrak{p}_x$ el ideal primo asociado a M_i y supongamos que es minimal entre los ideales primos asociados a los M_j. Entonces,*

$$M_i = M \cap M'_x$$

10. Ejercicio: Prueba que los ideales primos minimales asociados a un submódulo M' de un módulo noetheriano M, coinciden con los ideales primos minimales asociados al ideal anulador de M/M'.

5.5. Una descomposición primaria canónica

1. Proposición: *Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida y $\mathfrak{p}_x$ un ideal primo. Denotemos $J := \cap_{\mathfrak{q}_i \subseteq \mathfrak{p}_x} \mathfrak{q}_i$. Entonces*

$$J = A \cap I_x.$$

Por tanto, el ideal J no depende de la descomposición primaria de I escogida.

Demostración. Se deduce de la Proposición 5.2.7 □

2. Corolario: *Sean $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$ dos descomposiciones primarias reducidas de primos asociados $r(\mathfrak{q}'_i) = r(\mathfrak{q}_i) = \mathfrak{p}_{x_i}$. Se cumple que*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j \cap \mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$$

para todo j. En consecuencia, si $\mathfrak{q}''_i$ son ideales $\mathfrak{p}_{x_i}$-primarios, y cada uno de ellos aparece en alguna descomposición primaria reducida de I, entonces

$$I = \mathfrak{q}''_1 \cap \cdots \cap \mathfrak{q}''_n.$$

Demostración. Reordenando, podemos suponer que $\mathfrak{q}_i, \mathfrak{q}'_i \subseteq \mathfrak{p}_{x_j} \Leftrightarrow i \leq j$. Por la proposición anterior, $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_j$. Denotemos $J_i = A \cap I_{x_i}$. Por la proposición anterior, $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} = \cap_{i<j} J_i = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1}$. Por tanto,

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1} \cap \mathfrak{q}'_j \overset{5.5.1}{=} \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

Cortando con $\mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$ concluimos. □

Procedamos a ver que entre las descomposiciones primarias de I hay una canónica.

3. Proposición: *Sea I un ideal de un anillo noetheriano, de ideales primos asociados $x_1, \ldots, x_r$. Sea n_i el número natural más pequeño posible tal que $\mathfrak{p}_{x_i}^{n_i}$ está incluido en algún ideal $\mathfrak{p}_{x_i}$-primario que aparezca en alguna descomposición primaria reducida de I. Denotemos $\alpha_i := A \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i}$ (α_i es el ideal $\mathfrak{p}_{x_i}$-primario más pequeño que contiene a $\mathfrak{p}_{x_i}^{n_i}$ y a I). Entonces*

$$I = \alpha_1 \cap \cdots \cap \alpha_r$$

es una descomposición primaria reducida de I (y diremos que es la descomposición primaria canónica de I).

Demostración. Observemos que $\operatorname{rad}((I + \mathfrak{p}_{x_i}^{n_i})_{x_i}) = \mathfrak{p}_{x_i} \cdot A_{x_i}$, luego es un ideal $\mathfrak{p}_{x_i} \cdot A_{x_i}$-primario de A_{x_i} y α_i es un ideal $\mathfrak{p}_{x_i}$-primario. Consideremos una descomposición primaria reducida $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, tal que $\mathfrak{p}_{x_i}^{n_i} \subset \mathfrak{q}_i$, para todo i. Entonces, $I + \mathfrak{p}_{x_i}^{n_i} \subseteq \mathfrak{q}_i$ y por tanto $\alpha_i = A \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i} \subseteq A \cap \mathfrak{q}_{i,x_i} = \mathfrak{q}_i$ y

$$I \subseteq \cap_{i=1}^r \alpha_i \subseteq \cap_{i=1}^r \mathfrak{q}_i = I$$

luego todas las desigualdades son igualdades.

□

Tenemos pues unos números $n_1,\dots,n_r$ canónicamente asociados al ideal I. Determinemos de un modo algo más algorítmico los números n_i. Sea $I_i = \cap_{\alpha_j \subset \mathfrak{p}_i} \alpha_j$. Entonces, n_i es el mínimo número tal que $I_{i,x_i} \cap (I + \mathfrak{p}_{x_i}^{n_i}))_{x_i} = I_{x_i}$. Como

$$I_{i,x_i} \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i} = (I_i \cap (I + \mathfrak{p}_{x_i}^{n_i})_{x_i} = (I + (I_i \cap \mathfrak{p}_{x_i}^{n_i}))_{x_i},$$

n_i es el mínimo numero tal que $(I_i \cap \mathfrak{p}_{x_i}^{n_i})_{x_i} \subseteq I_{x_i}$, es decir, $(I : I_i \cap \mathfrak{p}_{x_i}^{n_i})_{x_i} = A_{x_i}$. Por tanto, n_i es el mínimo número tal que $(I : I_i \cap \mathfrak{p}_{x_i}^{n_i}) \not\subseteq \mathfrak{p}_{x_i}$.

Del mismo modo obtenemos descomposiciones primarias canónicas para los submódulos de un módulo noetheriano. Las demostraciones de las siguientes proposiciones se pueden copiar de sus equivalentes en el caso de ideales.

4. 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.

5. 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 $\{L_i\}_{1 \le i \le n}$ son submódulos $\mathfrak{p}_{x_i}$-primarios y cada uno de ellos aparece en alguna descomposición primaria de M', entonces

$$M' = L_1 \cap \cdots \cap L_n.$$

6. 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'.

5.6. Biografía de Emmy Noether

NOETHER BIOGRAPHY

Emmy Noether's father, Max Noether, was a distinguished mathematician and a professor at Erlangen but he came from a family of wholesale hardware dealers. Her mother was Ida Amalia Kaufmann (1852-1915), from a wealthy Cologne family. Both Emmy's parents were of Jewish origin and the reader may be surprised at this since Noether is not a Jewish name. We should explain, therefore, how this came about and, at the same time, give some information on Emmy Noether's ancestors. Max Noether's paternal grandfather was Elias Samuel, the founder of a business in Bruchsal. Elias had nine children, one being a son Hertz Samuel. In 1809 the State of Baden made the Tolerance Edict which required Jews to adopt Germanic names. Elias Samuel chose the surname Nöther, becoming Elias Nöther, but also changed the given names of his children, giving Hertz the name Hermann. When he was eighteen years old, Hermann Nöther left his home town of Bruchsal and studied theology at the University of Mannheim. Then in 1837, together with his brother Joseph, he set up a wholesale business in iron hardware. Hermann Nöther and his wife Amalia had five children, the third of which was Max. The two children older than Max were Sarah (born 6 November 1839) and Emil. It is worth noting at this point that the Nöther iron-wholesaling business remained a family firm for exactly one hundred years, until the Nazis removed Jewish families from their own businesses in 1937. One other comment is necessary at this point. Although the family name was chosen to be Nöther by Max's grandfather, Max and his family always used the form Noether (except on Max's wedding certificate where the form Nöther appears).

Emmy was the eldest of her parents' four children, the three younger children being boys. Alfred Noether (1883-1918) studied chemistry and was awarded a doctorate from Erlangen in 1909. However, his career was short since he died nine years later. Fritz Noether (1884-1941) became an applied mathematician. However, as a Jew he was unable to work and left Germany in 1937. He was appointed as a professor at the University of Tomsk in the Soviet Union but accused of anti-Soviet acts he was sentenced to death and shot. He was found not guilty by the Supreme Court of the Soviet Union in 1988. Gustav Robert Noether (1889-1928) had bad health all his life. He was mentally handicapped, spent most of his life in an institution and died young. The first school that Emmy attended was on Fahrstrasse. Auguste Dick wrote:

Emmy did not appear exceptional as a child. Playing among her peers in the schoolyard on Fahrstrasse she probably was not especially noticeable - a near-sighted, plain-looking little girl, though not without charm. Her teachers and classmates knew

Emmy as a clever, friendly, and likeable child. She had a slight lisp and was one of the few who attended classes in the Jewish religion.

After elementary school, Emmy Noether attended the Städtische Höhere Töchter Schule on Friedrichstrasse in Erlangen from 1889 until 1897. She had been born in the family home at Hauptstrasse 23 and lived there until, in the middle of her time at high school, in 1892, the family moved to a larger apartment at Nürnberger Strasse 32. At the high school she studied German, English, French, arithmetic and was given piano lessons. She loved dancing and looked forward to parties with children of her father's university colleagues. At this stage her aim was to become a language teacher and after further study of English and French she took the examinations of the State of Bavaria and, in 1900, became a certificated teacher of English and French in Bavarian girls schools. She was awarded the grade of "very good" in the examinations, the weakest part being her classroom teaching.

However Noether never became a language teacher. Instead she decided to take the difficult route for a woman of that time and study mathematics at university. Women were allowed to study at German universities unofficially and each professor had to give permission for his course. Noether obtained permission to sit in on courses at the University of Erlangen during 1900 to 1902. She was one of only two female students sitting in on courses at Erlangen and, in addition to mathematics courses, she continued her interest in languages being taught by the professor of Roman Studies and by an historian. At the same time she was preparing to take the examinations which allowed a student to enter any university. Having taken and passed this matriculation examination in Nürnberg on 14 July 1903, she went to the University of Göttingen. During 1903-04 she attended lectures by Karl Schwarzschild, Otto Blumenthal, David Hilbert, Felix Klein and Hermann Minkowski. Again she was not allowed to be a properly matriculated student but was only allowed to sit in on lectures. After one semester at Göttingen she returned to Erlangen.

At this point the rules were changed and women students were allowed to matriculate on an equal basis to the men. On 24 October 1904 Noether matriculated at Erlangen where she now studied only mathematics. In 1907 she was granted a doctorate after working under Paul Gordan. The oral examination took place on Friday 13 December and she was awarded the degree 'summa cum laude'. Hilbert's basis theorem of 1888 had given an existence result for finiteness of invariants in n variables. Gordan, however, took a constructive approach and looked at constructive methods to arrive at the same results. Noether's doctoral thesis followed this constructive approach of Gordan and listed systems of 331 covariant forms. Colin McLarty wrote that:

... her dissertation of 1908 with Gordan pursued a huge calculation that had stumped Gordan forty years before and which Noether could not complete either. So far as I know no one has ever completed it or even checked it as far as she went. It was

old-fashioned at the time, a witness to the pleasant isolation of Erlangen, and made no use of Gordan's own work building on Hilbert's ideas.

Having completed her doctorate the normal progression to an academic post would have been the habilitation. However this route was not open to women so Noether remained at Erlangen, helping her father who, particularly because of his own disabilities, was grateful for his daughter's help. Noether also worked on her own research, in particular she was influenced by Ernst Fischer who had succeeded Gordan to the chair of mathematics when he retired in 1911. Noether wrote about Fischer's influence:

Above all I am indebted to Mr E Fischer from whom I received the decisive impulse to study abstract algebra from an arithmetical viewpoint, and this remained the governing idea for all my later work.

Fischer's influence took Noether towards Hilbert's abstract approach to the subject and away from the constructive approach of Gordan. Now this was very important to her development as a mathematician for Gordan, despite his remarkable achievements, had his limitations. Noether's father, Max Noether, said of Gordan:

Gordan was never able to do justice to the development of fundamental concepts; even in his lectures he completely avoided all basic definitions of a conceptual nature, even that of the limit.

Noether's reputation grew quickly as her publications appeared. In 1908 she was elected to the Circolo Matematico di Palermo, then in 1909 she was invited to become a member of the Deutsche Mathematiker-Vereinigung and in the same year she was invited to address the annual meeting of the Society in Salzburg. She gave the lecture Zur Invariantentheorie der Formen von n Variabeln (On the theory of invariants for the forms of n variables). In 1913 she lectured in Vienna, again to a meeting of the Deutsche Mathematiker-Vereinigung. Her lecture on this occasion was Über rationale Funktionenkörper (On fields of rational functions). While in Vienna she visited Franz Mertens and discussed mathematics with him. One of Merten's grandsons remembered Noether's visit:

... although a woman, [she] seemed to me like a Catholic chaplain from a rural parish - dressed in a black, almost ankle-length and rather nondescript, coat, a man's hat on her short hair ... and with a shoulder bag carried crosswise like those of the railway conductors of the imperial period, she was rather an odd figure.

During these years in Erlangen she advised two doctoral students who were both officially supervised by her father. These were Hans Falckenberg (doctorate 1911) and Fritz Seidelmann (doctorate 1916).

In 1915 Hilbert and Klein invited Noether to return to Göttingen. The reason for this was that Hilbert was working on physics, in particular on ideas on the theory of relativity close to those of Albert Einstein. He decided that he needed the help

of an expert on invariant theory and, after discussions with Klein, they issued the invitation. Van der Waerden wrote:

She came and at once solved two important problems. First: How can one obtain all differential covariants of any vector or tensor field in a Riemannian space? ... The second problem Emmy investigated was a problem from special relativity. She proved: To every infinitesimal transformation of the Lorentz group there corresponds a Conservation Theorem.

This result in theoretical physics is sometimes referred to as Noether's Theorem, and proves a relationship between symmetries in physics and conservation principles. This basic result in the theory of relativity was praised by Einstein in a letter to Hilbert when he referred to Noether's penetrating mathematical thinking. Of course, she arrived in Göttingen during World War I. This was a time of extreme difficulty and she lived in poverty during these years and politically she became a radical socialist. However, they were extraordinarily rich years for her mathematically. Hermann Weyl, in wrote about Noether's political views:

During the wild times after the Revolution of 1918, she did not keep aloof from the political excitement, she sided more or less with the Social Democrats; without being actually in party life she participated intensely in the discussion of the political and social problems of the day. ... In later years Emmy Noether took no part in matters political. She always remained, however, a convinced pacifist, a stand which she held very important and serious.

Hilbert and Klein persuaded her to remain at Göttingen while they fought a battle to have her officially on the Faculty. In a long battle with the university authorities to allow Noether to obtain her habilitation there were many setbacks and it was not until 1919 that permission was granted and she was given the position of Privatdozent. During this time Hilbert had allowed Noether to lecture by advertising her courses under his own name. For example a course given in the winter semester of 1916-17 appears in the catalogue as:

Mathematical Physics Seminar: Professor Hilbert, with the assistance of Dr E Noether, Mondays from 4-6, no tuition.

At Göttingen, after 1919, Noether moved away from invariant theory to work on ideal theory, producing an abstract theory which helped develop ring theory into a major mathematical topic. Idealtheorie in Ringbereichen (1921) was of fundamental importance in the development of modern algebra. In this paper she gave the decomposition of ideals into intersections of primary ideals in any commutative ring with ascending chain condition. Emanuel Lasker (who became the world chess champion) had already proved this result for a polynomial ring over a field. Noether published Abstrakter Aufbau der Idealtheorie in algebraischen Zahlkorpern in 1924. In this paper she gave five conditions on a ring which allowed her to deduce that in such com-

mutative rings every ideal is the unique product of prime ideals.

In the same year of 1924 B.L. van der Waerden came to Göttingen and spent a year studying with Noether. After returning to Amsterdam van der Waerden wrote his book Moderne Algebra in two volumes. The major part of the second volume consists of Noether's work. From 1927 onwards Noether collaborated with Helmut Hasse and Richard Brauer in work on non-commutative algebras. They wrote a beautiful paper joint paper Beweis eines Hauptsatzes in der Theorie der Algebren which was published in 1932. In addition to teaching and research, Noether helped edit Mathematische Annalen. Much of her work appears in papers written by colleagues and students, rather than under her own name.

Further recognition of her outstanding mathematical contributions came with invitations to address the International Congress of Mathematicians at Bologna in September 1928 and again at Zurich in September 1932. Her address to the 1932 Congress was entitled Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie. In 1932 she also received, jointly with Emil Artin, the Alfred Ackermann-Teubner Memorial Prize for the Advancement of Mathematical Knowledge. In April 1933 her mathematical achievements counted for nothing when the Nazis caused her dismissal from the University of Göttingen because she was Jewish. She received no pension or any other form of compensation but, nevertheless, she considered herself more fortunate than others. She wrote to Helmut Hasse on 10 May 1933:

Many thanks for your dear compassionate letter! I must say, though, that this thing is much less terrible for me than it is for many others. At least I have a small inheritance (I was never entitled to a pension anyway) which allows me to sit back for a while and see.

Weyl spoke about Noether's reaction to the dire events that were taking place around her in the address he gave at her funeral:

You did not believe in evil, indeed it never occurred to you that it could play a role in the affairs of man. This was never brought home to me more clearly than in the last summer we spent together in Göttingen, the stormy summer of 1933. In the midst of the terrible struggle, destruction and upheaval that was going on around us in all factions, in a sea of hate and violence, of fear and desperation and dejection - you went your own way, pondering the challenges of mathematics with the same industriousness as before. When you were not allowed to use the institute's lecture halls you gathered your students in your own home. Even those in their brown shirts were welcome; never for a second did you doubt their integrity. Without regard for your own fate, openhearted and without fear, always conciliatory, you went your own way. Many of us believed that an enmity had been unleashed in which there could be no pardon; but you remained untouched by it all.

She accepted a one-year visiting professorship at Bryn Mawr College in the USA and in October 1933 sailed to the United States on the ship Bremen to take up the appointment. She had hoped to delay accepting the invitation since she would have liked to have gone to Oxford in England but it soon became clear that she had to leave quickly. At Bryn Mawr she was made very welcome by Anna Johnson Pell Wheeler who was head of mathematics. Noether ran a seminar during the winter semester of 1933-34 for three students and one member of staff. They worked through the first volume of van der Waerden's Moderne Algebra. In February 1934 she began giving weekly lectures at the Institute for Advanced Study, Princeton. In a letter to Hasse, dated 6 March 1934, she wrote:

I have started with representation modules, groups with operators ...; Princeton will receive its first algebraic treatment this winter, and a thorough one at that. My audience consists mostly of research fellows, besides Albert and Vandiver, but I'm beginning to realise that I must be careful; after all, they are essentially used to explicit computation and I have already driven a few of them away with my approach.

Noether returned to Germany in the summer of 1934. There see saw her brother Fritz for what would be the last time, and visited Artin in Hamburg before going on to Göttingen. In 1980 Artin's wife recalled Noether's visit:

Now the one thing I remember most vividly is the trip on the Hamburg Untergrund, which is the subway in Hamburg. We picked up Emmy at the Institute, and she and Artin immediately started talking mathematics. At that time it was Idealtheorie, and they started talking about Ideal, Führer, and Gruppe, and Untergruppe, and the whole car suddenly started pricking up their ears. [Each of the German nouns has both mathematical and political meanings.] And I was frightened to death - I thought, my goodness, next thing's going to happen, somebody's going to arrest us. Of course, that was in 1934, and all. But Emmy was completely oblivious, and she talked very loudly and very excitedly, and got louder and louder, and all the time the "Führer" came out, and the "Ideal". She was very full of life, and she constantly talked very fast and very loud.

She returned to the United States where her visiting professorship at Bryn Mawr had been extended for a further year. She continued her weekly lectures at Princeton where Richard Brauer had now arrived. After her lectures she enjoyed talking about mathematics with Weyl, Veblen and Brauer.

Noether's death was sudden and unexpected. In April 1935 doctors discovered that she had a tumour. Two days later they operated, finding further tumours which they believed to be benign and did not remove. The operation seemed a success and for three days her condition improved. However, on the fourth day she suddenly collapsed and developed a very high temperature. She died later that day.

Weyl in his Memorial Address said:

Her significance for algebra cannot be read entirely from her own papers, she had great stimulating power and many of her suggestions took shape only in the works of her pupils and co-workers.

Van der Waerden wrote:

For Emmy Noether, relationships among numbers, functions, and operations became transparent, amenable to generalisation, and productive only after they have been dissociated from any particular objects and have been reduced to general conceptual relationships.

Although she received little recognition in her lifetime considering the remarkable advances that she made, she has been honoured in many ways following her death. A crater on the moon is named for her. A street in her hometown is named for her and the school she attended is now named the Emmy Noether School. Various organisations name scholarships and lectures after Emmy Noether.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

5.7. Cuestionario

1. Da todos los ideales primarios de $\mathbb{Z}$.
2. ¿Son todos los ideales primarios de $k[x]$ irreducibles?
3. Prueba que si A es un anillo íntegro entonces (0) es irreducible. Prueba que los ideales primos son irreducibles.
4. Sea A un anillo noetheriano. Si $I \subsetneq A$ es un ideal irreducible, prueba que $(I)_0$ es irreducible.
5. ¿Son las descomposicones primarias reducidas de todo ideal $I \subsetneq \mathbb{Z}$ únicas?
6. Sea $I \subsetneq A$ un ideal radical de un anilllo noetheriano ¿Existe una única descomposición primaria reducida de I?
7. Calcula los divisores de cero del anillo $k[x,y]/((x)\cap(y)\cap(x,y)^3)$.

5.8. Problemas

1. Sea $A = k[x,y]/(x,y)^2$. Escribe el ideal (0) como intersección de ideales irreducibles ¿Es el ideal (0) un ideal primario?

2. Sea A un anillo noetheriano e $I \subseteq A$ un ideal. Si I no es irreducible, sean I_1 e I_2 dos ideales que contienen estrictamente a I tales que $I = I_1 \cap I_2$. Repitiendo este proceso con I_1 e I_2 y así sucesivamente, prueba que este proceso termina en un número finito de pasos, obteniéndose I como intersección de un número finito de ideales irreducibles.

3. Prueba que en $k[x,y]$ se cumple que $(x) \cap (x,y)^2 = (x) \cap (y,x^2)$ ¿Son las descomposiciones primarias únicas?

4. Sea $\mathfrak{m} \subset A$ un ideal maximal y $\mathfrak{p} \subset \mathfrak{m}$ un ideal primo tal que $\mathfrak{p} \not\subseteq \mathfrak{m}^2$ ¿Puede ser $\mathfrak{p} \cap \mathfrak{m}^2$ un ideal primario?

5. Calcula la descomposición primaria de $60 \cdot \mathbb{Z} \subset \mathbb{Z}$.

6. Sea $\mathfrak{q} \subset A$ un ideal $\mathfrak{p}$-primario. Prueba que $(\mathfrak{q}) \subset A[x]$ es un ideal $(\mathfrak{p})$-primario.

7. Sea $A = k[x,y,z]$, $\mathfrak{q} = (y^2, z^3) \subset A$ y $\mathfrak{p} = (y,z) \subset A$. Prueba que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario, $\mathfrak{q} \subset (y^2, xy, z^3) \subset \mathfrak{p}$ y que (y^2, xy, z^3) no es un ideal primario.

8. Sea I un ideal de un anillo noetheriano A. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida y supongamos que $r(\mathfrak{q}_1) = \mathfrak{m}_x$ es un ideal maximal de A y que $\mathfrak{q}_1$ no es una componente primaria sumergida. Prueba que existe $r > 0$ tal que $0 = \overline{\mathfrak{m}_x^r} \subset A/(I + \mathfrak{m}_x^{r+1})$ y en tal caso $I = (I + \mathfrak{m}_x^r) \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$.

9. Calcula la descomposición primaria de $I = (xy, -y + x^2 + y^2)$ en $\mathbb{C}[x,y]$.

10. Calcula una descomposición primaria reducida de los ideales

    a) $I = (x,y) \cdot (x, y-1)$ en $\mathbb{C}[x,y]$.

    b) $I = (x) \cdot (x,y) \cdot (x, y-1)$ en $\mathbb{C}[x,y]$.

11. Halla la descomposición primaria del ideal de $\mathbb{C}[x,y]$ de los polinomios que se anulan en los puntos de corte 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.

12. Sean I, J dos ideales de un anillo noetheriano A. Prueba

a) Sea $\pi : A \to A/I$ el morfismo de paso al cociente. Entonces, $\pi(I : J) = (0 : \pi(J))$ y $(I : J) = \pi^{-1}(0 : \pi(J))$.

b) Sea $S \subset A$ un sistema multiplicativo. Entonces, $(I : J)_S = (I_S : J_S)$.

c) $(I : (a_1, \ldots, a_n)) = \bigcap_{i=1}^{n} (I : a_i)$.

d) Si $I \cap (a) = (ab_1, \ldots, ab_r)$, entonces $(I : a) = (b_1, \ldots, b_r) + (0 : a)$.

e) Si $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ son ideales primos tales que $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$, para todo $i \neq j$, entonces $(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n : \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m) = \mathfrak{p}_{m+1} \cap \cdots \cap \mathfrak{p}_n$.

f) Si I es un ideal radical, entonces $(I : J)_0$ es la unión de la componentes irreducibles de $(I)_0$ que no están contenidas en $(J)_0$.

Capítulo 6

Teoría de la eliminación

El objetivo de este capítulo es proporcionar algoritmos para el cálculo efectivo de diversos objetos definidos a lo largo del curso: el cierre de la imagen de un morfismo de variedades algebraicas (o teoría de la eliminación o resolución de un sistema de ecuaciones algebraicas), el cierre proyectivo de una variedad afín, la resolución de un módulo por módulos libres, la descomposición primaria de un ideal, etc.

Para ello, definiremos la resultante de dos polinomios y las bases de Gröbner. Para el cálculo de ambos introduciremos un algoritmo de división, que puede decirse que es la generalización en varias variables del algoritmo de división de Euclides.

6.1. Resultante de dos polinomios

Sean $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m$ variables $\mathbb{Z}$-algebraicamente independientes y sean $P(x) := a_0x^n + a_1x^{n-1} + \cdots + a_n$ y $Q(x) := b_0x^m + b_1x^{m-1} + \cdots + b_m$ polinomios genéricos de grados n y m.

Sean $x_1, \ldots, x_n$ las raíces de $P(x)$ e $y_1, \ldots, y_m$ las raíces de $Q(x)$. Observemos que $a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m$ son $\mathbb{Z}$-algebraicamente independientes: El morfismo

$$\mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m) \hookrightarrow \mathbb{Q}(a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m)$$

es finito, por tanto $\operatorname{gr\,tr}_{\mathbb{Q}} \mathbb{Q}(a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m) = \operatorname{gr\,tr}_{\mathbb{Q}} \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m) = n + m + 2$, luego $a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m$ son $\mathbb{Z}$-algebraicamente independientes.

1. Definición: Llamaremos resultante genérica (de dos polinomios de grados n y m), que denotaremos $R(P,Q)$, a la resultante de P y Q, es decir:

$$R(P,Q) := a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

2. Propiedades: *1.* $R(P,Q) = (-1)^{nm} R(Q,P)$.

2. $R(P,Q) = a_0^m \prod_{i=1}^n Q(x_i)$.

3. $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$.

Demostración. (1)

$$\begin{aligned} R(P,Q) &= a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (-1)(y_i - x_j) \\ &= (-1)^{nm} b_0^n a_0^m \prod_{j=1}^m \prod_{i=1}^n (y_i - x_j) = (-1)^{nm} R(Q,P). \end{aligned}$$

(2)

$$R(P,Q) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = a_0^m \prod_{i=1}^n b_0 \prod_{j=1}^m (x_i - y_j) = a_0^m \prod_{i=1}^n Q(x_i).$$

(3) Por el apartado anterior se obtiene que $R(P,Q)$ es un polinomio en las $\{b_i\}$ y en a_0 y simétrico en las $\{x_i\}$, luego $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]_{a_0}$. 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, $R(P,Q) \in \mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m]$. □

Sea $\bar{A}$ un anillo cualquiera y

$$\left.\begin{aligned} \overline{P}(x) &= \overline{a}_0 x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_n \\ \overline{Q}(x) &= \overline{b}_0 x^m + \overline{b}_1 x^{m-1} + \cdots + \overline{b}_m \end{aligned}\right\} \in \bar{A}[x], \quad \overline{a}_0, \overline{b}_0 \neq 0$$

3. Definición: $R(\overline{P},\overline{Q}) \in \bar{A}$ es el valor obtenido en la resultante genérica $R(P,Q)$ dando a las variables $\{a_0,\dots,a_n,b_0,\dots,b_m\}$ los valores $\{\overline{a}_0,\dots,\overline{a}_n,\overline{b}_0,\dots,\overline{b}_m\}$.

Estabilidad por cambio de anillo base: Si $i\colon \bar{A} \to \bar{B}$ es un morfismo de anillos tal que $i(\bar{a}_0) \neq 0$ y $i(\bar{b}_0) \neq 0$, entonces $i(R(\bar{P},\bar{Q})) = R(P',Q')$, donde $P' = i(\overline{a_0})x^n + \cdots + i(\overline{a}_n)$ y $Q' := i(\overline{b}_0)x^m + \cdots + i(\overline{b}_m)$.

Evidentemente, $R(\bar{P},\bar{Q}) = (-1)^{nm} R(\bar{Q},\bar{P})$.

Esta definición da sentido a la resultante de polinomios cualesquiera (de grados positivos) aunque no se conozcan sus raíces, incluso sin hacer presunción de que éstas existan. Ahora bien, si $\bar{P} = \bar{a}_0(x-\bar{x}_1)\cdots(x-\bar{x}_n)$ y $\bar{Q} = \bar{b}_0(x-\bar{y}_1)\cdots(x-\bar{y}_n)$, entonces

$$R(\overline{P},\overline{Q}) = \bar{a}_0^m \bar{b}_0^n \prod_{i=1}^n \prod_{j=1}^m (\bar{x}_i - \bar{y}_j)$$

ya que ya si damos a las variables x_i el valor $\bar{x}_i$ y a a_0 el valor $\bar{a}_0$ (luego a a_i el valor $\bar{a}_i$) y si damos a las variables y_i el valor $\bar{y}_i$ y a b_0 el valor $\bar{b}_0$ (luego a b_i el valor $\bar{b}_i$), entonces el valor de $R(P,Q) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j)$ es lo requerido.

Igualmente, si $\bar{P} = \bar{a}_0(x-\bar{x}_1)\cdots(x-\bar{x}_n)$, entonces $R(\overline{P},\overline{Q}) = \bar{a}_0^m \prod_{i=1}^n \bar{Q}(\bar{x}_i)$,
El interés de la resultante lo da el siguiente teorema.

4. Teorema: *Sea k un cuerpo. Dos polinomios $\overline{P}(x),\overline{Q}(x) \in k[x]$, tienen alguna raíz en común si y solo si $R(\overline{P},\overline{Q}) = 0$.*

5. Proposición: *Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$ y $Q(x) = \sum_{i=0}^{m} b_i x^{m-i}$ dos polinomios genéricos y $P_r(x) = \sum_{i=0}^{n} a_i x^i$ y $Q_r(x) = \sum_{i=0}^{m} b_i x^i$ los polinomios recíprocos. Entonces,*

$$R(P,Q) = R(Q_r,P_r).$$

Como consecuencia se tiene que $R(P,Q) \in (a_0,b_0)$.

Demostración. $a_n = (-1)^n a_0 \cdot \prod_{i=1}^{n} x_i$ y $b_m = (-1)^m b_0 \prod_{j=1}^{m} y_j$. Luego, $a_n^m b_m^n = a_0^m b_0^n \prod_{i,j}^{n,m} x_i y_j$ y

$$R(Q_r,P_r) = a_n^m b_m^n \prod_{i,j}^{n,m} \left(\frac{1}{y_j} - \frac{1}{x_i}\right) = a_0^m b_0^n \prod_{i,j}^{n,m} (x_j - y_i) = R(P,Q).$$

Si hacemos $a_0 = b_0 = 0$, entonces $R(Q_r,P_r) = 0$, porque el cero es raíz común de ambos. Por tanto, $R(P,Q) = R(Q_r,P_r) \in (a_0,b_0) \subset \mathbb{Z}[a_0,\ldots,a_n,b_0,\ldots,b_m]$.

□

6. Proposición: *Sean Q_1 y Q_2 dos polinomios de grados m_1 y m_2 y supongamos que $\mathrm{gr}(Q_1Q_2) = m_1 + m_2$. Entonces,*

$$R(P,Q_1\dot{Q}_2) = R(P,Q_1)\cdot R(P,Q_2)$$
$$R(Q_1\dot{Q}_2,P) = R(Q_1,P)\cdot R(Q_2,P)$$

Demostración. Podemos suponer que $P(x)$ es el polinomio genérico, de raíces $x_1,\ldots,x_n$. Entonces,

$$\begin{aligned} R(P(x),Q_1(x)\cdot Q_2(x)) &= a_0^{m_1+m_2}\prod_{i=1}^{n} Q(x_i) = a_0^{m_1+m_2}\prod_{i=1}^{n} Q_1(x_i)\cdot Q_2(x_i) \\ &= a_0^{m_1}\prod_{i=1}^{n} Q_1(x_i)\cdot a_0^{m_2}\prod_{i=1}^{n} Q_2(x_i) = R(P(x),Q_1(x))\cdot R(P(x),Q_2(x)). \end{aligned}$$

Etc.

□

6.1.1. Métodos de cómputo de la resultante

Vamos a dar algoritmos explícitos de cómputo de la resultante.

A. Método directo mediante el algoritmo de Euclides:

En este apartado, supondremos que el anillo de coeficientes de los polinomios es íntegro. Este método se basa en la siguiente proposición.

7. Proposición: *Sean $C(x), R(x)$ polinomios tales que $P(x) = C(x) \cdot Q(x) + R(x)$. Entonces, se cumple la igualdad*

$$R(P,Q) = (-1)^{nm} b_0^{n-grR} R(Q,R),$$

siendo n, m los grados de P, Q respectivamente y b_0 el coeficiente en grado máximo de Q.

Demostración. De la igualdad del enunciado se obtiene $P(y_j) = R(y_j)$, siendo $\{y_j\}$ las raíces de Q, luego:

$$\begin{aligned} R(P,Q) &= (-1)^{nm} R(Q,P) = (-1)^{nm} b_0^n \textstyle\prod_j P(y_j) \\ &= (-1)^{nm} b_0^n \textstyle\prod_j R(y_j) = (-1)^{nm} b_0^n b_0^{-grR} R(Q,R). \end{aligned}$$

□

Con el algoritmo de división de Euclides y la aplicación reiterada de esta proposición podemos calcular la resultante de dos polinomios.

B. Resultante de Bézout:

8. Teorema: *Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$, $Q(x) = \sum_{i=1}^{m} b_i x^{m-i}$ polinomios con coeficientes en un cuerpo k, de grados n y m respectivamente. El determinante del endomorfismo k-lineal*

$$Q(x)\cdot : k[x]/(P(x)) \to k[x]/(P(x)), \overline{H(x)} \mapsto \overline{Q(x) \cdot H(x)},$$

multiplicado por a_0^m, es igual a $R(P,Q)$.

Demostración. Podemos suponer que P y Q son polinomios genéricos y que k es algebraicamente cerrado. En este caso, $P(x) = a_0 \cdot (x - x_1) \cdots (x - x_n)$. Por el teorema chino de los restos $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, $\overline{H(x)} \mapsto (H(x_1), \ldots, H(x_n))$. Por tanto, $\overline{Q(x)}$ es igual a $(Q(x_1), \ldots, Q(x_n))$ en $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, y el determinante $|Q(x)\cdot| = Q(x_1) \cdots Q(x_n)$. Luego, $a_0^m \cdot |Q(x)\cdot| = R(P,Q)$. □

9. Supongamos que $n = m$. Consideremos en $k[x]/(P(x))$ las dos bases siguientes $B = \{a_0, a_0 \cdot x + a_1, \ldots, a_0 x^{n-1} + \cdots + a_{n-1}\}$ y $B' = \{x^{n-1}, \ldots, x, 1\}$. Observemos que

$$Q(x) \cdot (a_0 x^i + \cdots + a_i) - P(x) \cdot (b_0 x^i + \cdots + b_i) = \sum_{j=1}^{n} c_{i+1,j} x^{n-j} \qquad (*)$$

para ciertos $c_{i+1,j} \in k$. Entonces, la matriz de $Q(x)\cdot$ en las bases B, B' es (c_{ij}) y el determinante de la matriz de cambio de base de B a B' es a_0^n. Luego,

$$R(P,Q) = (a_0)^n \cdot |Q(x)\cdot| = |(c_{ij})|.$$

Es fácil comprobar que $\boxed{c_{ij} = \sum_{\substack{r+s=i+j-1 \\ r<i, s\geq i}} a_r b_s - a_s b_r}$.

10. 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).

Supongamos que $\operatorname{gr} P(x) = n < m = \operatorname{gr} Q(x)$. $R(xP,Q) = R(x,Q)\cdot R(P,Q) = b_m \cdot R(P,Q)$ y $R(P,xQ) = R(P,x)\cdot R(P,Q) = (-1)^n \cdot P(0) \cdot R(P,Q) = (-1)^n a_n \cdot R(P,Q)$. Por lo tanto, para el cálculo de $R(P,Q)$, podemos reducirnos al caso a_n y b_m no nulos. Entonces, $x^{m-n}P$ y Q tienen grado m y $R(x^{m-n}P,Q) = Q(0)^{m-n} \cdot R(P,Q) = b_m^{m-n} \cdot R(P,Q)$.

C. Resultante de Sylvester:

11. Lema de Euler: *Sea k un cuerpo. Dos polinomios $P(x), Q(x) \in k[x]$ de grados $n, m > 0$ respectivamente, tienen una raíz común si y solo si existen polinomios no nulos $\lambda(x), \mu(x) \in k[x]$ de grados menores que m y n respectivamente, tales que:*

$$\lambda(x)P(x) + \mu(x)Q(x) = 0$$

Demostración. Supongamos que $P(x), Q(x)$ no tienen ninguna raíz en común, es decir, que son primos entre sí. Si se verifica $\lambda(x)P(x) + \mu(x)Q(x) = 0$, entonces $Q(x)$ divide a $\lambda(x)P(x)$, luego por ser primo con $P(x)$ divide a $\lambda(x)$ de donde $gr\,\lambda(x) \geq gr\,Q(x)$ en contra de lo supuesto. Si no son primos entre sí, sea $D(x) = m.c.d.(P,Q)$. Dados $\lambda(x) := \frac{Q(x)}{D(x)}$ y $\mu(x) := -\frac{P(x)}{D(x)}$ y se tiene que $\lambda(x)P(x) + \mu(x)Q(x) = 0$. □

Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$ y $Q(x) = \sum_{i=0}^{m} b_i x^{m-i} \in k[x]$.

Por el lema de Euler, estos polinomios tienen una raíz común si y solo si existen polinomios $\lambda(x), \mu(x)$ de grados menores que los de $Q(x), P(x)$ respectivamente tales que:

$$\lambda(x)P(x) + \mu(x)Q(x) = 0$$

es decir, si denotamos $k[x]_{<s} \subset k[x]$ el subespacio vectorial de los polinomios de grado menor que s, esto equivale a que la aplicación lineal:

$$\begin{aligned} k[x]_{<m} \times k[x]_{<n} &\to k[x]_{<m+n} \\ (\lambda(x), \mu(x)) &\mapsto \lambda(x)P(x) + \mu(x)Q(x) \end{aligned}$$

tenga núcleo no nulo. Eligiendo en cada espacio vectorial $k[x]_{<s}$ la base $\{x^{s-1}, x^{s-2}, \ldots, x, 1\}$, y calculando el determinante de la matriz (transpuesta) de esta aplicación lineal en dichas bases, resulta la condición:

$$S(P,Q) := \left| \begin{array}{ccccccc} a_0 & \cdots & \cdots & a_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & \cdots & \cdots & a_n \\ b_0 & \cdots & \cdots & \cdots & b_m & & \\ & \ddots & & & & \ddots & \\ & & b_0 & \cdots & \cdots & \cdots & b_m \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \end{array} = 0$$

12. Teorema: $S(P,Q) = R(P,Q)$.

Demostración. Podemos suponer que P y Q son polinomios genéricos. Observemos que $S(P,Q) = a_0^m b_0^n \cdot p(x,y) \in \mathbb{Z}[a_0, b_0][x_1, \ldots, x_n, y_1, \ldots, y_m]$ y es nulo cuando hacemos cociente por $x_i - y_j$. Por tanto, $S(P,Q)$ es múltiplo de $R(P,Q)$. Como el coeficiente que acompaña al monomio $((-1)^m y_1 \cdots y_m)^n$, que es el monomio en las y_i de grado máximo para ambos, es $a_0^m b_0^n$ para ambos, entonces coinciden.

□

6.1.2. Aplicaciones de la resultante

A. Intersección de dos curvas planas.

Sean $P(x,y), Q(x,y) \in k[x,y]$ dos polinomios en dos variables primos entre sí y sea el sistema de ecuaciones:

$$\begin{aligned} P(x,y) &= a_0(y) \cdot x^n + \cdots + a_{n-1}(y) \cdot x + a_n(y) = 0 \\ Q(x,y) &= b_0(y) \cdot x^m + \cdots + b_{m-1}(y) \cdot x + b_m(y) = 0 \end{aligned} \qquad (a_0(y), b_0(y) \neq 0)$$

que son las ecuaciones de la intersección de las curvas $P(x,y) = 0$ y $Q(x,y) = 0$.

13. Proposición: *Sea $R(y)$ la resultante de P y Q entendidos respectivamente como polinomios en x con coeficientes en $k[y]$. Entonces, β es una raíz de $R(y)$ si y solo si β es una raíz común de $a_0(y)$ y $b_0(y)$, o existe α tal que (α, β) es un punto de corte de las curvas $P(x,y) = 0$ y $Q(x,y) = 0$.*

Demostración. Por la proposición 6.1.5, $R(y) \subseteq (a_0(y), b_0(y))$, 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, $R(\beta) = a_0(\beta)^{m-\mathrm{gr}Q(x,\beta)} \cdot R(P(x,\beta), Q(x,\beta))$. Por tanto, si $R(\beta) = 0$, tenemos que $R(P(x,\beta), Q(x,\beta) = 0$ y existe α tal que $P(\alpha,\beta) = Q(\alpha,\beta) = 0$.

□

Si $\{(\alpha_1,\beta_1),\ldots,(\alpha_n,\beta_n)\}$ son los puntos de corte de las curvas $P(x,y) = 0$ y $Q(x,y) = 0$, entonces $\{(\alpha_1,\ldots,\alpha_n\},\{\beta_1,\ldots,\beta_n\}$ son respectivamente raíces de $R(x)$ y $\overline{R}(y)$.

B. Cálculo de las raíces complejas de un polinomio complejo.

Sea $P(z) \in \mathbb{C}[z]$ y escribamos $z = x + i \cdot y$. Entonces, $P(z) = U(x,y) + V(x,y) \cdot i$, con $U(x,y), V(x,y) \in \mathbb{R}[x]$. El número complejo $a + b \cdot i$ es una raíz compleja de $P(z)$ si y solo si (a,b) es una solución del sistema de ecuaciones reales

$$\begin{aligned} U(x,y) &= 0 \\ V(x,y) &= 0 \end{aligned}$$

Por el apartado anterior, si (a,b) es una solución real del sistema de ecuaciones, entonces a es una raíz real de la resultante, $R(x) = R(U(x,y), V(x,y))$, considerados como polinomios en y; y b es una raíz real de la resultante de $\bar{R}(y) = R(U(x,y), V(x,y))$, considerados como polinomios en x. Para calcular las raíces complejas de $P(z)$ basta calcular las raíces reales de $R(x)$ y $\bar{R}(y)$.

C. Solución de un sistema de ecuaciones algebraicas

Consideremos un sistema de ecuaciones algebraicas

$$\begin{aligned} P_1(x_1,\ldots,x_n) &= 0 \\ &\cdots \\ P_n(x_1,\ldots,x_n) &= 0 \end{aligned}$$

Sea $R_i(x_2,\ldots,x_n) := R(P_1(x_1,\ldots,x_n), P_i(x_1,\ldots,x_n))$, para todo $1 < i \leq n$, 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 $R_2 = \ldots = R_n = 0$.

D. Discriminante.

Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n$.

14. 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. Observemos que

$$R(P,Q)=R(\frac{P(x)}{x-\alpha}(x-\alpha),Q(x))=R(\frac{P(x)}{x-\alpha},Q(x))\cdot R(x-\alpha,Q(x))=R(\frac{P(x)}{x-\alpha},Q(x))\cdot Q(\alpha).$$

Luego,

$$\boxed{\frac{1}{Q(\alpha)}=\frac{1}{R(P,Q)}\cdot R(\frac{P(x)}{x-\alpha},Q)}$$

F. Polinomio de raíces una función de las raíces de otro polinomio.

Sea $P(x)\in k[x]$ y $\alpha_1,\ldots,\alpha_n$ las raíces de $P(x)$ y, sea $f(x)=\frac{A(x)}{B(x)}\in k(x)$ una función racional, tal que B es primo con P (para que tenga sentido hacer $x=\alpha_i$ en $f(x)$). *Se trata de calcular otro polinomio* $Q(x)\in k[x]$ *cuyas raíces sean* $f(\alpha_1),\ldots,f(\alpha_n)$.

Para ello se considera el sistema de ecuaciones:

$$\left.\begin{aligned}P(x)&=0\\A(x)-B(x)y&=0\end{aligned}\right\}$$

Las raíces del polinomio $R(y):=R(P(x),A(x)-B(x)y)$ son $f(\alpha_1),\ldots,f(\alpha_n)$: La condición necesaria y suficiente para que $R(\beta)=0$ es que los polinomios $\{P(x),A(x)-B(x)\beta\}$ tengan una raíz común α. Esto es que exista α tal que

$$\left.\begin{aligned}P(\alpha)&=0\\\beta&=\frac{A(\alpha)}{B(\alpha)}\end{aligned}\right\}$$

es decir, que $\beta=f(\alpha)$ para alguna raíz α de $P(x)$.

15. 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 $x = z^2$.)

6.2. Bases de Gröbner

6.2.1. Órdenes monomiales

1. Notaciones: Denotaremos $R = k[x_1, \ldots, x_r]$ y será L un R-módulo libre de base $\{e_1, \ldots, e_s\}$. Dado un monomio $x^\alpha \in R$, diremos que $x^\alpha \cdot e_i \in L$ es un monomio de L. Un término de L es un monomio multiplicado por un escalar $\lambda \in k$.

Dados dos términos $m = \lambda \cdot x^\alpha \cdot e_i, n = \mu \cdot x^\beta \cdot e_j \in L$, diremos que m es divisible por n si $i = j$ y x^α es divisible por x^β, y escribiremos $m/n = \frac{\lambda}{\mu} x^{\alpha-\beta}$. Definiremos

$$m.c.d(m,n) = \begin{cases} m.c.d.(x^\alpha, x^\beta) \cdot e_i, & \text{si } i = j. \\ \emptyset, & \text{si } i \neq j. \end{cases}$$

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, $m_1 > m_2$ y x^α es un monomio de R con $\alpha \neq 0$, 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.

3. Ejercicio: Prueba que dar un orden monomial en R es equivalente a dar un orden $<$ en $\mathbb{N}^r$ que cumple que si $\alpha > \beta$ entonces $\alpha + \gamma > \beta + \gamma > \beta$ para todo $\gamma \neq 0$.

Demos algunos ejemplos de órdenes monomiales en R. Dado $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$ denotamos $|\alpha| = \alpha_1 + \cdots + \alpha_r$.

4. Definición: Diremos que $>_{lex}$ es el orden lexicográfico en R si $x^\alpha >_{lex} x^\beta$ si y solo si $\alpha_i > \beta_i$ para el primer índice i que $\alpha_i \neq \beta_i$.

Diremos que $>_{hlex}$ es el orden lexicográfico homogéneo en R si $x^\alpha >_{hlex} x^\beta$ si y solo si $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ y $\alpha_i > \beta_i$ para el primer índice i que $\alpha_i \neq \beta_i$.

Diremos que $>_{ilex}$ es el orden lexicográfico inverso en R si $x^\alpha >_{ilex} x^\beta$ si y solo si $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ y $\alpha_i < \beta_i$ para el último índice i que $\alpha_i \neq \beta_i$.

Por ejemplo, $x_1x_3^2 >_{hlex} x_2x_3^2$ y $x_1x_3^2 >_{ilex} x_2x_3^2$; $x_1x_2x_3 >_{hlex} x_2^3$ y $x_1x_2x_3 <_{ilex} x_2^3$.

Si L es un R-módulo libre de base $\{e_1,\dots,e_s\}$ y tenemos un orden monomial $>$ en R, podemos definir un orden monomial en L del modo que sigue: $x^\alpha e_i > x^\beta e_j$ si $i < j$ ó $i = j$ y $x^\alpha > x^\beta$.

5. Lema: *Sean $z, z_1,\dots,z_s$ términos de L. Si $z \in \langle z_1,\dots,z_s\rangle_R$, entonces z es divisible por algún z_i.*

Demostración. Se cumple que $z = \sum_{i=1}^s p_i \cdot z_i$, para ciertos $p_i \in R$. Por tanto, para algún i y algún término t_i de p_i, $z = t_i \cdot z_i$ (salvo un escalar). □

6. Proposición: *Todo orden monomial en L es artiniano (es decir, todo subconjunto de monomios tiene un mínimo).*

Demostración. Sea Z un conjunto de monomios de L. El R-submódulo de L generado por Z está generado por un número finito de ellos $\{z_1,\dots,z_s\}$, pues L es noetheriano. Por el lema anterior, cada monomio de Z es múltiplo de algún z_i. Por tanto, el menor de $\{z_1,\dots,z_s\}$ es el mínimo de Z. □

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 $i_1 > i_2 > \cdots > i_n > \cdots$.

7. 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 $max(M)$).

8. Ejercicio: Sea $f \in R = k[x_1,\dots,x_r]$ homogénea.

1. Si $max_{>_{hlex}} f \in k[x_s,\dots,x_r]$ para algún s, entonces $f \in k[x_s,\dots,x_r]$.

2. Si $max_{>_{ilex}} f \in (x_s,\dots,x_r)$ para algún s, entonces $f \in (x_s,\dots,x_r)$.

Dado $f \in L$ y $p \in R$, sea n el término de p tal que $n \cdot max(f)$ sea máximo, entonces $max(pf) = n \cdot max(f)$: sea m un término de f y n' otro término de p tenemos que $n' \cdot m \leq n' \cdot max(f) \leq n \cdot max(f)$. En particular, $max(x^\alpha \cdot f) = x^\alpha \cdot max(f)$. Por tanto, $max(M) = \langle max(f), f \in M\rangle_k$.

9. Definición: Sea E un k-espacio vectorial e I un conjunto totalmente ordenado artiniano. Sea para cada $i \in I$, un subespacio vectorial $E_i \subseteq E$, de modo que $E_i \subseteq E_{i'}$, si $i < i'$. Diremos que la cadena de subespacios vectoriales de E, $\{E_i\}_{i\in I}$, es filtrante si $\cup_{i\in I} E_i = E$. Denotaremos $G_iE := E_i/\cup_{j<i} E_j$ y $GE := \oplus_{i\in I} G_iE$ (si $0 \in I$ es el mínimo de I, definimos $G_0E := E_0$).

10. Lema: *Si para cada $i \in I$, $\{e_{ij}\}_j$ son vectores de E_i cuyas clases forman una base de G_iE entonces los vectores $\{e_{ij}\}_{i,j}$ forman una base de E.*

Demostración. Dado $0 \neq e \in E$, sea i mínimo tal que $e \in E_i$. Entonces, $\bar{e} = \sum_j \lambda_{ij}\bar{e}_{ij}$ en G_iE y sea $e' = e - \sum_j \lambda_{ij}e_{ij}$. Si $e' \neq 0$, sea $i' < i$ mínimo tal que $e' \in E_{i'}$. Entonces, $\bar{e}' = \sum_{j'} \lambda'_{i'j'}\bar{e}_{i'j'}$ en $G_{i'}E$ y sea $e'' = e' - \sum_{j'} \lambda_{i'j'}e_{i'j'}$. Por ser I artiniano este proceso termina en un número finito de pasos, con lo que podremos escribir e como combinación lineal de los e_{rs}.

Los vectores $\{e_{ij}\}_{i,j}$ son linealmente independientes: Sea $e = \sum_{ij} \lambda_{ij}e_{ij}$, con algún $\lambda_{i'j'} \neq 0$. Sea i'' maximal cumpliendo que existe j'' tal que $\lambda_{i''j''} \neq 0$. Entonces, $\bar{e} = \sum_j \lambda_{i''j}\bar{e}_{i''j}$ en $G_{i''}E$, y $\bar{e}$ es no nulo porque $\{\bar{e}_{i''j}\}_j$ es la base considerada en $G_{i''}E$. Por tanto, e es no nulo.

□

11. 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 $i \in I$. Tenemos el morfismo natural $GT: GE \to GE'$, $(\bar{e}_i)_{i\in I} \mapsto (\overline{T(e_i)})_{i\in I}$.*

Entonces, T es inyectivo (resp. epiyectivo, isomorfismo) si $GT: GE \to GE'$ es inyectivo (resp. epiyectivo, isomorfismo).

Demostración. Si GT es inyectivo entonces T es inyectivo: Dado $0 \neq e \in E$ sea i mínimo tal que $e \in E_i$. Entonces $0 \neq \bar{e} \in G_iE$, luego $0 \neq GT(\bar{e}) = \overline{T(e)}$ y $T(e) \neq 0$.

Si GT es epiyectivo entonces T es epiyectivo: Si T no es epiyectivo, sea i mínimo para el que existe $e' \in E'_i$ de modo que $e' \notin \operatorname{Im} T$. Evidentemente, $0 \neq \bar{e'} \in G_iE'$. Sea $\bar{e} \in G_iE$, tal que $GT(\bar{e}) = \bar{e'}$. Entonces, $\overline{e' - T(e)} = 0 \in G_iE'$, luego existe $j < i$ tal que $e' - T(e) \in E'_j$. Por tanto, por la elección de i, existe $v \in E$ tal que $e' - T(e) = T(v)$. En conclusión, $e' = T(e + v) \in \operatorname{Im} T$ y hemos llegado a contradicción. □

Sea E espacio vectorial con una cadena filtrante $\{E_i\}_{i\in I}$ de subespacios vectoriales. Dado un subespacio vectorial $E' \subseteq E$ tenemos la cadena filtrante de subespacios vectoriales de E', $\{E' \cap E_i\}_{i\in I}$. En el espacio vectorial cociente $\bar{E} = E/E'$ tenemos la cadena filtrante de subespacios vectoriales $\{\bar{E}_i\}_{i\in I}$. Se cumple que la sucesión natural

$$0 \to GE' \to GE \to G\bar{E} \to 0$$

es exacta.

12. Sea I el conjunto de los monomios de L. Para cada $m \in I$, denotemos $L_m = \langle m \rangle_k$ y consideremos en L la cadena filtrante de subespacios vectoriales

$$\{L_{\leq m} := \underset{i \leq m}{\oplus} L_i\}_{m \in I}.$$

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,

$$max(M) = GM \subset GL = L.$$

13. Teorema de Macaulay: *Las clases en L/M de los monomios de L que no pertenecen a $max(M)$ forman una base de L/M.*

Demostración. De la sucesión exacta

$$0 \longrightarrow max(M) = GM \longrightarrow GL = L \longrightarrow G(L/M) \longrightarrow 0$$

obtenemos que las clases de los monomios de L que no pertenecen a $max(M)$ forman una base de $G(L/M)$. Por el lema anterior, las clases en L/M de los monomios de L que no pertenecen a $max(M)$ forman una base de L/M.

□

14. 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 6.2.11.

□

6.2.2. Criterio de Buchberger

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.

15. 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 $max(M)$.

16. 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 la proposición 6.2.6), f_1' cumple la proposición, luego f también.

□

17. 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.

18. Criterio de Buchberger: *Sea $M = \langle f_1, \ldots, f_t\rangle \subseteq L$ un submódulo. Para $1 \leq i < j \leq t$, sea*

$$f_{ij} = \begin{cases} \frac{max(f_j)}{m.c.d.(max(f_i).max(f_j))} \cdot f_i - \frac{max(f_i)}{m.c.d.(max(f_i).max(f_j))} \cdot f_j, & si\ m.c.d.(max(f_i), max(f_j)) \neq \emptyset \\ 0, & si\ m.c.d.(max(f_i), max(f_j)) = \emptyset \end{cases}$$

y 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 solo si $f_{ij}' = 0$, para todo $i < j$.

Demostración. Si $f_1, \ldots, f_t$ forman una base de Gröbner de M, entonces como $f_{ij}' = f_{ij} - \sum_i p_i f_i \in M$, entonces $max(f_{ij}') \in max(M) = \langle max(f_1), \ldots, max(f_t)\rangle$ 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 $\{\xi_1, \ldots, \xi_t\}$ y consideremos el epimorfismo de R-módulos $\pi : R^t \to M$, $\pi(\xi_i) = f_i$.

Consideremos en R^t el orden monomial $>$ definido por:

$$x^\alpha \cdot \xi_i > x^\beta \cdot \xi_j \text{ si } \begin{cases} max(x^\alpha \cdot f_i) > max(x^\beta \cdot f_j). \\ \text{ó} \\ max(x^\alpha \cdot f_i) = max(x^\beta \cdot f_j) \text{ (salvo un escalar) e } i < j. \end{cases}$$

Sea J el conjunto de todos los monomios de R^t. Consideremos en M la filtración $\{M_{\leq x^\alpha \cdot \xi_i} := \pi((R^t)_{\leq x^\alpha \cdot \xi_i})\}_{x^\alpha \cdot \xi_i \in J}$. Evidentemente, $G_{x^\alpha \cdot \xi_i} M = k \cdot \overline{x^\alpha \cdot f_i}$. Se cumple que

$$G_{x^\alpha \cdot \xi_i} M = \begin{cases} 0, & \text{si existe } x^\beta \xi_j < x^\alpha \cdot \xi_i : x^\beta \cdot max(f_j) = x^\alpha \cdot max(f_i). \\ \neq 0, & \text{en otro caso.} \end{cases}$$

En efecto, supongamos que existen $x^\beta \xi_j < x^\alpha \cdot \xi_i$ de modo que $x^\beta \cdot max(f_j) = x^\alpha \cdot max(f_i)$. Tomemos el j mínimo posible, es decir, $x^\beta \cdot \xi_j$ es el máximo monomio menor que $x^\alpha \cdot \xi_i$. Entonces, $G_{x^\alpha \cdot \xi_i} = M_{\leq x^\alpha \cdot \xi_i} / M_{\leq x^\beta \cdot \xi_j}$. Denotemos $m_{ij} = m.c.d.(max(f_i), max(f_j))$. De la igualdad $x^\beta \cdot max(f_j) = x^\alpha \cdot max(f_i)$, se deduce que $x^\alpha = x^\gamma \cdot (max(f_j)/m_{ij})$ y que $x^\beta = x^\gamma \cdot (max(f_i)/m_{ij})$, para cierto monomio x^γ. Entonces,

$$x^\alpha \cdot f_i - x^\beta \cdot f_j = x^\gamma \cdot ((max(f_j)/m_{ij}) \cdot f_i - (max(f_i)/m_{ij}) \cdot f_j) = x^\gamma \cdot f_{ij} = x^\gamma \cdot \sum_k p_k f_k,$$

que pertenece a $M_{\leq x^\beta \cdot \xi_j}$ porque todo término $\lambda \cdot x^{\gamma'}$ del polinomio p_k, con $\lambda \neq 0$, cumple que $x^\gamma \cdot x^{\gamma'} \cdot \text{máx}(f_k) \leq x^\gamma \cdot \text{máx}(p_k f_k) \leq x^\gamma \cdot \text{máx}(f_{ij}) < \text{máx}(x^\beta f_j) = x^\beta \,\text{máx}(f_j)$. Por lo tanto, $x^\alpha \cdot f_i \in M_{\leq x^\beta \cdot \xi_j}$ y $G_{x^\alpha \cdot \xi_i} M = 0$. En caso contrario, tenemos un morfismo natural $G_{x^\alpha \cdot \xi_i} M \to G_{x^\alpha \cdot \text{máx}(f_i)} M \subset G_{x^\alpha \cdot \text{máx}(f_i)} L$, obviamente $G_{x^\alpha \cdot \xi_i} M = k \cdot \overline{x^\alpha \cdot f_i}$ y como el morfismo $G_{x^\alpha \cdot \xi_i} M \to G_{x^\alpha \cdot max(f_i)} L$ aplica $\overline{x^\alpha \cdot f_i}$ en $x^\alpha \cdot max(f_i)$, que es no nulo, concluimos que $\overline{x^\alpha \cdot f_i}$ es no nulo.

Dado $f \in M$, sea $x^\alpha \cdot \xi_i$ el mínimo tal que $f \in M_{\leq x^\alpha \cdot \xi_i}$. Entonces, $0 \neq \bar{f} \in G_{x^\alpha \cdot \xi_i} M$ y $\bar{f} = \lambda \cdot \overline{x^\alpha \cdot f_i}$, para cierto escalar λ no nulo, y su imagen en $G_{x^\alpha \cdot max(f_i)} M$ es $\lambda \cdot x^\alpha \cdot max(f_i)$. En conclusión, $max(M) = \langle max(f_1), \ldots, max(f_t) \rangle$.

□

19. Observación: El criterio de Buchberger nos da un algoritmo para calcular una base de Gröbner. Dado un submódulo $M = \langle f_1, \ldots, f_t \rangle \subset L$ si $f_1, \ldots, f_t$ no forman una base de Gröbner entonces algún $f'_{ij} \neq 0$ (seguimos notaciones del criterio). Sustituyamos $f_1, \ldots, f_t$ por $f_1, \ldots, f_t, f'_{ij}$ y repitamos el proceso. Este proceso acaba en un número finito de pasos pues las inclusiones $\langle max(f_1), \ldots, max(f_t) \rangle \underset{\neq}{\subset} \langle max(f_1), \ldots, max(f_t), max(f'_{ij}) \rangle$ son estrictas.

20. Ejemplo: Sea $p_1(x_1,\dots,x_n) = \cdots = p_r(x_1,\dots,x_n) = 0$ un sistema de ecuaciones algebraicas y supongamos que la variedad de soluciones X es de dimensión cero. Es decir, por el teorema de normalización de Noether tenemos un morfismo finito $k \hookrightarrow k[x_1,\dots,x_n]/(p_1,\dots,p_r) = A_X$. Sea $(g_1,\dots,g_s)$ una base de Gröbner de $(p_1,\dots,p_r)$. Las clases en A_X de los monomios x^β, que no son divisibles por ningún máx(g_i), forman una base de A_X. Sabemos calcular, pues, $(X) := \dim_k A_X$.

21. Teorema de Schreyer: *Sea $M = \langle g_1,\dots,g_t\rangle \subseteq L$ un submódulo generado por una base de Gröbner. Denotemos $m_{ij} = m.c.d.(max(g_i), max(g_j))$. Si $m_{ij} \neq \emptyset$, denotemos $g_{ij} := \frac{max(g_j)}{m_{ij}} \cdot g_i - \frac{max(g_i)}{m_{ij}} \cdot g_j$, y sea por el criterio de Buchberguer*

$$g_{ij} = \sum_k p_k g_k$$

una expresión estándar de g_{ij} respecto de $g_1,\dots,g_t$.

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 $\phi\colon \Lambda^2 R^t \to R^t$ el morfismo definido por

$$\phi(\xi_i \wedge \xi_j) = \begin{cases} 0, & \text{si } m_{ij} = \emptyset. \\ \frac{max(g_j)}{m_{ij}} \cdot \xi_i - \frac{max(g_i)}{m_{ij}} \cdot \xi_j - \sum_k p_k \xi_k, & \text{si } m_{ij} \neq \emptyset. \end{cases}$$

Entonces, la sucesión de morfismos de R-módulos

$$\Lambda^2 R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$$

es exacta.

Además, si en R^t definimos el orden monomial $>$: $x^\alpha \cdot \xi_i > x^\beta \cdot \xi_j$ si $max(x^\alpha \cdot g_i) > max(x^\beta \cdot g_j)$ o $max(x^\alpha \cdot g_i) = max(x^\beta \cdot g_j)$ (salvo un escalar) y $i < j$, entonces $\phi(\xi_i \wedge \xi_j)$ es una base de Gröbner de $\operatorname{Ker}\pi$.

Demostración. Por la proposición 6.2.11, la sucesión $\Lambda^2 R^t \xrightarrow{\phi} R^t \xrightarrow{\pi} M \to 0$ es exacta si tomando "graduados" es exacta.

Sea J el conjunto de todos los monomios de R^t y consideremos el R^t el orden monomial definido en el enunciado del teorema. 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,

$$G_{x^\alpha \cdot \xi_i} M = \begin{cases} 0, & \text{si existe } x^\beta \xi_j < x^\alpha \cdot \xi_i \text{ tal que } x^\beta \cdot max(g_j) = x^\alpha \cdot max(g_i). \\ k \cdot \overline{x^\alpha \cdot g_i} \neq 0, & \text{en otro caso.} \end{cases}$$

Definamos

$$(\Lambda^2 R^t)_{x^\alpha\cdot\xi_i} := \bigoplus_{\substack{j>i \\ x^\gamma\cdot max(g_j)/m_{ij}=x^\alpha}} k\cdot x^\gamma\cdot\xi_i\wedge\xi_j$$

Existe x^γ (único) tal que $x^\gamma\cdot max(g_j)/m_{ij}=x^\alpha$ si y solo si $max(g_j)$ divide a $x^\alpha\cdot m_{ij}$, que equivale a que divida a $x^\alpha\cdot max(g_i)$, que equivale a que existe x^β tal que $x^\beta\cdot max(g_j)=x^\alpha\cdot max(g_i)$. Por tanto, $(\Lambda^2R^t)_{x^\alpha\cdot\xi_i}=0$ si y solo si no existe $j>i$ tal que $x^\beta\cdot max(g_j)=x^\alpha\cdot max(g_i)$. Consideremos en Λ^2R^t la filtración $\{(\Lambda^2R^t)_{\leq x^\alpha\cdot\xi_i}:=\oplus_{x^\beta\cdot\xi_j\leq x^\alpha\cdot\xi_i}(\Lambda^2R^t)_{x^\beta\cdot\xi_j}\}$. Por tanto, $G_{x^\alpha\cdot\xi_i}\Lambda^2R^t=(\Lambda^2R^t)_{x^\alpha\cdot\xi_i}$. Observemos que $\phi((\Lambda^2R^t)_{\leq x^\alpha\cdot\xi_i})\subseteq(R^t)_{\leq x^\alpha\cdot\xi_i}$. Las sucesiones

$$G_{x^\alpha\cdot\xi_i}\Lambda^2R^t\xrightarrow{G\phi}G_{x^\alpha\cdot\xi_i}R^t\xrightarrow{G\pi}G_{x^\alpha\cdot\xi_i}M\to 0$$

son exactas (en la demostración del criterio de Buchberger probamos que $G_{x^\alpha\cdot\xi_i}M=k\cdot\overline{x^\alpha\cdot f_i}$ y que es nulo si solo si existen x^β y $j>i$ tales que $x^\beta\cdot max(g_j)=x^\alpha\cdot max(g_i)$). Luego, $G\Lambda^2R^t\to G\operatorname{Ker}\pi$ es epiyectivo. Por la proposición 6.2.11, tenemos que el morfismo $\Lambda^2R^t\to\operatorname{Ker}\pi$ es epiyectivo y concluimos que

$$\Lambda^2R^t\xrightarrow{\phi}R^t\xrightarrow{\pi}M\to 0$$

es exacta. Por último, como $G\Lambda^2R^t=\Lambda^2R^t=\langle\xi_i\wedge\xi_j\rangle$, entonces

$$max(\operatorname{Ker}\pi)=G\operatorname{Ker}\pi=G\phi(\Lambda^2R^t)=\langle G\phi(\xi_i\wedge\xi_j)\rangle=\langle max(\phi(\xi_i\wedge\xi_j))\rangle,$$

y $\phi(\xi_i\wedge\xi_j)$ es una base de Gröbner de $\operatorname{Ker}\pi$.

□

22. Observación: Si $M=\langle f_1,\dots,f_t\rangle\subset L$ no está generado por una base de Gröbner, mediante el algoritmo de Buchberger completemos a una base de Gröbner $M=\langle f_1,\dots,f_{t'}\rangle$. Consideremos la sucesión exacta $\Lambda^2R^{t'}\xrightarrow{\phi'}R^{t'}\xrightarrow{\pi'}M\to 0$ del teorema de Schreyer. Escribamos $f_i=\sum_{j=1}^t p_{ij}f_j$, para todo $1\leq i\leq t'$ (podemos decir que $p_{ij}=\delta_{ij}$, para todo $i\leq t$ y todo j). Sea $\varphi\colon R^{t'}\to R^t$ el epimorfismo definido por $\varphi(\xi_i)=\sum_j p_{ij}\xi_j$ y $\pi\colon R^t\to M$, $\pi(\xi_i)=f_i$. Entonces, el diagrama

$$\begin{array}{ccccccc}\Lambda^2R^{t'} & \xrightarrow{\phi'} & R^{t'} & \xrightarrow{\pi'} & M & \longrightarrow & 0\\ & & \downarrow{\scriptstyle\varphi} & \nearrow{\scriptstyle\pi} & & & \\ & & R^t & & & & \end{array}$$

es conmutativo y la sucesión

$$\Lambda^2R^{t'}\xrightarrow{\varphi\circ\phi'}R^t\xrightarrow{\pi}M\to 0$$

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.

6.2.3. Aplicaciones

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 6.2.16, sabemos (de modo algorítmico) decidir si $f \in M$ y en caso afirmativo escribir $f = \sum_i p_i g_i$. y por tanto sabemos escribir $f = \sum_i p'_i f_i$.

Las clases de los monomios que no pertenecen a $max(M) = \langle max(g_1), \dots, max(g_{t'}) \rangle$ forman una base de L/M. Dado $\bar{f} \in L/M$, por la proposición 6.2.16, 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.

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

$$\bar{x}_{s+1}, \dots, \bar{x}_r \in k[x_1, \dots, x_r]/(p_1, \dots, p_t)$$

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 $k[x_{s+1}, \dots, x_r] \cap (p_1, \dots, p_t)$. Este cálculo es equivalente a 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 $\bar{y}_i$. Nos hemos reducido al caso anterior.

De nuevo, este problema es equivalente a calcular el cierre de la imagen de un morfismo entre variedades afines

$$\begin{array}{rcl} X = \operatorname{Spec} k[x_1, \dots, x_r]/(p_1, \dots, p_t) & \longrightarrow & \mathbb{A}^s = \operatorname{Spec} k[y_1, \dots, y_s] \\ (\alpha_1, \dots, \alpha_r) & \longmapsto & (q_1(\alpha_1, \dots, \alpha_r), \dots, q_s(\alpha_1, \dots, \alpha_r)) \end{array}$$

Dado un morfismo $f: X \to Y$ entre variedades algebraicas afines y una inclusión $i: Y \hookrightarrow \mathbb{A}^s$, el cierre de la imagen de f es igual al cierre de la imagen de $i \circ f: X \to \mathbb{A}^s$.

23. 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 $f \in k[x_s,\dots,x_r]$.*

24. Proposición: *Consideremos el orden lexicográfico en $k[x_1,\dots,x_r]$ y un ideal $I \subseteq k[x_1,\dots,x_r]$ de base de Gröbner $g_1,\dots,g_t$. Si $g_1,\dots,g_{t'}$ son aquellos g_i en los que no aparecen las variables $x_1,\dots,x_s$, entonces*

$$k[x_{s+1},\dots,x_r] \cap I = (g_1,\dots,g_{t'}), \qquad (\textit{ideal de } k[x_{s+1},\dots,x_r]).$$

Demostración. Obviamente, $(g_1,\dots,g_{t'}) \subseteq k[x_{s+1},\dots,x_r] \cap I$.

Dado $f \in k[x_{s+1},\dots,x_r] \cap I$, se tiene que $max(f)$ es un múltiplo de un $max(g_i)$ y en él no aparecen las variables $x_1,\dots,x_s$, luego $max(f) \in \langle max(g_1),\dots,max(g_{t'})\rangle_{k[x_{s+1},\dots,x_r]}$. Por tanto, la inclusión $(g_1,\dots,g_{t'}) \subseteq k[x_{s+1},\dots,x_r] \cap I$ en graduados es epiyectiva, luego es una igualdad. □

25. Ejemplo: Sea $p_1(x_1,\dots,x_n) = \cdots = p_r(x_1,\dots,x_n) = 0$ un sistema de ecuaciones k-algebraicas y supongamos que la variedad de soluciones X es de dimensión cero. Cada $\bar{x}_i$ en $k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ es k-algebraico. Calculemos $k[x_i] \cap (p_1,\dots,p_r) = (q_i(x_i))$. Entonces, el conjunto de soluciones del sistema de ecuaciones está incluido en el conjunto {Raíces de $q_1(x_1)$} $\times \cdots \times$ {Raíces de $q_n(x_n)$}.

26. Proposición: *Sean I, J dos ideales de $k[x_1,\dots,x_n]$. Consideremos en $k[t,x_1,\dots,x_n]$ el ideal $(tI + (1-t)J)$, que es el ideal generado por los elementos $ti + (1-t)j$, para todo $i \in I$ y $j \in J$. Entonces,*

$$I \cap J = (tI + (1-t)J) \cap k[x_1,\dots,x_n]$$

Demostración. Si $f \in I \cap J$, entonces $f = tf + (1-t)f \in (tI + (1-t)J)$. Recíprocamente, dado $g \in (tI + (1-t)J) \cap k[x_1,\dots,x_n] \subset k[t,x_1,\dots,x_n]$, si hacemos cociente por (t), tendremos que $g \in J$ y si hacemos cociente por $(1-t)$ tendremos que $g \in I$, luego $g \in I \cap J$. □

Como consecuencia de las dos proposiciones obtenemos el algoritmo para calcular la intersección de dos ideales de $R = k[x_1,\dots,x_n]$. Si $R' = R/(f_1,\dots,f_m)$, $\pi: R \to R'$ el morfismo de paso al cociente y $I = (\bar{g}_1,\dots,\bar{g}_r)$ y $J = (\bar{g}'_1,\dots,\bar{g}'_s)$ dos ideales de R', entonces

$$I \cap J = \pi(\pi^{-1}(I) \cap \pi^{-1}(J)) = \overline{(f_1,\dots,f_m,g_1,\dots,g_r) \cap (f_1,\dots,f_m,g'_1,\dots,g'_s)}.$$

Dado $\bar{a} \in R' = R/I'$, sabemos calcular $(I : \bar{a})$, porque por el problema 12 del capítulo 5,

$$(I : \bar{a}) = \frac{I \cap (\bar{a})}{\bar{a}} + (0 : \bar{a}) = \frac{I \cap (\bar{a})}{\bar{a}} + \overline{(I' : a)} = \frac{I \cap (\bar{a})}{\bar{a}} + \frac{\overline{I' \cap (a)}}{a}.$$

.

Proponemos que el lector generalice estas proposiciones para calcular la intersección de dos submódulos. Dado un morfismo de módulos $f : M \to M'$ y un submódulo $N' \subset M'$, sean $\tilde{M} = \{(m, f(m)) \in M \oplus M', \forall m \in M\}$ y $\tilde{N}' = M \oplus N' \subset M \oplus M'$, entonces

$$f^{-1}(N') = \tilde{M} \cap \tilde{N}',\ m \mapsto (m, f(m)).$$

27. Proposición: *Sea $I \subset R$ un ideal y $f \in R$ y $i : R \to R_f$ el morfismo de localización. Consideremos el ideal $(I + (1 - tf)) \subset R[t]$. Entonces,*

$$i^{-1}(I_f) = (I + (1 - tf)) \cap R.$$

Demostración. Sabemos que $R_f = R[t]/(1 - tf)$. Sea $\pi : R[t] \to R[t]/(1 - tf)$ el morfismo de paso al cociente. la composición $R \hookrightarrow R[t] \xrightarrow{\pi} R[t]/(1 - tf) = R_f$ es el morfismo de localización. Luego $i^{-1}(I_f) = \pi^{-1}(I_f) \cap R = (I + (1 - tf)) \cap R$.

□

28. Ejercicio: Sea $R' = R/J$, $\bar{I} \subset R'$ un ideal y $\bar{f} \in R'$. Denotemos $\bar{i} : R' \to R'_{\bar{f}}$ el morfismo de localización. Sigamos las notaciones de la proposición anterior. Prueba que

$$\bar{i}^{-1}(\bar{I}_{\bar{f}}) = \overline{(I + J + (1 - tf)) \cap R}.$$

Cierre proyectivo de una variedad afín

Dado $f \in k[x_1, \ldots, x_r]$, diremos que el polinomio homogéneo

$$F = x_0^{\operatorname{gr} f} \cdot f(x_1/x_0, \ldots, x_r/x_0) \in k[x_0, \ldots, x_r]$$

es la homogeneización de f por x_0. Si $G \in k[x_0, \ldots, x_r]$ es un polinomio homogéneo cuya deshomogeneización por x_0, $G/x_0^{\operatorname{gr} G}$, es igual a $f(x_1/x_0, \ldots, x_r/x_0)$, entonces $G = x_0^{\operatorname{gr}(G)} \cdot f(x_1/x_0, \ldots, x_r/x_0)$, luego $G = x_0^{\operatorname{gr} G - \operatorname{gr} F} \cdot F$.

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 $X = \operatorname{Spec} k[x_1, \ldots, x_r]/I$ se dice que $\operatorname{Proj} k[x_0, \ldots, x_r]/J$ es el cierre proyectivo de X.[1]

[1] No es un concepto intrínseco de X, depende del sistema de generadores algebraicos $\bar{x}_1, \ldots, \bar{x}_r$ escogido.

29. Proposición: *Consideremos en $k[x_1,\dots,x_r]$ el orden $>_{hlex}$. Sea $I \subseteq k[x_1,\dots,x_r]$ un ideal y $g_1,\dots,g_t$ una base de Gröbner de I. Entonces, la homogeneización de I por x_0 es el ideal homogéneo generado por las homogeneizaciones $G_1,\dots,G_t$ de $g_1,\dots,g_t$ por x_0.*

Demostración. Sea $x_{r+1} := x_0$ y consideremos el orden lexicográfico homogéneo en $k[x_1,\dots,x_{r+1}]$. Dado $f \in k[x_1,\dots,x_r]$ y su homogeneización F por x_{r+1}, es claro que $max(f) = max(F)$. Sea $J = (F)_{f\in I} \subseteq k[x_1,\dots,x_{r+1}]$. Por tanto,

$$max(J) = (max(I)) = (max(g_1),\dots,max(g_t)) = (max(G_1),\dots,max(G_t))$$

Luego la inclusión $(G_1,\dots,G_t) \subseteq J$ es epiyectiva. □

Polinomio 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:

$$H_S(n) := \dim_k S_n = \begin{array}{l}\text{La dimensión del subespacio vectorial de } S\\ \text{generado por las clases de los monomios de grado } n\end{array}$$

30. Proposición: *Consideremos en $k[x_1,\dots,x_r]$ un orden monomial 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 $[S]_{\le n} = \oplus_{m\le n}[S]_m$ el subespacio vectorial de S formado por las clases de los polinomios de grado menor o igual que n. Sea M el conjunto de los monomios de $k[x_1,\dots,x_r]$. La filtración $\{S_{\le x^\alpha} := \overline{k[x_1,\dots,x_r]_{\le x^\alpha}}\}_{x^\alpha\in M}$ refina a la filtración $\{[S]_{\le n}\}_{n\in\mathbb{N}}$ (si x^α es el mayor monomio de grado n, entonces $S_{\le x^\alpha} = [S]_{\le n}$). Por tanto,

$$\dim_k [S]_n = \dim_k([S]_{\le n}/[S]_{\le n-1}) = \sum_{|\alpha|=n} \dim_k G_{x^\alpha} S = \dim_k [GS]_n$$

□

Sea ahora $I = (m_1,\dots,m_t) \subseteq k[x_1,\dots,x_r]$ un ideal generado por monomios. Calculemos, por inducción sobre t, la función de Hilbert de R/I. Sean

$$I' := (m_2,\dots,m_t) \text{ e } I'' := (m_2/m.c.d.(m_2,m_1),\dots,m_t/m.c.d.(m_t,m_1))$$

Es fácil comprobar que la sucesión

$$0 \to R/I'' \xrightarrow{m_1\cdot} R/I' \to R/I \to 0$$

es exacta. Por inducción conocemos la función de Hilbert de R/I' y R/I'', luego la de R/I, pues por la sucesión exacta anterior

$$H_{R/I}(n) = H_{R/I'}(n) - H_{R/I''}(n-d),$$

siendo $d = \mathrm{gr}(m_1)$.

También por inducción obtenemos que $H_{R/I}(n)$ es un polinomio para $n \gg 0$, es decir, existe un polinomio (único) $h_{R/I}(x) \in \mathbb{Q}[x]$, tal que $H_{R/I}(n) = h_{R/I}(n)$, para todo $n \gg 0$. Solo necesitamos observar que

$$H_R(n) = \binom{n+r}{r} - \binom{n+r-1}{r} = \binom{n+r-1}{r-1},$$

que es un polinomio (en n) de grado $r-1 = \dim R - 1$. En efecto, escribamos $x_1^{m_1}\cdots x_r^{m_r}$ (con $m_1+\cdots+m_r = m \le n$) así: $y_1\cdots y_{m_1}x_1\cdots y_{m-m_r+1}\cdots y_m x_r \cdot y_{m+1}\cdots y_n$. Entonces, el número de monomios x^α de grado menor o igual que n, es igual, al número de estas escrituras, que es $\frac{(r+n)!}{r!n!}$.

Por la proposición 6.2.30, $H_{R/I}(x)$ es un polinomio para $n \gg 0$, para todo ideal homogéneo $I \subset R$, denominado polinomio de Hilbert de R/I y que denotamos $h_{R/I}(x)$. Si $h_{R/i}(x) = 0$, entonces $(R/I)_n = 0$, para todo $n \gg 0$, luego $\bar{x}_1,\ldots,\bar{x}_r$ son nilpotentes y el único ideal primo es el ideal irrelevante, y por tanto $\dim R = 0$. Si $h_{R/I}(x) \neq 0$, el coeficiente del término de grado máximo de $h_{R/I}(x)$ es positivo, ya que $\lim_{n\to\infty} h_{R/I}(n) > 0$. Observemos que $h_{R/I}(x) = h_{GR/I}(x)$.

31. Lema: *Sea $I \subset R$ un ideal generado por monomios. El grado de $h_{R/I}(x)$ es igual a $\dim R/I - 1$. Es decir,* $\mathrm{gr}(h_{R/I}(x)) = \dim \mathrm{Proj}\, R/I$.

Demostración. Escribamos $I = (m_1,\ldots,m_t)$, m_i monomios. Procedemos por inducción sobre $\mathrm{gr}(m_1)+\cdots+\mathrm{gr}(m_t)$. Si $I = 0$ sabemos que $\dim R = r = \mathrm{gr}\, h_R(x)+1$. Podemos suponer $I \neq 0$. Las componentes irreducibles de $\mathrm{Spec}\, R/I = (I)_0 = \cap (m_j)_0$ son intersección de hiperplanos $(x_i)_0$ y $(x_{i_1},\ldots,x_{i_r})_0$ es una componente si y solo si $m_j \in (x_{i_1},\ldots,x_{i_r})$, para todo j, y para un cierto j y cierto k $m_j \notin (x_{i_1},\ldots,\hat{x}_{i_k},\ldots,x_{i_r})$. Sea i tal que $(x_i)_0$ pasa por una de las componentes irreducibles de dimensión máxima. Algún m_j es múltiplo de x_i, porque en caso contrario $(m_1,\ldots,m_t) \subset (x_1,\ldots,\hat{x}_i,\ldots,x_n)$ y tomando ceros tendríamos que $((x_1,\ldots,\hat{x}_i,\ldots,x_n)_0 \subset (x_i)_0$, lo cual es falso. Además, $\dim R/(x_i,I) = \dim R/I =: n$. Sean $m'_k = \frac{m_k}{m.c.d.(x_i,m_k)}$, para todo k e $I' = (m'_1,\ldots,m'_t)$. Observemos que $I \subset I'$, luego $(I')_0 \subset (I)_0$ y $\dim R/I' \le \dim R/I = n$. La sucesión obvia

$$0 \longrightarrow R/I' \xrightarrow{x_i\cdot} R/I \longrightarrow R/(x_i,I) \longrightarrow 0$$

es exacta, luego $H_{R/I}(x) = H_{R/I'}(x) + H_{R/(x_i,I)}(x)$ y $h_{R/I}(x) = h_{R/I'}(x) + h_{R/(x_i,I)}(x)$. Por hipótesis de inducción, $\mathrm{gr}\, h_{R/I'}(x) = \dim R/I' - 1 \le n-1$ y $\mathrm{gr}\, h_{R/(x_i,I)}(x) = \dim R/(x_i,I) - 1 = n-1$, luego $h_{R/I}(x)$ es un polinomio de grado $n-1$.

□

32. Teorema: *Sea $I \subset R$ un ideal homogéneo. El grado de $h_{R/I}(x)$ es igual a* $\dim R/I - 1$. *Es decir,* $\operatorname{gr}(h_{R/I}(x)) = \dim \operatorname{Proj} R/I$.

Demostración. 1. $\dim R/I - 1 \leq \operatorname{gr} h_{R/I}(x)$: Procedemos por inducción sobre el grado. Si $\operatorname{gr} h_{R/I}(x) = -1$, es decir, $h_{R/I}(x) = 0$, y ya hemos probado que $\dim R/I = 0$. Supongamos, $\operatorname{gr} h_{R/I}(x) \geq 0$. Sea $\bar{z} \subset \operatorname{Spec} R/I$ una componente irreducible de dimensión $n = \dim R/I$. Basta probar que $\dim R/\mathfrak{p}_z - 1 \geq h_{R/\mathfrak{p}_z}(x)$, porque si es así entonces $\dim R/I - 1 = \dim R/\mathfrak{p}_z - 1 \leq h_{R/\mathfrak{p}_x}(x) \leq h_{R/I}(x)$. Sea $f_s \in (R/\mathfrak{p}_x)_s$ un elemento homogéneo no nulo, con $s > 0$. Consideremos la sucesión exacta

$$0 \longrightarrow R/\mathfrak{p}_z \xrightarrow{f_s \cdot} R/\mathfrak{p}_z \longrightarrow R/(f_s, \mathfrak{p}_z) \longrightarrow 0$$

Entonces, $h_{R/(f_s,\mathfrak{p}_z)}(n) = h_{R/\mathfrak{p}_z}(n) - h_{R/\mathfrak{p}_z}(n-s)$. Por tanto, por inducción

$$n - 1 = \dim R/(f_s, \mathfrak{p}_z) = \operatorname{gr} h_{R/(f_s,\mathfrak{p}_z)}(n) + 1 \leq \operatorname{gr} h_{R/\mathfrak{p}_z}(n)$$

y $n - 1 \leq \operatorname{gr} h_{R/\mathfrak{p}_z}(n)$.

2. $\dim R/I \geq \dim GR/I$: $GR/I = R/\operatorname{máx}(I)$ y sea $n = \dim R/\operatorname{máx}(I)$. Por el problema 21 del capítulo 3, existe un subconjunto $\{j_1, \ldots, j_n\} \subseteq \{1, \ldots, r\}$ tal que el morfismo $k[x_{j_1}, \ldots, x_{j_n}] \to R/\operatorname{máx}(I)$, $p(x_{j_1}, \ldots, x_{j_n}) \mapsto \overline{p(x_{j_1}, \ldots, x_{j_n})}$ es inyectivo. Por tanto, el morfismo $k[x_{j_1}, \ldots, x_{j_n}] \to R/I$, $p(x_{j_1}, \ldots, x_{j_n}) \mapsto \overline{p(x_{j_1}, \ldots, x_{j_n})}$ es inyectivo, porque lo es al tomar graduados. De nuevo, por el problema 21, $\dim R/I \geq n$.

3. Tenemos que $\dim R/I - 1 \overset{2.}{\geq} \dim GR/I - 1 \overset{6.2.31}{=} \operatorname{gr} h_{GR/I}(x) = \operatorname{gr} h_{R/I}(x)$. Por el apartado 1., $\dim R/I - 1 = \operatorname{gr} h_{R/I}(x)$.

□

33. Corolario: *Sea $X = \operatorname{Spec} k[x_1, \ldots, x_r]/I$ una variedad algebraica afín y*

$$H_X(n) := \dim_k \langle \overline{p(x_1, \ldots, x_r)} \in k[x_1, \ldots, x_r]/I : \operatorname{gr}(p(x_1, \ldots, x_r)) \leq n \rangle_k$$

Entonces,

1. *Si* $\operatorname{Proj} k[x_0, \ldots, x_r]/J$ *es el cierre proyectivo de X, $H_X(x) = H_{k[x_0,\ldots,x_r]/J}(x)$.*
2. *$H_X(x)$ es un polinomio de grado* $\dim X$, *para $n \gg 0$.*

Demostración. 1. La aplicación k-lineal

$$\begin{array}{rcl} [R/J]_n & \longrightarrow & \langle \overline{p(x_1, \ldots, x_r)} \in k[x_1, \ldots, x_r]/I : \operatorname{gr}(p(x_1, \ldots, x_r)) \leq n \rangle_k \\ \overline{p_n(x_0, \ldots, x_r)} & \longmapsto & \overline{p_n(1, x_1 \ldots, x_r)} \end{array}$$

es un isomorfismo, luego $H_X(x) = H_{k[x_0,\dots,x_r]/J}(x)$.

2. Por 1., para todo $n \gg 0$, $H_X(n) = h_{k[x_0,\dots,x_r]/J}(n)$, y sabemos que es un polinomio y $\operatorname{gr} h_{k[x_0,\dots,x_r]/J}(x) = \dim \operatorname{Proj} k[x_0,\dots,x_r]/J$. $\operatorname{Proj} k[x_0,\dots,x_r]/J$ es la mínima subvariedad proyectiva de $\mathbb{P}^r$ cuyo corte con $U^h_{x_0} \subset \mathbb{P}^r$ es igual a X. Por tanto, ninguna componente irreducible de $\operatorname{Proj} k[x_0,\dots,x_r]/J$ está incluida en $(x_0)^h_0$ y

$$\dim \operatorname{Proj} k[x_0,\dots,x_r]/J = \dim U^h_{x_0} \cap \operatorname{Proj} k[x_0,\dots,x_r]/J = \dim X.$$

□

Morfismo de explosión

34. Sea $A = k[x_1,\dots,x_r]/(p_1,\dots,p_r)$ e $I = (\xi_1,\dots,\xi_s)$ un ideal de A. Se define el dilatado de A por I, que denotamos $D_I A$, como sigue

$$D_I A := A \oplus I \oplus \cdots \oplus I^n \oplus \cdots = A[\xi_1 \cdot t, \dots, \xi_s \cdot t] \subseteq A[t]$$

Luego, $D_I A = k[\bar{x}_1,\dots,\bar{x}_r,\xi_1 \cdot t,\dots,\xi_s \cdot t] \subset A[t] = k[x_1,\dots,x_r,t]/(p_1,\dots,p_r)$, que sabemos calcular porque sabemos calcular las relaciones que cumplen $\bar{x}_1,\dots,\bar{x}_r,\xi_1 \cdot t,\dots,\xi_s \cdot t$.

Se dice que $\operatorname{Proj} D_I A$ es la explosión de $\operatorname{Spec} A$ a lo largo de $(I)_0$. Se cumple que

$$\operatorname{Proj} D_I A = \cup_i \operatorname{Spec} A[\xi_1/\xi_i,\dots,\xi_s/\xi_i].$$

Sabemos calcular $A[\xi_1/\xi_i,\dots,\xi_s/\xi_i] = k[\bar{x}_1,\dots,\bar{x}_r,\xi_1/\xi_i,\dots,\xi_s/\xi_i] \subseteq A_{\xi_i} = A[y]/(\xi_i \cdot y - 1)$, luego sabemos calcular la explosión de una variedad a lo largo de un cerrado.

Cálculo de la descomposición primaria de un ideal

35. Lema : *Supongamos por sencillez que k es un cuerpo de característica cero y A una k-álgebra finita. Sabemos calcular el radical de A. Si sabemos descomponer todo polinomio $p(x) \in k[x]$ como producto de polinomios irreducibles entonces sabemos descomponer A en producto directo de k-álgebras finitas locales y sabemos calcular la descomposición primaria del ideal* (0).

Demostración. El radical de $k[x]/(p(x))$ es $(\overline{\frac{p}{m.c.d.(p,p')}})$.

Si sabemos calcular el radical de una k-álgebra finita B, sabemos calcular el radical de B/I, porque $\operatorname{rad}(B/I) = \overline{\operatorname{rad} B}$, pues

$$(B/I)/\overline{\operatorname{rad} B} = B/(\operatorname{rad} B + I) = (B/\operatorname{rad} B)/\bar{I}$$

es reducido (todo cociente de la k-álgebra finita reducida $B/\operatorname{rad} B$ es reducido).

Si sabemos calcular el radical de B y C, sabemos calcular el radical de $B \otimes_k C$: $\operatorname{rad}(B \otimes_k C) = \operatorname{rad} B \otimes C + B \otimes \operatorname{rad} C$, porque

$$(B \otimes C)/(\operatorname{rad} B \otimes C + B \otimes \operatorname{rad} C) = (B/\operatorname{rad} B) \otimes (C/\operatorname{rad} C)$$

es reducido.

Toda k-álgebra finita es cociente de una k-álgebra $k[x_1,\dots,x_n]/(p_1(x_1),\dots,p_n(x_n))$. Por tanto, sabemos calcular el radical de toda k-álgebra finita.

Sea A una k-álgebra finita separable (de dimensión n). Todos los elementos de A son primitivos salvo los que pertenecen a un número (menor que $\binom{n}{2}$)) finito de hiperplanos: si $\bar{k}$ es el cierre algebraico de k, $\operatorname{Hom}_{k-alg}(A,\bar{k}) = \{\phi_1,\dots,\phi_n\}$, entonces si $a \notin \operatorname{Ker}(\phi_i - \phi_j)$ para todo $i \neq j$, entonces a es primitivo. Si $a \in A$ es primitivo, entonces tenemos isomorfismos explícitos $A = k[a] = k[x]/(p(x))$, donde $p(x)$ es el polinomio característico del endomorfismo $a\cdot\colon A \to A$, $b \mapsto ab$. Como sabemos descomponer $p(x)$ en producto de polinomios irreducibles sabemos descomponer A en producto directo de cuerpos.

Por último, sea A una k-álgebra finita. Tenemos $A/\operatorname{rad} A = K_1 \times \cdots \times K_r$. Tenemos que $A = \prod_i A_i$, con $A/\operatorname{rad} A_i = K_i$ y tenemos que calcular los k-álgebras finitas locales A_i. Sea $\pi\colon A \to A/\operatorname{rad} A$ el morfismo de paso al cociente. Sea $c_i \in A$ tal que $\pi(c_i) = (0,\dots,0,\underset{i}{1},0,\dots,0)$ (tendremos que $c_i = (c_{ij}) \in \prod_i A_i$, con $c_{ij} \in A_j$ nilpotente si $j \neq i$ y c_{ii} invertible). Sea $n_i > 0$ tal que $\operatorname{Ker} c_i^{n_i}\cdot = \operatorname{Ker} c_i^{n_i+1}\cdot$. Tendremos que $A_i = c_i^{n_i} \cdot A$ y la descomposición primaria del cero es $\cap_i(A_1 \times \cdots \times \underset{i}{0} \times \cdots \times A_n)$.

□

36. Lema : *Sea $I \subseteq k[x_1,\dots,x_n]$ un ideal y $S = k[x_i,\dots,x_n]\backslash\{0\}$ con $i > 1$. Sabemos calcular $I_S \cap k[x_1,\dots,x_n]$.*

Con mayor precisión, consideremos en el anillo $k[x_1,\dots,x_n]$ el orden lexicográfico y sea $\{g_1,\dots,g_s\}$ una base de Gröbner de I. Escribamos $g_i = \sum_{\alpha_i=\cdots=\alpha_n=0} a_\alpha x^\alpha$, con $a_\alpha \in k[x_i,\dots,x_n]$, sea α tal que $\operatorname{máx}(g_i) = \operatorname{máx}(a_\alpha)x^\alpha$ y definamos $a_i = a_\alpha$ y $a = \prod_{i=1}^s a_i$. Entonces, $I_S \cap k[x_1,\dots,x_n] = I_a \cap k[x_1,\dots,x_n]$.

Demostración. Escribamos $A = k[x_i,\dots,x_n]$ y $k[x_1,\dots,x_n] = A[x_1,\dots,x_{i-1}]$. Consideremos la siguiente filtración en $A[x_1,\dots,x_{i-1}]$ de susbespacios vectoriales de índices $\alpha = (\alpha_1,\cdots,\alpha_{i-1})$, $E_\alpha := \oplus_{\alpha' \leq \alpha} A \cdot x^{\alpha'}$. Denotemos con G' la graduación por esta filtración. Obviamente, $G'_\alpha A[x_1,\dots,x_{i-1}] = A \cdot x^\alpha$, luego $G'A[x_1,\dots,x_{i-1}] = A[x_1,\dots,x_{i-1}]$. Un refinamiento de esta filtración es la filtración dada por el orden lexicográfico de $k[x_1,\dots,x_n]$: tenemos $E_{\alpha'} \subset E_{(\alpha,\beta)} \subset E_\alpha$ si $\alpha' < \alpha$, y $E_\alpha = \cup_{\beta=(\beta_i,\dots,\beta_n)} E_{(\alpha,\beta)}$. Por tanto, $G_{(\alpha,\beta)}G'_\alpha k[x_1,\dots,x_n] = G_{(\alpha,\beta)}k[x_1,\dots,x_n]$.

Consideremos en I la filtración $I_a := E_a \cap I$. Sea $\tilde{g}_i := \frac{max(g_i)}{\text{máx}(a_i)} \in k[x_1,\dots,x_{i-1}]$. Veamos que $G'I = (a_1\tilde{g}_1,\dots,a_s\tilde{g}_s)$: Obviamente $(a_1\tilde{g}_1,\dots,a_s\tilde{g}_s) \subseteq G'I$. Ahora bien, $GG'I = GI = (\text{máx}(g_1),\dots,\text{máx}(g_s))$ y por otra parte

$$(\text{máx}(g_1),\dots,\text{máx}(g_s)) = (\text{máx}(a_1)\tilde{g}_1,\dots,\text{máx}(a_s)\tilde{g}_s) \subset G(a_1\tilde{g}_1,\dots,a_s\tilde{g}_s).$$

Por tanto, la inclusión $(a_1\tilde{g}_1,\dots,a_s\tilde{g}_s) \subseteq G'I$ es epiyectiva, es decir, una igualdad.

Por tanto, el conúcleo de la inclusión $G'I_a = (G'I)_a = (\tilde{g}_1,\dots,\tilde{g}_s) \subset A_a[x_1,\dots,x_{i-1}]$ es un A_a-módulo libre. Luego, el morfismo $a'\cdot\colon A_a[x_1,\dots,x_{i-1}]/I_a \to A_a[x_1,\dots,x_{i-1}]/I_a$, $\bar{b} \mapsto \overline{a'b}$ es inyectivo para todo $a' \in A$ no nulo, porque en los graduados es inyectivo. Luego, el morfismo $(k[x_1,\dots,x_n]/I)_a \to (k[x_1,\dots,x_n]/I)_S$ es inyectivo y

$$\begin{aligned} I_S \cap k[x_1,\dots,x_n] &= \text{Ker}[k[x_1,\dots,x_n] \to (k[x_1,\dots,x_n]/I)_S] \\ &= \text{Ker}[k[x_1,\dots,x_n] \to (k[x_1,\dots,x_n]/I)_a] = I_a \cap k[x_1,\dots,x_n]. \end{aligned}$$

□

37. Teorema: *Sea $I \subset K[x_1,\dots,x_n]$ un ideal, con $K = \mathbb{Q}(y_1,\dots,y_m)$. Sabemos calcular una descomposición primaria de I.*

Demostración. Procedemos por inducción sobre n. Supongamos $n = 1$. Podemos suponer $I \neq 0$. Sabemos calcular el máximo común divisor de dos polinomios luego sabemos escribir $I = (p)$. Sabemos factorizar todo polinomio en $K[x_1]$ en producto de irreducibles, luego sabemos calcular la descomposición primaria de I. Supongamos $n > 1$.

Si $I \cap K[x_i] = (p_i(x_i)) \neq 0$ para todo i, la K-álgebra $K[x_1,\dots,x_n]/I$ es un cociente de $K[x_1,\dots,x_n]/(p_1(x_1),\dots,p_n(x_n))$, luego es una K-álgebra finita, luego sabemos calcular la descomposición primaria del ideal (0) y concluimos.

Podemos suponer que $I \cap K[x_i] = 0$, para cierto i. Sea $S = K[x_i]\backslash\{0\}$. Observemos que $I_S \neq K[x_1,\dots,x_n]_S$. Sabemos calcular $s \in S$ tal que

$$I_S \cap K[x_1,\dots,x_n] = I_s \cap K[x_1,\dots,x_n] =: I'.$$

Por inducción sobre n, sabemos calcular una descomposición primaria de I_S, luego sabemos calcular una descomposición primaria de I'. Si $I = I'$, hemos terminado. Si $I \subsetneq I'$, sea m, tal que $I' = (I : s^m)$. Entonces, $I = I' \cap (I + (s^m))$. Como $I \subsetneq I + (s^m)$, por inducción noetheriana sabemos calcular una descomposición primaria de $I + (s^m)$, luego sabemos calcular una descomposición primaria de I.

□

La descomposición de un polinomio en producto de polinomios irreducibles es computacionalmente elaborado, pero imprescindible para el cálculo de descomposiciones primarias. Si queremos calcular el radical de un ideal $(p(x)) \subseteq k[x]$, no necesitamos calcular las raíces de $p(x)$, si no que solo tendremos que calcular $m.c.d.(p(x), p'(x))$.

38. Proposición : *Sabemos calcular el radical de todo ideal* $I \subset K[x_1,\dots,x_n]$ *con* $\operatorname{car} K = 0$.

Demostración. Procedemos por inducción sobre n. Supongamos $n = 1$. Sabemos calcular el máximo común divisor de dos polinomios luego sabemos escribir $I = (p)$. Entonces, $\operatorname{rad}(I) = (\frac{p}{m.c.d.(p,p')})$. Supongamos $n > 1$.

Si $I \cap K[x_i] = (p_i(x_i)) \neq 0$ para todo i, entonces $K[x_1,\dots,x_n]/I$ es un cociente de $K[x_1,\dots,x_n]/(p_1(x_1),\dots,p_n(x_n))$, luego sabemos calcular su radical, luego $\operatorname{rad} I$.

Podemos suponer que $I \cap K[x_i] = 0$, para cierto i. Sea $S = K[x_i]\backslash\{0\}$. Por inducción sobre n sabemos calcular $\operatorname{rad} I_S$ y sabemos calcular $(\operatorname{rad} I_S) \cap K[x_1,\dots,x_n] =: J$. Si $I = \cap_i \mathfrak{q}_i$ es una descomposición primaria reducida (de primos asociados $\mathfrak{p}_i := \operatorname{rad}(\mathfrak{q}_i)$), entonces $J = \cap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{p}_i$. Reordenando si es necesario, sean $\mathfrak{p}_1,\dots,\mathfrak{p}_m$ primos minimales de la descomposición, disjuntos con S, luego $J = \cap_{i=1}^{m} \mathfrak{p}_i$. Sea $I' = (I : J^r)$, para $r >> 0$. Observemos que $I' = \cap_{\mathfrak{p}_1,\dots,\mathfrak{p}_r \not\subseteq \mathfrak{p}_j} \mathfrak{q}_j$. $I \subsetneq I'$. Por inducción noetheriana sabemos calcular $\operatorname{rad} I'$ y concluimos porque $\operatorname{rad} I = J \cap \operatorname{rad} I'$.

□

6.3. Biografía de Buchberger

BUCHBERGER BIOGRAPHY

Bruno Buchberger (born 22 October 1942) is Professor of Computer Mathematics at Johannes Kepler University in Linz, Austria. In his 1965 Ph.D. thesis, he created the theory of Gröbner bases, and has developed this theory throughout his career. He named these objects after his advisor Wolfgang Gröbner.

Since 1995, he has been active in the Theorema project at the University of Linz. In 1987 Buchberger founded and chaired the Research Institute for Symbolic Computation (RISC) at Johannes Kepler University. In 1985 he started the Journal of Symbolic Computation, which has now become the premier publication in the field of computer algebra.

Buchberger also conceived Softwarepark Hagenberg in 1989 and since then has been directing the expansion of this Austrian technology park for software.

In 2014 he became a member of the Global Digital Mathematical Library Working Group of the International Mathematical Union.

[Tomado de la Wikipedia, 2025]

6.4. Cuestionario

1. Prueba que $R(P(x), x-\alpha) = (-1)^{\mathrm{gr}P(x)} \cdot P(\alpha)$.

2. Sean $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$ y $Q(x) = \sum_{i=0}^{m} b_i x^{m-i}$ dos polinomios genéricos. Prueba que $R(P(x), Q(x)) \in (a_n, b_m) \subset \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$.

3. Prueba que $>_{hlex}$ y $>_{ilex}$ son órdenes monomiales.

4. Escribe el término mayor de $2x+3y+z+x^2-z^2+x^3$, para cada uno de los órdenes monomiales $>_{lex}$, $>_{hlex}$, $>_{ilex}$.

5. Consideremos los órdenes monomiales $>_{lex}$, $>_{hlex}$, $>_{ilex}$ ¿Con cuál de ellos hemos ordenado los monomios (de mayor a menor) del polinomio $7x^2y^4z - 2xy^6 + x^2y^2$?¿Y del polinomio $xy^3z + xy^2z^2 + x^2z^3$?¿Y del polinomio $x^4y^5 + 2x^3y^2z - 4xy^2z^4$?

6. Consideremos un orden monomial en $R = k[x_1, \ldots, x_n]$. Dados $f, g \in R$, prueba que $\max(fg) = \max(f) \cdot \max(g)$ y $\max(f+g) \leq \max\{\max(f), \max(g)\}$ y si $\max(f) \neq -\max(g)$ entonces $\max(f+g) = \max\{\max(f), \max(g)\}$.

6.5. Problemas

1. Prueba que $R(P'(x), Q'(x)) = (-1)^{\mathrm{gr}(P)\cdot\mathrm{gr}(Q)} \cdot R(P(x), Q(x)) \cdot R(P(x), Q(-x))$, donde $P'(x^2) := P(x) \cdot P(-x)$ y $Q'(x^2) := Q(x) \cdot Q(-x)$.

2. Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calcula un polinomio de raíces $\alpha_i + \frac{1}{\alpha_i}$.

3. Calcula el polinomio cuyas raíces son

$$cos\,\frac{2k\pi}{5}, \qquad k = 0, 1, 2, 3, 4$$

4. Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calcula el polinomio de raíces $\alpha_i - \frac{1}{\alpha_i}$.

5. Generalización de 2 y 4: Calcula el polinomio de raíces $a\alpha_i + \frac{b}{\alpha_i}$, con $a, b \in k$.

6. 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). Calcula α, β.

7. Prueba que el discriminante de $x^2 + ax + b$ es $\Delta = a^2 - 4b$.

8. Prueba que el discriminante de $x^3 + px + q$ es $\Delta = -(4p^3 + 27q^2)$.

9. Consideremos n aplicaciones lineales $w_i : \mathbb{Q}^n \to \mathbb{Q}$ linealmente independientes, tales que $w_i = \sum_{j=1}^{n} a_{ij} x_j$ con $a_{ij} \geq 0$, para todo i, j. Prueba que el orden $<$ definido por: $x^\alpha < x^\beta$ si existe i tal que

$$w_1(\alpha) = w_1(\beta), \ldots, w_{i-1}(\alpha) = w_{i-1}(\beta) \text{ y } w_i(\alpha) < w_i(\beta),$$

es un orden monomial.

¿Qué orden monomial definen las aplicaciones lineales $x_1, \ldots, x_n$?¿Qué orden monomial definen las aplicaciones lineales $x_1 + \cdots + x_n, x_1, x_2, \ldots, x_{n-1}$?¿Qué orden monomial definen $x_1 + \cdots + x_n$, $x_1 + \cdots + x_{n-1}$,...,x_1?

10. Sea $\{g_1, \ldots, g_s\}$ una base de Gröbner de un R-módulo $M \subset L$. Se dice que es minimal si $\langle g_1, \ldots, \widehat{g_i}, \ldots, g_s \rangle \subsetneq M$, para todo i. Se dice que es reducida si ninguno de los términos de $g_i - \text{máx}(g_i)$ pertenece a máx(M), para todo i. Prueba

    a) Es minimal si y solo si $\{\text{máx}(g_1), \ldots, \text{máx}(g_s)\}$ es el sistema generador mínimo (único salvo multiplicación por constantes no nulas) de máx(M).

    b) Salvo multiplicación por constantes no nulas solo hay una base de Gröbner minimal y reducida en M.

11. Sea $\leq$ un orden monomial en L y $M \subset L$ un R-submódulo y $f \in L$.

    a) Prueba que f se puede escribir de la forma $f = g + r$, donde $g \in M$ y ningún término de r pertenece a máx$\, M$.

    b) Dadas dos expresiones $f = g + r = g' + r'$ verificando el apartado a), prueba que $g = g'$ y $r = r'$.

12. Calcula el número de puntos de corte, contando grados y multiplicidades, de las dos curvas planas afines $y^3 + xy + x^3 = 0$ y $y^2 x + 2xy + 3 = 0$.

13. Sean $I = (x^2 y)$ y $J = (xy^2)$ dos ideales de $k[x, y]$. Calcula $I \cap J$.

14. Calcula el polinomio de Hilbert de la variedad afín $(x^3 y - z^4, x^2 - y^3)_0 \subset \mathbb{A}^3$.

Solución de los problemas del curso

Solución de los problemas del capítulo cero

P1. Sea $f:\mathbb{Z}\to\mathbb{Z}$ un morfismo de anillos. Tenemos que $f(1)=1$, luego $f(2)=f(1+1)=f(1)+f(1)=1+1=:2$,..., $f(n)=n$, para todo $n\in\mathbb{N}$ y por tanto $f(-n)=-n$ para todo $n\in\mathbb{N}$. Es decir, $f=\mathrm{Id}$.

Sea $f:\mathbb{Q}\to\mathbb{Q}$ un morfismo de anillos. $f_{|\mathbb{Z}}=\mathrm{Id}_{|\mathbb{Z}}$. Entonces, $f(\frac{n}{m})=f(n\cdot m^{-1})=n\cdot m^{-1}=\frac{n}{m}$ y $f=\mathrm{Id}$.

Sea $f:\mathbb{R}\to\mathbb{R}$ un morfismo de anillos. De nuevo, $f_{|\mathbb{Q}}=\mathrm{Id}_{|\mathbb{Q}}$. Dado $r>0$, tenemos que $r=s^2$, para un $s>0$. Entonces, $f(r)=f(s)^2>0$. Si $r>s$ entonces $r-s>0$, luego $f(r)-f(s)=f(r-s)>0$ y $f(r)>f(s)$. Dado $r\in\mathbb{R}$, sean $q_1,q_2\in\mathbb{Q}$ tales que $q_1<r<q_2$, entonces $q_1=f(q_1)<f(r)<f(q_2)=q_2$. Por tanto, $f(r)=r$ y $f=\mathrm{Id}$.

P2. Observemos que dado $p(x)\in A[x]$ existen un polinomio único $q(x)\in A[x]$ y $b\in A$ tales que $p(x)=q(x)\cdot(x-a)+b$. Por tanto, $p(a)=0$ si y solo si $b=0$, es decir, $p(x)\in(x-a)$. Consideremos el epimorfismo $\pi:A[x]\to A$, $\pi(p(x)):=p(a)$. Tenemos que $\mathrm{Ker}\,\pi=(x-a)$, luego por el teorema de isomorfía, $A[x]/(x-a)\simeq A$.

P3. Por el teorema chino de los restos

$$\begin{aligned}\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) &= \mathbb{R}[x]/(x^2+1)\times\mathbb{R}[x]/(x^2-1)\\ &= \mathbb{R}[x]/(x^2+1)\times\mathbb{R}[x]/(x-1)\times\mathbb{R}[x]/(x+1)=\mathbb{C}\times\mathbb{R}\times\mathbb{R}.\end{aligned}$$

P4. a) Calculemos $t(x)=\sum_i^n b_i x^i$, tal que $1=s(x)\cdot b(x)=\sum_i^{n=0}\sum_{i+j=n} a_i b_j x^n$. Luego, $b_0=a_0^{-1}$ (luego a_0 ha de ser invertible. Además, $0=\sum_{i+j=n} a_i b_j$, para $n>0$,es decir, $b_n=-\frac{a_0}{\sum_{j=0}^{n-1} a_{n-j}b_j}$ y argumentando por recurrencia fácilmente concluimos.

b) El morfismo es claramente epiyectivo e inyectivo.

P5. Sabemos que $I \times J$ es un subgrupo de $A \times B$, con la operación $+$. Dado $(i,j) \in I \times J$ y $(a,b) \in A \times B$, entonces $(a,b)\cdot(i,j) = (ai, bj) \in I \times J$. El núcleo del epimorfismo $A \times B \to A/I \times B/J$, $(a,b) \mapsto (\bar{a}, \bar{b})$ es $I \times J$. Luego, $(A \times B)/I \times J = A/I \times B/J$.

P6. Si existe un morfismo g, éste ha de cumplir que $g(\frac{a}{s}) = g(\frac{a}{1}) \cdot g(\frac{1}{s}) = f(a) \cdot g(\frac{s}{1}^{-1}) = f(a) \cdot f(s)^{-1}$ (luego $f(s)$ es invertible para todo $s \in S$) y el morfismo así definido (cuando $f(s)$ es invertible para todo $s \in S$) está bien definido y cumple lo requerido.

P7. Los morfismos $A_{SS'} \to (A_S)_{S'}$, $\frac{a}{ss'} \mapsto \frac{\frac{a}{s}}{s'}$ y $(A_S)_{S'} \to A_{SS'}$, $\frac{\frac{a}{s}}{s'} \mapsto \frac{a}{ss'}$ están bien definido y son inversos entre sí.

P8. $(M/IM)_S = M \otimes_A A/I \otimes_A A_S = M \otimes_A A_S \otimes_A A/I = M_S/I \cdot M_S$.

P9. Si $M = M_S$, $s\cdot$ es isomorfismo porque lo es en $M_S = M \otimes_A A_S$, ya que lo es en A_S. Recíprocamente, veamos que el morfismo de localización $M \to M_S$ es isomorfismo. Es epiyectivo: dado $\frac{m}{s}$, sea $m' \in M$ tal que $s \cdot m' = m$, entonces $m' \mapsto \frac{m'}{1} = \frac{m}{s}$. Es inyectivo: si $\frac{m}{1} = 0$, entonces existe $s \in S$ tal que $s \cdot m = 0$, luego $m = 0$.

P10. Dado un conjunto de A-módulos $\{M_j\}_{j\in J}$ y de submódulos $\{N_j \subseteq M_j\}_{j\in J}$, tenemos el submódulo $\oplus_{j\in J} N_j \subseteq \oplus_{j\in J} M_j$, $(n_j)_{j\in J} \mapsto (n_j)_{j\in J}$. Además, $(\oplus_{j\in J} M_j)/\oplus_{j\in J} N_j = \oplus_{j\in J} M_j/N_j$, $\overline{(m_j)_{j\in J}} \mapsto (\bar{m}_j)_{j\in J}$.

Dado un conjunto I y un A-módulo M denotemos $M^{(I)} = \oplus_I M$. Dado un morfismo de módulos $f : M \to N$, sea $f^{(I)} : M^{(I)} \to M'^{(I)}$, $f^{(I)}((m_i)_{i\in I}) = (f(m_i))_{i\in I}$. Se cumple que $\operatorname{Ker} f^{(I)} = (\operatorname{Ker} f)^{(I)}$, $\operatorname{Im} f^{(I)} = (\operatorname{Im} f)^{(I)}$ y $\operatorname{Coker} f^{(I)} = (\operatorname{Coker} f)^{(I)}$.

El problema es consecuencia de que si $N = \oplus_I A$, entonces $M \otimes_A N = M^{(I)}$ y dado un morfismo $f : M \to M'$, entonces $f \otimes \mathrm{Id} : M \otimes N \to M' \otimes N$ se identifica con $f^{(I)}$.

P11. El morfismo $g \otimes \mathrm{Id}$ es epiyectivo: Sea $m_3 \otimes n \in M_3 \otimes N$. Sea $m_2 \in M_2$ tal que $g(m_2) = m_3$. Entonces, $(g \otimes \mathrm{Id})(m_2 \otimes n) = m_3 \otimes n$.

$\operatorname{Im}(f \otimes \mathrm{Id}) \subseteq \operatorname{Ker}(g \otimes \mathrm{Id})$: $(g \otimes \mathrm{Id}) \circ (f \otimes \mathrm{Id}) = (g \circ f) \otimes \mathrm{Id} = 0 \otimes \mathrm{Id} = 0$.

Tenemos pues un epimorfismo

$$\overline{g \otimes \mathrm{Id}} : (M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id}) \to M_3 \otimes N,\ \overline{g \otimes \mathrm{Id}}(\overline{m_2 \otimes n}) = (g \otimes \mathrm{Id})(m_2 \otimes n) = g(m_2) \otimes n.$$

Veamos que es un isomorfismo: Sea $s : M_3 \otimes N \to (M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id})$, definido por $s(m_3 \otimes n) = \overline{m_2 \otimes n}$, donde m_2 es cualquier elemento de M_2 tal que $g(m_2) = m_3$ (si $g(m_2') = m_3$, entonces $m_2 = m_2' + m'$, con $m' \in \operatorname{Ker} g = \operatorname{Im} f$, luego $\overline{m_2 \otimes n} = \overline{m_2' \otimes n} + \overline{m' \otimes n} = \overline{m_2' \otimes n}$). Es claro que $s \circ \overline{g \otimes \mathrm{Id}} = \mathrm{Id}$ y que $\overline{g \otimes \mathrm{Id}} \circ s = \mathrm{Id}$.

En conclusión, $(M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id}) = M_3 \otimes N$ y $\operatorname{Im}(f \otimes \mathrm{Id}) = \operatorname{Ker}(g \otimes \mathrm{Id})$.

P12. Si tensamos la sucesión exacta

$$0 \to E' \to E \to E/E' \to 0$$

por $\otimes_k V$, obtenemos la sucesión exacta

$$0 \to E' \otimes_k V \to E \otimes_k V \to (E/E') \otimes_k V \to 0$$

Luego, $(E/E') \otimes_k V = (E \otimes_k V)/(E' \otimes_k V)$.

P13. Si tensamos las sucesiones exactas

$$0 \to \operatorname{Ker} f \to E' \to \operatorname{Im} f \to 0, \quad 0 \to \operatorname{Im} f \to E$$

por $\otimes_k V$, obtenemos las sucesiones exactas

$$0 \to (\operatorname{Ker} f) \otimes_k V \to E' \otimes_k V \to (\operatorname{Im} f) \otimes_k V \to 0, \quad 0 \to (\operatorname{Im} f) \otimes_k V \to E \otimes_k V$$

De las que se deduce que $(\operatorname{Im} f) \otimes_k V = \operatorname{Im}(f \otimes \operatorname{Id})$ y que $(\operatorname{Ker} f) \otimes_k V = \operatorname{Ker}(f \otimes \operatorname{Id})$.

P14. Si N y $N' \subseteq M$ son dos A-submódulos y denotamos $\bar{N} = \{\bar{n} \in M/N', \forall n \in N\}$, entonces $(M/N')/\bar{N} = M/(N+N')$. En efecto, el núcleo del epimorfismo $M/N' \to M/(N+N')$, $\bar{m} \mapsto \bar{m}$, es $\bar{N}$, porque si $\bar{m} = 0$ en $M/(N+N')$, entonces $m \in N+N'$, luego existen $n \in N$ y $n' \in N'$ tales que $m = n+n'$ y $\bar{m} = \overline{n+n'} = \bar{n}$ en M/N'. Por tanto, $(M/N')/\bar{N} = M/(N+N')$. Luego, $A/I \otimes_A A/J = (A/I)/J \cdot (A/I) = (A/I)/\bar{J} = A/(I+J)$

Demos otra demostración. Los morfismos $A/I \otimes_A A/J \to A/(I+J)$, $\bar{a} \otimes \bar{b} \mapsto \overline{ab}$ y $A/(I+J) \to A/I \otimes_A A/J$, $\bar{a} \mapsto \bar{a} \otimes 1$, están bien definidos y son inversos entre sí.

P15. Por el teorema chino de los restos $A/(IJ) = A/I \times A/J$. Por tanto,

$$\begin{aligned} M/IJM &= M \otimes_A (A/(IJ)) = M \otimes_A (A/I \times A/J) = (M \otimes_A A/I) \oplus (M \otimes_A A/J) \\ &= M/IM \oplus M/JM \end{aligned}$$

P16. $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(n\mathbb{Z} + m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$.

P17. Es consecuencia inmediata del ejemplo 0.5.11.

P18. Las coordenadas del vector $e \otimes 1$ en la base $\{e_i \otimes 1\}_{1 \le i \le n}$ son $(x_1, \dots, x_n)$. En efecto, $e \otimes 1 = (\sum_i x_i e_i) \otimes 1 = \sum_i x_i \cdot (e_i \otimes 1)$.

P19. El morfismo $A[x_1, \dots, x_n] \otimes_A B \to B[x_1, \dots, x_n]$, $p(x) \otimes b \mapsto b \cdot p(x)$ y el morfismo $B[x_1, \dots, x_n] \to A[x_1, \dots, x_n] \otimes_A B$, $\sum_\alpha b_\alpha \otimes x^\alpha \mapsto \sum_\alpha x^\alpha \otimes b_\alpha$ son inversos entre sí.

P20. Denotemos $R = A[x_1,\dots,x_n]$. Entonces,

$$\begin{aligned} R/(p_1,\dots,p_r)\otimes_A B &= (R/(p_1,\dots,p_r)\otimes_R R)\otimes_A B \\ &= R/(p_1,\dots,p_r)\otimes_R B[x_1,\dots,x_n] \\ &= B[x_1,\dots,x_n]/(p_1,\dots,p_r)\cdot B[x_1,\dots,x_n] \\ &= B[x_1,\dots,x_n]/(p_1,\dots,p_r) \end{aligned}$$

P21. El morfismo $M\otimes_A N \to M\otimes_B N$, $m\otimes n \mapsto m\otimes n$ se anula en R, luego tenemos el morfismo $(M\otimes_A N)/R \to M\otimes_B N$, $\overline{m\otimes n}\mapsto m\otimes n$. El morfismo inverso es el morfismo $M\otimes_B N \to (M\otimes_A N)/R$, $m\otimes n\mapsto \overline{m\otimes n}$.

P22. Sea $I\colon E^*\otimes F \to \mathrm{Hom}_k(E,F)$, el morfismo definido por $I(w\otimes f)(e) := w(e)\cdot f$, para todo $e\in E$ (y todo $w\in E^*$ y $f\in F$). Sea $\{e_i\}_{i\in I}$ una base de E, $\{w_i\}_{i\in I}$ la base dual de E^* y sea $\{f_j\}$ una base de F. Entonces, $\{w_i\otimes f_j\}_{(i,j)\in I\times J}$ es una base de $E^*\otimes F$. Se tiene que $I(w_i\otimes f_j)(e_k)=0$, para $k\neq i$ y $I(w_i\otimes f_j)(e_i)=f_j$, para $k=i$; es decir, $\{I(w_i\otimes f_j)\}_{(i,j)\in I\times J}$ es la base estándar de $\mathrm{Hom}_k(E,F)$ (fijadas las bases de E y F). Por tanto, I es un isomorfismo.

Solución de los problemas del capítulo primero

P1. La primera afirmación ha sido probada en la demostración de la proposición 0.2.37.

Dado $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n$ sea $|\alpha|=\alpha_1+\cdots+\alpha_n$ y dado $p(x)=\sum_\alpha \lambda_\alpha x^\alpha \in k[x_1,\dots,x_n]$ sea $\mathrm{gr}(p(x)) = \max\{|\alpha| : \lambda_\alpha\neq 0\}$. Toda cadena ascendente de ideales $(p_1(x))\subset (p_2(x))\subset\cdots\subset(p_n(x))\subset\cdots$ estabiliza porque $\mathrm{gr}(p_1(x))\geq\mathrm{gr}(p_2(x))\geq\cdots\geq\mathrm{gr}(p_n(x))$ y $\mathrm{gr}(p_i(x)) = \mathrm{gr}(p_{i+1}(x))$ si y solo si $(p_i(x)) = (p_{i+1}(x))$. Para $s(x)=\sum_\alpha\lambda_\alpha x^\alpha \in k[[x_1,\dots,x_n]]$ define $\mathrm{gr}(s(x)) = \min\{|\alpha|\colon \lambda_\alpha\neq 0\}$ y demuestra que toda cadena ascendente de ideales $(s_1(x))\subset(s_2(x))\subset\cdots\subset(s_n(x))\subset\cdots$ de $k[[x_1,\dots,x_n]]$ estabiliza.

P2. Dado $p(x)\in k[x_1,\dots,x_n,\dots] =: A$ sea $n\in\mathbb{N}$, tal que $p(x)\in k[x_1,\dots,x_n]=B$. Si $p(x)$ es reducible en A, entonces es reducible en B (al lector). Por el lema de Gauss, B es DFU, luego A también. A no es noetheriano, porque el ideal $(x_1,\dots,x_n,\dots)$ no es finito generado, como el lector puede comprobar.

P3. Supongamos $\mathrm{Ker}\, f\neq 0$. Entonces $\mathrm{Ker}\, f \underset{\neq}{\subset} \mathrm{Ker}\, f^2$: sea $m\in\mathrm{Ker}\, f$ no nulo y $m'\in M$, tal que $f(m')=m$, entonces $m'\in\mathrm{Ker}\, f^2$ y $m'\notin\mathrm{Ker}\, f$. Igualmente, $\mathrm{Ker}\, f^2 \underset{\neq}{\subset} \mathrm{Ker}\, f^4$ y tenemos la cadena de inclusiones estrictas

$$\mathrm{Ker}\, f \underset{\neq}{\subset} \mathrm{Ker}\, f^2 \underset{\neq}{\subset}\cdots\underset{\neq}{\subset}\mathrm{Ker}\, f^{2^n}\underset{\neq}{\subset}\cdots$$

Lo cual contradice la noetherianidad de M.

P4. La aplicación $(a_1,\ldots,a_n,\ldots)\mapsto(a_2,\ldots,a_n,\ldots)$.

P5. Si $N+N_0$ es noetheriano, entonces los submódulos suyos N, N_0 son noetherianos. Si N y N_0 son noetherianos entonces $N\oplus N_0$ es noetheriano y como el morfismo $N\oplus N_0\to N+N_0$, $(n.n_0)\mapsto n+n_0$ es epiyectivo, entonces $N+N-0$ es noetheriano.

P6. Si M es noetheriano, entonces los cocientes M/N y M/N_0 son noetherianos. Si M/N y M/N_0, entonces M es noetheriano porque el morfismo $M\to M/N\oplus M/N_0$, $m\mapsto(\bar{m},\bar{m})$ es inyectivo

P7. a) A/I es un A-módulo noetheriano, luego es un A/I-módulo noetheriano, y por tanto A/I es un anillo noetheriano.

b) Sea $i\colon A\to A_S$ el morfismo de localización. Para todo ideal $J\subset A_S$ se cumple que $J=i^{-1}(J)_S$. Por tanto, como $i^{-1}(J)$ es un ideal finito generado de A, J es un ideal finito generado de A_S.

P8. Escribamos $N=\langle n_1,\ldots,n_r\rangle$. El morfismo de A-módulos

$$\mathrm{Hom}_A(N,M)\to M\oplus\overset{r}{\cdots}\oplus M,\ f\mapsto(f(n_1),\ldots,f(n_r))$$

es inyectivo. Como M es noetheriano entonces $M\oplus\overset{r}{\cdots}\oplus M$ es notehriano, luego $\mathrm{Hom}_A(N,M)$ es noetheriano.

P9. Escribamos $M=\langle m_1,\ldots,m_r\rangle$. El morfismo de A-módulos

$$A/\mathrm{Anul}(M)\to M\oplus\overset{r}{\cdots}\oplus M,\ \bar{a}\mapsto(am_1,\ldots,am_r)$$

es inyectivo. Luego, $A/\mathrm{Anul}(M)$ es un A-módulo notheriano, luego $A/\mathrm{Anul}(M)$ es un $A/\mathrm{Anul}(M)$-módulo noetheriano, es decir, $A/\mathrm{Anul}(M)$ es un anillo noetheriano.

P10. Escribamos $M=\langle m_1,\ldots,m_n\rangle$ y consideremos el epimorfismo $\pi\colon A^n\to M$, $\pi((a_i))=\sum_i a_i m_i$. . Tenemos que $N\oplus\overset{n}{\cdots}\oplus N=N\otimes_A A^n$ es noetheriano y el morfismo $N\otimes_A A^n\to N\otimes_A M$, $n\otimes(a_i)\mapsto n\otimes\pi((a_i))$ es epiyectivo, luego $N\otimes_A M$ es noetheriano.

P11. Sea $I_n=\{(a_1,\ldots,a_n,0,\ldots,0,\ldots)\subset\overset{\mathbb{N}}{\prod}\mathbb{Z}\colon\forall\, a_1,\ldots,a_n\in\mathbb{Z}\}$. Tenemos la cadenas de inlcusiones estrictas de ideales

$$I_1\underset{\neq}{\subset}I_2\underset{\neq}{\subset}\cdots\underset{\neq}{\subset}I_n\underset{\neq}{\subset}\cdots$$

que muestra que $\overset{\mathbb{N}}{\prod}\mathbb{Z}$ no es un anillo noetheriano.

P12. Supongamos que $I = (f_1, \ldots, f_n)$. Sea V_i el conjunto de puntos donde se anula f_i y B una bola centrada en 0, tal que $B \subset \cap_i V_i$. Entonces, toda $f \in I$ se anula en B, lo cual es falso. Por lo tanto, I no es finito generado.

P13. Supongamos que $\xi_1, \ldots, \xi_n, \alpha$ no son k-algebraicamente independientes. Entonces existe un polinomio $p(x_1, \ldots, x_n, y)$ no nulo con coeficientes en k, tal que $p(\xi_1, \ldots, \xi_n, \alpha) = 0$. Con las notaciones obvias escribamos $p(x_1, \ldots, x_n, y) = p(x, y) = \sum_n p_n(x) \cdot y^n$ (algún $p_n(x)$ es no nulo). Entonces, $p(\xi, y) \in k(\xi_1, \ldots, \xi_n)[y]$ es no nulo (porque algún $p_n(\xi) \neq 0$) y cumple que $p(\xi, \alpha) = 0$, luego α es $k(\xi_1, \ldots, \xi_n)$-algebraico.

Supongamos que α es $k(\xi_1, \ldots, \xi_n)$-algebraico, entonces existe un polinomio $p(y) \in k(\xi_1, \ldots, \xi_n)[y]$ no nulo tal que $p(\alpha) = 0$. Con las notaciones obvias escribamos $p(y) = \sum_n \frac{p_n(\xi)}{q_n(\xi)} y^n$. Observemos que $q(y) := \prod_n q_n(\xi) \cdot p(y) \in k[\xi_1, \ldots, \xi_n][y]$. Entonces, $\xi_1, \ldots, \xi_n, \alpha$ no son k-algebraicamente independientes porque $q(\alpha) = 0$.

P14. Sea $\xi_1, \ldots, \xi_n \in K$ una base de k-trascendencia de K y $\eta_1, \ldots, \eta_m$ una base de K-trascendencia de Σ. Veamos que $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m$ es una base de k-trascendencia de Σ.

Son k-algebraicamente independientes: Sea $p(x_1, \ldots, x_n, y_1, \ldots, y_m)$ un polinomio con coeficientes en k tal que $p(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m) = 0$. Escribamos, con las notaciones evidentes, $p(x_1, \ldots, x_n, y_1, \ldots, y_m) = p(x, y) = \sum_\gamma p_\gamma(x) \cdot y^\gamma$ (donde los $p_\gamma(x) \in k[x]$) Entonces, $p(\xi, y) = \sum_\gamma p_\gamma(\xi) \cdot y^\gamma \in K[y]$, cumple que $p(\xi, \eta) = 0$, luego $p_\gamma(\xi) = 0$, para todo γ, porque las η son K-algebraicamente independientes, entonces $p_\gamma(x) = 0$, porque las ξ son k-algebraicamente independientes. Luego, $p(x, y) = 0$ y $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m$ son algebraicamente independientes.

El morfismo $k(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m) \hookrightarrow \Sigma$ es algebraico, porque es composición de los morfismos algebraicos $k(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m) \hookrightarrow K(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m) \hookrightarrow \Sigma$.

En conclusión,

$$\operatorname{gr\,tr}_k \Sigma = n + m = \operatorname{gr\,tr}_k K + \operatorname{gr\,tr}_K \Sigma.$$

P15. $\operatorname{gr\,tr}_{\mathbb{R}} \mathbb{C}(x, y) = \operatorname{gr\,tr}_{\mathbb{R}} \mathbb{C} + \operatorname{gr\,tr}_{\mathbb{C}} \mathbb{C}(x, y) = 0 + 2 = 2$.

P16. Sea $\xi_1, \ldots, \xi_n \in \Sigma$ k-algebraicamente independientes. Sea $\eta_1, \ldots, \eta_m \in \Sigma$ una base de $k(\xi_1, \ldots, \xi_n)$-trasecendencia de Σ. En el problema 14 hemos probado que $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m$ es una base de k-trascendencia de Σ.

P17. Sea $\sum_{i=1}^{m} a_i \otimes b_i \in K \otimes_k K'$ nilpotente. Sea $\Sigma = k(a_1, \ldots, a_m)$. Como el morfismo de anillos $\Sigma \otimes_k K' \hookrightarrow K \otimes_k K'$ es inyectivo, basta que probemos que $\Sigma \otimes_k K'$ es reducido. Sea $x_1, \ldots, x_n \in \Sigma$ una base de trascendencia. Observemos que $k(x_1, \ldots, x_n) \otimes_k K'$

es una localización del anillo íntegro $k[x_1,\dots,x_n]\otimes_k K' = K'[x_1,\dots,x_n]$, luego está incluido en $K'(x_1,\dots,x_n)$. Entonces,

$$\Sigma\otimes_k K' = \Sigma\otimes_{k(x_1,\dots,x_n)} k(x_1,\dots,x_n)\otimes_k K' \hookrightarrow \Sigma\otimes_{k(x_1,\dots,x_n)} K'(x_1,\dots,x_n)$$

que es reducido porque Σ es una $k(x_1,\dots,x_n)$-extensión finita separable.

Solución de los problemas del capítulo segundo

P1. La recta que pasa por $p=(\alpha,\beta)$ y $(2,2)$, es $\frac{x-2}{\alpha-2}=\frac{y-2}{\beta-2}$ y corta a $y=0$ en el punto $((\alpha-2)\cdot\frac{-2}{\beta-2}+2,0)$, luego definimos $f(x)=(x-2)\cdot\frac{-2}{y-2}+2$.

P2. Si $J\subset A$ es un ideal y $\bar{J}=\{\bar{j}\in A/I,\,\forall\, j\in J\}$, entonces $(A/I)/\bar{J}=A/(I+J)$. Por tanto, si $\mathfrak{m}\subset A$ es un ideal de A que contiene a I, entonces $(A/I)/\bar{m}=A/I+\mathfrak{m}=A/\mathfrak{m}$. Si en la biyección $\operatorname{Spec}A/I=(I)_0$ nos quedamos con los ideales racionales, obtenemos la igualdad requerida.

P3. $\mathbb{R}[x,y,z]/((x,y,z)\cap(x,y,z-2)\cap(x,x^2+y^2+z^2-1))$.

P4. Dado un ideal primo $\mathfrak{p}_z$ de una k-álgebra B, denotemos $k(z)=(B/\mathfrak{p}_z)_z$. Si $S\subset B$ es un sistema multiplicativo, $\mathfrak{p}_z\cap S=\emptyset$ y denotamos $\mathfrak{p}_{\tilde{z}}=\mathfrak{p}_z\cdot B_S$, entonces

$$k(\tilde{z})=(B_s/\mathfrak{p}_z\cdot B_S)_{\tilde{z}}=(B_z/\mathfrak{p}_z\cdot B_z)_{\tilde{z}}=k(z).$$

Observemos además que $\mathfrak{p}_z\subset B$ es racional si y solo si $k(z)=k$. Ahora ya, el problema es consecuencia de que $\operatorname{Spec}A_S=\{z\in\operatorname{Spec}A:\ s(z)\neq 0.\,\forall\, s\in S\}$.

P5. a) Por el ejemplo 2,2,13 sabemos que la aplicación es biyectiva. Dado un ideal $I\subset C(X)$ se cumple que $I\subseteq\mathfrak{m}_p$ si y solo si todas las funciones $f\in I$ se anulan en p. $(I)_0\cap\operatorname{Spec}_{max}C(X)$ se corresponde con los puntos de X donde se anulan todas las funciones $f\in I$, que es un cerrado. Por tanto la aplicación es continua. Si C es un cerrado de X y $p\notin C$, entonces existe una función continua f tal que $f_{|C}=0$ y $f(p)\neq 0$. Si $I_C=\{f\in C(X)\colon f_{|C}=0\}$, entonces C se corresponde vía la aplicación con $(I_C)_0\cap\operatorname{Spec}_{max}C(X)$. Luego la aplicación es un homeomorfismo.

b) Cada morfismo de $\mathbb{R}$-álgebras $h\colon C(Y)\to C(X)$, induce el morfismo natural $X=\operatorname{Spec}_{rac}C(X)\xrightarrow{h^*}\operatorname{Spec}_{rac}C(Y)=Y$. La asignación $h\mapsto h^*$ es la asignación inversa de la dada.

c) El morfismo de $\mathbb{R}$-álgebras $C(X)\to C(Y)$, $f\mapsto f_{|Y}$ es epiyectivo por el teorema de extensión de Tietze y su núcleo es I. Por tanto,

$$\operatorname{Spec}_{max}C(X)/I=\operatorname{Spec}_{max}C(Y)=Y.$$

P6. Por el teorema de Hadamard, $\mathfrak{m}_p = (x_1 - p_1, \ldots, x_n - p_n)$ (donde $p = (p_1, \ldots, p_n)$). Si $\mathfrak{m} \subset \mathscr{C}^\infty(\mathbb{R}^n)$ es un ideal racional, sea $p_i = \bar{x}_i \in \mathscr{C}^\infty(\mathbb{R}^n)/\mathfrak{m} = \mathbb{R}$. Entonces, $\mathfrak{m}_p \subseteq \mathfrak{m}$, luego son iguales. Por tanto, ϕ es biyectiva. Dado un ideal $I \subset \mathscr{C}^\infty(\mathbb{R}^n)$, $\phi^{-1}((I)_0^{rac}) = \{p \in \mathbb{R}^n : f(p) = 0, \forall f \in I\}$ que es un cerrado, luego ϕ es continua. Dado un cerrado $C \subset \mathbb{R}^n$ y $p \notin C$, existe una función machacona f tal que $f(p) = 1$ y $f_{|C} = 0$. Por tanto, si $I_C = \{f \in \mathscr{C}^\infty(\mathbb{R}^n) : f_{|C} = 0\}$, entonces $\phi(C) = (I_C)_0^{rac}$ y ϕ es un homeomorfismo.

P7. Si $A = A_1 \times A_2$, entonces $(1,0)\cdot(0,1) = (0,0)$ y $(1,0) + (0,1) = (1,1)$, luego $\operatorname{Spec} A = ((1,0))_0 \coprod (0,1))_0$ y no es conexo.

Supongamos ahora que $\operatorname{Spec} A$ es la unión disjunta de dos cerrados C_1 y C_2. Sea I_i el ideal de las funciones que se anulan en todos los puntos de C_i. Sabemos que $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0 = C_1 \cup C_2 = \operatorname{Spec} A$, luego $I_1 \cdot I_2 \subset \operatorname{rad} A$ y que $(I_1 + I_2)_0 = (I_1)_0 \cap (I_2)_0 = C_1 \cap C_2 = \emptyset$, luego $I_1 + I_2 = A$ y existen $f_1 \in I_1$ y $f_2 \in I_2$ tales que $f_1 + f_2 = 1$. Sea $n \in \mathbb{N}$ tal que $0 = (f_1 f_2)^n = f_1^n f_2^n$. Observemos que $((f_1^n) + (f_2^n))_0 = (f_1^n)_0 \cap (f_2^n)_0 = (f_1)_0 \cap (f_2)_0 = ((f_1) + (f_2))_0 = \emptyset$, luego $(f_1^n) + (f_2^n) = A$. Por el teorema chino de los restos

$$A = A/(f_1^n)\cdot(f_2^n) = A/(f_1^n) \times A/(f_2^n).$$

P8. Sea $\mathfrak{p}_z \subset A$ un ideal primo. Si $\overline{x-n} \in \mathfrak{p}_z$, entonces $\overline{x-m} \notin \mathfrak{p}_z$, para $m \neq n$ y $\overline{x-m}$ es invertible en A_z. Luego, $A_z = (\mathbb{Q}[x, x_n]/((x-n)\cdot x_n))_z$ que es noetheriano. Si $\overline{x-n} \notin \mathfrak{p}_z$, para todo n, entonces $A_z = \mathbb{Q}[x]_z$ que es noetheriano.

A no es noetheriano, porque tenemos la cadena de inclusiones estrictas

$$(\overline{x_0}) \underset{\neq}{\subset} (\overline{x_0}, \overline{x_1}) \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} (\overline{x_0}, \ldots, \overline{x_n}) \underset{\neq}{\subset} \cdots$$

ya que $0 \neq \bar{x}_{n+1} \in A/(\overline{x_0}, \ldots, \overline{x_n}, \overline{x_{n+2}}, \overline{x_{n+3}}, \ldots) = \mathbb{Q}[x, x_{n+1}]/((x-(n+1))\cdot x_{n+1})$.

P9. a) Supongamos que $\mathfrak{m}\cdot M = M$. Escribamos $M = \langle n_1, \ldots, n_r\rangle$. Podemos suponer que ninguno de los n_i es combinación lineal de los demás, porque en tal caso quitaríamos tal n_i. Si $r > 0$, $n_1 \in \mathfrak{m}\cdot M$, luego $n_1 = \sum_{i=1}^{r} a_i \cdot n_i$, con $a_i \in \mathfrak{m}$. Entonces, $(1-a_1)\cdot n_1 = \sum_{i=2}^{r} a_i \cdot n_i$ y como $1 - a_1 \in \mathscr{O}$ es invertible ya que no pertenece al maximal, tenemos que $n_1 = \sum_{i=2}^{r} \frac{a_i}{1-a_1} \cdot n_i$ y hemos llegado a contradicción. Luego $r = 0$ y $M = 0$.

b) $\Leftarrow$) Sea $\bar{M} = M/\langle m_1, \ldots, m_n\rangle$, entonces

$$\bar{M}/\mathfrak{m}\cdot\bar{M} = M \Big/ (\mathfrak{m}\cdot M + \langle m_1, \ldots, m_n\rangle) = (M/\mathfrak{m}\cdot M) \Big/ \langle \bar{m}_1, \ldots, \bar{m}_n\rangle = 0.$$

Luego, $\bar{M} = \mathfrak{m}\cdot\bar{M}$, $\bar{M} = 0$ y $M = \langle m_1,\dots,m_n\rangle$.

c) $\Leftarrow$) $m_1,\dots,m_n$ generan M, luego el morfismo $\pi\colon \mathscr{O}^n \to M$, $\pi(a_i) = \sum_i a_i m_i$ es epiyectivo. Como M es libre, el morfismo π tiene sección, luego $\mathscr{O}^n = M \oplus \operatorname{Ker}\pi$. Al tensar por $\otimes_{\mathscr{O}}\mathscr{O}/\mathfrak{m}$ obtenemos que $\operatorname{Ker}\pi \otimes_{\mathscr{O}} \mathscr{O}/\mathfrak{m} = 0$, luego $\mathfrak{m}\cdot\operatorname{Ker}\pi = \operatorname{Ker}\pi$, $\operatorname{Ker}\pi = 0$ y $\mathscr{O}^n = M$.

P10. Escribamos $M = \langle m_1,\dots,m_n\rangle$ y supongamos que $M_x = 0$. Entonces, $\frac{m_i}{1} = 0$ y existe $s_i \in A\setminus\mathfrak{p}_x$ tal que $s_i\cdot m_i = 0$. Sea $s = \prod_i s_i$, entonces $s\cdot m_i = 0$, para todo i. Por lo tanto, para todo $y \in U_s = \operatorname{Spec}A\setminus(s)_0$, se cumple que $M_y = 0$, ya que $0 = \frac{m_i}{1} \in M_y$ (pues $s\cdot m_i = 0$). En conclusión, U es un abierto.

P11. Si $I \subset \mathfrak{p}_x$, entonces $I_x \subset \mathfrak{p}_x A_x \subsetneq A_x$. Si $I \not\subseteq \mathfrak{p}_x$, entonces existe $s \in I \cap (A\setminus\mathfrak{p}_x)$ y $I_x = A_x$, ya que $\frac{s}{1} \in I_x$ es invertible.

Supongamos que I es finito generado y que $I = I^2$. El conjunto de puntos $x \in \operatorname{Spec}A$ tal que $I_x = 0$ es un abierto de $\operatorname{Spec}A$, incluido en $(I)_0$. Si $x \in (I)_0$, entonces $I \subset \mathfrak{p}_x$ y $I_x = I_x^2$, luego $I_x = \mathfrak{p}_x A_x \cdot I_x$; por el lema de Nakayama, $I_x = 0$. Luego, $(I)_0$ es igual al abierto de puntos x tales que $I_x = 0$. Si denotamos $U = (I)_0$ y $V = \operatorname{Spec}A\setminus(I)_0$, vía el isomorfismo $A \to A_U \times A_V$, el ideal I se identifica con $0\times A_V$, ya que así es localmente.

P12. a) $f = \sup(f,0) - \sup(-f,0) = \sqrt{\sup(f,0)}^2 - \sqrt{\sup(-f,0)}^2 \in \mathfrak{m}_x^2$.

b) El ideal $\mathfrak{m}_x\cdot C(X)_x$ de $C(X)_x$ es no nulo: $h(y) := d(y,x)$ no es cero en ningún entorno de x y $h \in \mathfrak{m}_x$, luego si $g \in C(X)$ no se anula en x entonces no se anula en ningún punto de un entorno V de x, luego $g\cdot h$ no es cero en V, luego $0 \neq \frac{h}{1} \in \mathfrak{m}_x\cdot C(X)_x \subset C(X)_x$. Por el lema de Nakayama, $\mathfrak{m}_x\cdot C(X)_x$ no es un ideal finito generado y $C(X)_x$ no es un anillo noetheriano. Por tanto, $C(X)$ no es un anillo noetheriano.

c) Es inyectivo: si $[f]\cdot[g]^{-1} = 0$ entonces f es cero en una bola

$$B_\delta := \{y \in X\colon d(y,x) < \delta\} \subsetneq X.$$

Sea $h(y) := 1 - \frac{d(y,B_{\delta/2})}{d(y,B_\delta^c)+d(y,B_{\delta/2})}$, entonces $f\cdot h = 0$ y $\frac{f}{g} = 0$. Es epiyectivo: sea f' una función definida en un entorno U de x y $B_\delta \subset U$, entonces la función

$$f(x) := \begin{cases} f(x)\cdot h(x), \text{ si } x \in B_\delta \\ 0, \text{ si } x \notin B_\delta \end{cases}$$

es continua en X y $[f'] = [f]$.

P13. El morfismo $C^\infty(\mathbb{R})_{or} \to \mathscr{O}$, $\frac{f}{g} \mapsto [f]\cdot[g]^{-1}$ es un morfismo de anillos bien definido.

Es epiyectivo: Dada una función diferenciable f' en un entorno abierto U de 0, $B_r \subset U$ una bola abierta de radio r centrada en 0 y h una función diferenciable en $\mathbb{R}^n$ que sea 1 sobre $B_{r/2}$ y nula en B_r^c. Entonces, la función diferenciable f en X, definida por $f_{|U} = f' \cdot h_{|U}$ y $f_{|X-U} = 0$ cumple que $\frac{f}{1} \mapsto [f] = [f']$.

Es inyectivo: Si $[f]\cdot[g]^{-1} = 0$, entonces f se anula en un entorno V del cero. Sea h una función diferenciable en X que sea igual a 1 en un entorno $W \subset V$ de 0 y nula en V^c. Entonces, $f \cdot h = 0$ y $\frac{f}{g} = 0$.

P14. Escribamos $\operatorname{rad} A = (a_1, \ldots, a_r)$ y sean n_i tales que $a_i^{n_i} = 0$. Sea $n = n_1 + \cdot + n_r$, entonces

$$\operatorname{rad}(A)^n = (a_1^{\beta_1} \cdots a_r^{\beta_r})_{\beta_1+\cdots+\beta_r=n} = (0).$$

Sea $\pi : A \to A/I$ el morfismo de paso al cociente. Se cumple que $\pi(r(I)) = \operatorname{rad}(A/I)$. Sea n tal que $\operatorname{rad}(A/I)^n = 0$, entonces $\pi(r(I)^n) = \operatorname{rad}(A/I)^n = 0$, luego $r(I)^n \subseteq I$.

P15. Sea $\mathfrak{p}_x$ el ideal primo minimal y $a \in \mathfrak{p}_x$. $\operatorname{Spec} A_x = \{\mathfrak{p}_x \cdot A_x\}$, entonces $\operatorname{rad}(A_x) = \mathfrak{p}_x \cdot A_x$ y $\frac{a}{1} \in \mathfrak{p}_x \cdot A_x$ es nilpotente. Sea $n \in \mathbb{N}$ mínimo tal que $\frac{a^n}{1} = 0$. Existe $s \in A \setminus \mathfrak{p}_x$ tal que $a^n \cdot s = 0$. Entonces, $a \cdot (a^{n-1}s) = 0$ y como $a^{n-1}s \neq 0$ (porque $\frac{a^{n-1}}{1} \neq 0$) tenemos que a es divisor de cero.

P16. a) Tenemos que probar que $\operatorname{Spec} A_x \cap \operatorname{Spec} A_{x'} = \emptyset$ si y solo si existen dos abiertos disjuntos U y U', tales que $x \in U$ y $x' \in U'$.

Sea $S = A \setminus \mathfrak{p}_x$ y $S' = A \setminus \mathfrak{p}_{x'}$.

$\Rightarrow$) $\operatorname{Spec} A_{SS'} = \operatorname{Spec} A_S \cap \operatorname{Spec} A_{S'} = \operatorname{Spec} A_x \cap \operatorname{Spec} A_{x'} = \emptyset$. Entonces, $A_{SS'} = 0$, $\frac{1}{1} = 0$ y existen $s \in S$ y $s' \in S'$ tales que $0 = ss' \cdot 1 = ss'$. Tómese $U = U_s$ y $U' = U_{s'}$.

$\Leftarrow$) Podemos suponer que los dos abiertos son básicos $U = U_a$ y $U' = U_{a'}$ y han de cumplir que $U_{aa'} = U_a \cap U_{a'} = \emptyset$, es decir, aa' se anula en todo punto de $\operatorname{Spec} A$, es decir, aa' es nilpotente, luego existe n tal que $a^n \cdot a'^n = 0$. Además, $x \in U_a$, luego $a^n \in S$, igualmente $a'^n \in S'$. Entonces, $0 = \frac{1}{1} \in A_{SS'}$, por lo tanto $A_{SS'} = 0$ y $\operatorname{Spec} A_x \cap \operatorname{Spec} A_{x'} = \operatorname{Spec} A_{SS'} = \emptyset$.

b) $\Rightarrow$) Todos los ideales primos de A son maximales, luego todos los puntos de $\operatorname{Spec} A$ son cerrados. Por a), $\operatorname{Spec} A$ es T_2.

c) Es consecuencia inmediata de a).

d) Un espacio topológico compacto y T_1 es discreto si y solo si es finito.

P17. $\Rightarrow$) Sea $\mathfrak{m}\subset\mathscr{C}(X)$ un ideal maximal. Dados $f_1,\dots,f_n\in\mathfrak{m}$, tenemos que $\bigcap_{i=1}^{n}(f_i)_0^{rac}=(f_1^2+\cdots+f_n^2)_0^{rac}\neq\emptyset$ (si $f_1^2+\cdots+f_n^2$ no se anula en ningún punto sería invertible). Como $\operatorname{Spec}_{rac}\mathscr{C}(X)$ es compacto, $\emptyset\neq\bigcap_{f\in\mathfrak{m}}(f)_0^{rac}=(\mathfrak{m})_0^{rac}$, luego $\mathfrak{m}$ es racional.

P18. $\operatorname{Spec}(A_{x_i})_{x_j}=\operatorname{Spec}A_{x_i}\cap\operatorname{Spec}A_{x_j}=\begin{cases}\operatorname{Spec}A_{x_i},\text{ si } i=j.\\ \emptyset,\text{ si } i\neq j.\end{cases}$. Por lo tanto, $(A_{x_i})_{x_j}=A_{x_i}$ si $i=j$ y $(A_{x_i})_{x_j}=0$ si $i\neq j$. El morfismo es un isomorfismo porque lo es al localizar en todo punto cerrado.

P19. a) Procedamos por reducción al absurdo. Desechando los ideales primos $\mathfrak{p}_{x_i}$ que convenga, podemos suponer que $I\not\subset\mathfrak{p}_{x_1}\cup\cdots\cup\widehat{\mathfrak{p}_{x_i}}\cup\cdots\cup\mathfrak{p}_{x_n}$, para todo i y que $\mathfrak{p}_{x_i}\not\subset\mathfrak{p}_{x_i}$ para todo $i\neq j$. Sea $f_i\in I$ tal que $f_i(x_j)\neq 0$ (y $f_i(x_i)=0$). Entonces, $g_i=\prod_{j\neq i}f_j$ cumple que $g_i(x_j)\neq 0$ si y solo si $i=j$. Por tanto, $f=\sum_i g_i$ no se anula en ningún x_i y $f\in I$, lo que es contradictorio.

b) En efecto,

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

P20. U y V son también cerrados disjuntos. Sea I_U el ideal de todas las funciones que se anulan en todos los puntos de U e I_V el ideal de todas las funciones que se anulan en todos los puntos de V. Entonces, $(I_U+I_V)_0=(I_U)_0\cap(I_V)_0=U\cap V=\emptyset$, luego $I_U+I_V=1$ y existe $a\in I_U$ y $b\in I_V$ tales que $a+b=1$. Observemos que como a se anula en los puntos de U, entonces b no puede anularse en ninguno de los puntos de U, pues $a+b=1$. Igualmente, a no puede anularse en ningún punto de V. Por tanto, $U=U_b$ y $V=U_a$.

P21. Un ideal (primo) $\mathfrak{p}$ no está incluido en $\mathfrak{m}_x\iff\mathfrak{p}+\mathfrak{m}_x=A\iff$ existe $p\in\mathfrak{p}$ y $m\in\mathfrak{m}_x$ tales que $p+m=1\iff\mathfrak{p}\cap\{1+\mathfrak{m}_x\}\neq\emptyset$. Por tanto, $\operatorname{Spec}A_x=\operatorname{Spec}A_{1+\mathfrak{m}_x}$ y $A_x=A_{1+\mathfrak{m}_x}$.

P22. a) Si $(I)_0\subset U\iff(I+J)_0(I)_0\cap(J)_0=\emptyset$ (donde $(J)_0=U^c$) $\iff$ existen $i\in I$ y $j\in J$ tales que $i+j=1\Rightarrow(i)_0\cap(j)_0=\emptyset$, $\Rightarrow(I)_0\cap(j)_0=\emptyset\Rightarrow(I)_0\subset U_j$ (donde $j=1-i$).

b) i se anula en todos los puntos de $(I)_0$, luego $1+i$ no se anula en ningún punto de $(I)_0$, es decir, $(I)_0\subset U_{1+i}$.

c) $\operatorname{Spec}A_{1+I}=\bigcap_{i\in I}U_{1+i}=\bigcap_{(I)_0\subset U}U$.

d) Como $(I)_0 \subset \operatorname{Spec} A_{1+I}$, entonces $(I)_0^{max} \subset \operatorname{Spec}_{max} A_{1+I}$. Sea $y \in \operatorname{Spec} A_{1+I}$. Si $\bar{y} \cap (I)_0 = \emptyset$, entonces $(I)_0 \subseteq \bar{y}^c$ y por el apartado c), $y \in \operatorname{Spec} A_{1+I} \subset \bar{y}^c$, lo que es absurdo. Por tanto, existe un punto cerrado $x \in \bar{y} \cap (I)_0$, luego $\mathfrak{p}_y \subseteq \mathfrak{p}_x$ y $x \in (I)_0^{max}$.

P23. Si A es íntegro, entonces es reducido y como el ideal $\mathfrak{p}_g = (0)$ es primo, tenemos que $\operatorname{Spec} A = (0)_0 = \bar{g}$ y es irreducible. Recíprocamente, como $\operatorname{Spec} A$ es irreducible, es el cierre de un punto x, y $\mathfrak{p}_x$ es el único ideal primo minimal de A, luego $\mathfrak{p}_x = \operatorname{rad} A = 0$ y A es un anillo íntegro.

P24. $\Rightarrow$) $\operatorname{Spec} A/\operatorname{rad} A = \operatorname{Spec} A$ es irreducible y $A/\operatorname{rad} A$ es reducido, por lo tanto $A/\operatorname{rad} A$ es íntegro. Si $a \cdot b = 0$, entonces $\bar{a} \cdot \bar{b} = 0$ en $A/\operatorname{rad} A$, luego $\bar{a} = 0$ o $\bar{b} = 0$, es decir, a es nilpotente o b es nilpotente.

$\Leftarrow$) $A/\operatorname{rad} A$ es íntegro: si $\bar{a} \cdot \bar{b} = 0$, entonces $a \cdot b$ es nilpotente, luego existe n tal que $a^n \cdot b^n = 0$, por tanto a^n es nilpotente o b^n es nilpotente, en conclusión a es nilpotente (es decir, $\bar{a} = 0$) o b es nilpotente (es decir, $\bar{b} = 0$).

Por tanto, $\operatorname{Spec} A = \operatorname{Spec} A/\operatorname{rad} A$ es irreducible.

P25. Consideremos la inclusión $i\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ y el morfismo inducido en los espectros $i^*\colon \operatorname{Spec} \mathbb{Z}[x] \to \operatorname{Spec} \mathbb{Z}$. Sea $\mathfrak{p}_p := (p) \subset \mathbb{Z}$, donde p es un número primo. Entonces,

$$i^{*-1}(p) = \operatorname{Spec} \mathbb{Z}[x]/(p) = \operatorname{Spec} \mathbb{F}_p[x] = \begin{cases} (\bar{0}) \\ (\bar{p}(x)),\ \bar{p}(x) \in \mathbb{F}_p[x] \text{ irreducible.} \end{cases}$$

Por tanto, $i^{*-1}(p) = \begin{cases} (p) \\ (p(x)),\ \overline{p(x)} \in \mathbb{F}_p[x] \text{ irreducible.} \end{cases}$ Sea $\mathfrak{p}_g = (0) \subset \mathbb{Z}$. Entonces,

$$i^{*-1}(g) = \operatorname{Spec} \mathbb{Z}[x]_g = \operatorname{Spec} \mathbb{Q}[x] = \begin{cases} (0) \\ (p(x)),\ p(x) \in \mathbb{Z}[x] \text{ irreducible y } \operatorname{gr}(p(x)) > 0. \end{cases}$$

Luego,

$$\operatorname{Spec} \mathbb{Z}[x] = \begin{cases} (0) \\ (p(x)),\ p(x) \in \mathbb{Z}[x] \text{ irreducible.} \\ (p, p(x)),\ p \text{ primo y } \overline{p(x)} \in \mathbb{F}_p[x] \text{ irreducible.} \end{cases}$$

P26. Consideremos la inclusión $i\colon \mathbb{R}[x] \hookrightarrow \mathbb{R}[x,y]$ y el morfismo inducido en los espectros $i^*\colon \operatorname{Spec} \mathbb{R}[x,y] \to \operatorname{Spec} \mathbb{R}[x]$. Sea $\mathfrak{p}_p := (p(x)) \subset \mathbb{R}[x]$, donde $p(x)$ es un polinomio mónico irreducible. Si $p(x) = (x-a)$, Entonces,

$$i^{*-1}(p) = \operatorname{Spec} \mathbb{R}[x,y]/(p) = \operatorname{Spec} \mathbb{R}[x]/(x-a)[y] = \operatorname{Spec} \mathbb{R}[y] \begin{cases} (\bar{0}) \\ (\overline{q(y)}),\ \overline{q(y)} \in \mathbb{R}[y] \text{ irred.} \end{cases}$$

Por tanto,

$$i^{*-1}(p) = \begin{cases} (x-a) \\ (x-a, q(y)),\ q(y) \in \mathbb{R}[y] \text{ mon. irreducible.} \end{cases}$$

Si $p(x) = (x^2 + ax + b)$ (con $a^2 - 4b < 0$). Entonces,

$$i^{*-1}(p) = \operatorname{Spec} \mathbb{R}[x,y]/(p) = \operatorname{Spec} \mathbb{R}[x]/(x^2+ax+b)[y] = \operatorname{Spec} \mathbb{C}[y] \begin{cases} (\bar{0}) \\ (\overline{y-\beta}),\ \beta \in \mathbb{C} \end{cases}$$

Si α es una raíz de $p(x)$, entonces $\beta = c + d \cdot \alpha$, para ciertos $c, d, \in \mathbb{R}$ y vía el isomorfismo $\mathbb{R}[x,y]/(p) \simeq \mathbb{C}[y]$, $\overline{y - c - d \cdot x}$ se corresponde con $y - \beta$.

Por tanto,

$$i^{*-1}(p) = \begin{cases} (x^2+ax+b) \\ (x^2+ax+b, y-c-dx),\ \forall\, c,d \in \mathbb{R} \end{cases}$$

Sea $\mathfrak{p}_g = (0) \subset \mathbb{R}[x]$. Entonces,

$$i^{*-1}(g) = \operatorname{Spec} \mathbb{R}[x,y]_g = \operatorname{Spec} \mathbb{R}(x)[y] = \begin{cases} (0) \\ (p(x,y)),\ p(x,y) \text{ irred. y } \operatorname{gr}_y(p(x,y)) > 0. \end{cases}$$

Luego,

$$\operatorname{Spec} \mathbb{R}[x,y] = \begin{cases} (0) \\ (p(x,y)),\ p(x,y) \in \mathbb{R}[x,y] \text{ irreducible.} \\ (x-a, q(y)),\ q(x) \in \mathbb{R}[x] \text{ món. irreducible.} \\ (x^2+ax+b, y+cx+d),\ a^2-4b<0,\ \forall\, c,d \in \mathbb{R}. \end{cases}$$

Pruebe el lector que $\operatorname{Spec}_{max} \mathbb{R}[x,y] = \mathbb{C}^2/\sim$, donde $(a+bi, c+di) \sim (a-bi, c-di)$.

P27. Consideremos el morfismo de anillos $i\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ y el morfismo inducido en espectro $i^*\colon \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$. Sea $\mathfrak{p}_p = (p) \subset \mathbb{Z}$, con p número primo. Por la fórmula de la fibra

$$i^{*-1}(p) = \operatorname{Spec} \mathbb{Z}[i]/(p) = \operatorname{Spec} \mathbb{F}_p[x]/(x^2+1)$$

El polinomio x^2+1 tiene raíces en $\mathbb{F}_p$ si y solo si $-1 \in \mathbb{F}_p^{*2} = \{a^2, a \in \mathbb{F}_p^*\}$. Supongamos $p \neq 2$. El núcleo del epimorfismo $\mathbb{F}_p^* \to \mathbb{F}_p^{*2}$, $a \mapsto a^2$ es $\{\pm 1\}$. Por tanto, $|\mathbb{F}_p^{*2}| = (p-1)/2$. Luego, $\mathbb{F}_p^{*2}$ es un subgrupo de $\mathbb{F}_p^*$ de índice 2 y coincide con el núcleo del epimorfismo $\mathbb{F}_p^* \to \{\pm 1\}$, $a \mapsto a^{\frac{p-1}{2}}$ (el polinomio $x^{\frac{p-1}{2}} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene

a lo más $\frac{p-1}{2}$ raíces en $\mathbb{Z}/p\mathbb{Z}$). Por tanto, $-1 \in \mathbb{F}_p^{*2}$ si y solo si $(-1)^{\frac{p-1}{2}} = 1$, que equivale a que $\frac{p-1}{2}$ sea par, que equivale a que $p \equiv 1 \mod 4$.

En conclusión, el polinomio x^2+1 no tiene raíces en $\mathbb{F}_p$ si y solo si $p \equiv 3 \mod 4$. En este caso, $i^{*-1}(p) = (p)$. Si p no es congruente con $3 \mod 4$, entonces $(p) \subset Z[i]$ no es un ideal primo y $p \in \mathbb{Z}[i]$ no es irreducible. Por tanto, $p = z_1 z_2$, entonces $z_1 = a+bi$, $z_2 = a-bi$ y $p = a^2+b^2$, además z_1 y z_2 son irreducibles. En este caso $i^{*-1}(p) = \{(a+bi),(a-bi)\}$. Por tanto,

$$\operatorname{Spec}\mathbb{Z}[i] = \begin{cases} (0) \\ (p),\ p \text{ número primo congruente con } 3 \mod 4. \\ (a+bi),(a-bi),\ a^2+b^2 = p \text{ núm. primo no congr. con } 3 \mod 4. \end{cases}$$

P28. Los morfismo $\overline{p(x,y,z)} \mapsto p(x, \frac{y}{x}x, \frac{y}{x})$ y $q(x, y/x) \mapsto q(x,z)$ son inversos entre sí.

a) $i^{*-1}(U_x) = U_{\bar{x}}$ y $(\mathbb{C}[x,y,z]/(zx-y))_{\bar{x}} \simeq \mathbb{C}[x,y]_x$, luego $U_{\bar{x}} \simeq U_x$.

b) $i^{*-1}((0,0)) = \operatorname{Spec}\mathbb{C}[x,y,z]/(x,y,zx-y) = \operatorname{Spec}\mathbb{C}[z] = \{(0),(z-\gamma)\}$ que se corresponden con los ideales primos $(\bar{x})$ y $(\bar{x},\bar{y},\bar{z}-\gamma)$ de $\mathbb{C}[x,y,z]/(zx-y)$. Observemos que $i^{*-1}((0,0)) = (\bar{x},\bar{y})_0 = ((\bar{x},\bar{x}\bar{z})_0 = (\bar{x})_0$.

c) $i^{*-1}((y-\lambda x)_0) = (\bar{y}-\lambda\bar{x})_0 = (\bar{x}\bar{z}-\lambda\bar{x})_0 = (\bar{z}-\lambda)_0 \cup (\bar{x})_0 = (\bar{y}-\lambda\bar{x},\bar{z}-\lambda)_0 \cup i^{*-1}((0,0))$.

P29. Tenemos que ver si el ideal definido por cada sistema de ecuaciones coincide con el dado. Podemos suponer que el cuerpo base es $\mathbb{C}$. Las soluciones complejas del sistema de ecuaciones dado son

$$\{(0,1),(0,-1),(1,0),(-1,0)\}.$$

Por lo tanto, $(x^2+y^2-1, x^2y^2)_0 = \{(x,y-1) = \mathfrak{m}_{(0,1)}, (x,y+1) = \mathfrak{m}_{(0,-1)}, (x-1,y) = \mathfrak{m}_{(1,0)}, (x+1,y) = \mathfrak{m}_{(-1,0)}\}$. El segundo y tercer sistema de ecuaciones no tienen las mismas soluciones complejas que el dado, los demás tienen las mismas soluciones complejas que el dado. Tenemos que ver si el ideal definido por cada sistema coincide localmente con el dado. Observemos que

$$(x^2+y^2-1, x^2y^2)_{(0,1)} = (x^2+y^2-1, x^2)_{(0,1)} = (y^2-1, x^2)_{(0,1)} = (y-1, x^2)_{(0,1)}$$

Calcule el lector la localización en los demás puntos. Veamos que sucede con el primer sistema de ecuaciones

$$(x^2+y^2-1, x^4-x^2)_{(0,1)} = (x^2+y^2-1, x^2)_{(0,1)} = \cdots = (y-1, x^2)_{(0,1)}$$

que coincide con el dado. Idem al localizar en los demás puntos. Veamos qué sucede con el cuarto sistema de ecuaciones

$$\begin{aligned}&(x^2+y^2-1,(x+y+1)^2(x+y-1)^2)_{(0,1)} = (x^2+y^2-1,(x+y-1)^2)_{(0,1)}\\&= (x^2+y^2-1,2+2xy-2x-2y)_{(0,1)}\\&= ((x^2+y^2-1,(y-1)(-2+2x))_{(0,1)} = ((x^2+y^2-1,(y-1))_{(0,1)} = (x^2,y-1)_{(0,1)}.\end{aligned}$$

que coincide con el dado. Idem al localizar en los demás puntos. Veamos qué sucede con el quinto sistema de ecuaciones

$$\begin{aligned}&(x^2+y^2-1,(x+y+1)^2(x+y-1)^2)_{(0,1)} = (x^2+y^2-1,x+y-1)_{(0,1)}\\&= ((1-y)^2+y^2-1,x+y-1)_{(0,1)} = (y-1,x+y-1)_{(0,1)} = (x,y-1)_{(0,0)}\end{aligned}$$

y no coinciden. Veamos qué sucede con el sexto sistema de ecuaciones

$$\begin{aligned}&(x^2+y^2-1,(x+y+1)(x+y-1)(x-y+1)(x-y-1))_{(0,1)}\\&= (x^2+y^2-1,(x+y-1)(x-y+1)_{(0,1)} = (x^2+y^2-1,x^2-(y-1)^2)_{(0,1)}\\&= (y^2-1+(y-1)^2,x^2-(y-1)^2) = (y-1,x^2)_{(0,1)}\end{aligned}$$

que coincide con el dado. Idem al localizar en los demás puntos.

P30. El morfismo de localización $A \to A_S$ induce un morfismo $\operatorname{Esp} A_S \to \operatorname{Esp} A$. Tenemos que probar que vía este morfismo

$$\operatorname{Esp} A_S(B) = \{x \in \operatorname{Esp} A(B)\colon s(x) \text{ es invertible, para todo } s \in S\}$$

que es justamente la propiedad universal de la localización de A por S.

Solución de los problemas del capítulo tercero

P1. Sean $b_1,\dots,b_n \in B$ y $b'_1,\dots,b'_m \in B'$, tales que $B = \sum_i A\cdot b_i$ y $B' = \sum_j A'\cdot b'_j$. Entonces, $B \otimes_k B' = \sum_{ij}(A \otimes_k A')\cdot b_i \otimes b'_j$.

P2. No es finito, porque el morfismo inducido en los espectros $\operatorname{Spec} A_a = U_a \hookrightarrow \operatorname{Spec} A$ no es epiyectivo.

P3. a) Sea $z \in \operatorname{Spec} A$ tal que $\emptyset = f^{*-1}(z) = \operatorname{Spec} B_z/\mathfrak{p}_z B_z$. Entonces, $\mathfrak{p}_z\cdot B_z = B_z$, luego existen $a_1,\dots,a_n \in \mathfrak{p}_z$ y $\frac{b_1}{s_1},\dots,\frac{b_n}{s_n} \in B_z$ tales que $\sum_i a_i\cdot\frac{b_i}{s_i} = 1$. Entonces, si consideramos el morfismo finito inyectivo $g\colon A \to A[b_1,\dots,b_n]$, $a \mapsto f(a)$, tendremos que $g^{*-1}(z) = \emptyset$. lo cual es imposible.

b) Cópiese la demostración de este resultado en el caso de que f es finito.

c) Sean $\mathfrak{p}_y \underset{\neq}{\subset} \mathfrak{p}_z \underset{\neq}{\subset} B$ dos ideales primos tales que $f^*(y) = f^*(z) = x$. Sea $b \in \mathfrak{p}_z \setminus \mathfrak{p}_y$. El morfismo obvio $f' : A \to A[b] \subset B$ es finito. Sea $\mathfrak{p}_{y'} = \mathfrak{p}_y \cap A[b]$ y $\mathfrak{p}_{z'} = \mathfrak{p}_z \cap A[b]$. Tenemos que $\mathfrak{p}_{y'} \underset{\neq}{\subset} \mathfrak{p}_{z'}$ y $f'^*(y') = x = f'^*(z)$ lo cual es imposible, porque las fibras de f'^* son de dimensión cero.

P4. $\Rightarrow$) Es obviamente entero y existen $b_1, \ldots, b_n \in B$ tales que $B = \sum_i A \cdot b_i$, luego $B = A[b_1, \ldots, b_n]$ y es una A-álgebra de tipo finito. $\Leftarrow$) $B = A[b_1, \ldots, b_n]$ y los b_i son enteros sobre A, luego son enteros sobre $A[b_1, \ldots, b_{i-1}]$ y los morfismos $A[b_1, \ldots, b_{i-1}] \to A[b_1, \ldots, b_i]$ son finitos. Como la composición de morfismos finitos es finito, entonces $A \to B$ es finito.

P5. Es consecuencia de que el morfismo de anillos $A \to A \otimes_k K$ es finito es inyectivo.

P6. a) Sea $f \in J$ no nula, entonces existe n tal que $f \in k[x_1, \ldots, x_{2^n}]$, luego $f \notin \mathfrak{p}_{y_m}$ para todo $m > n$. Por tanto, $J \nsubseteq \mathfrak{p}_{y_m}$ para todo $m > n$.

Probemos que si un ideal $I \subset \underset{i \in \mathbb{N}}{\cup} \mathfrak{p}_{y_i}$, entonces $I \subseteq \mathfrak{p}_{y_n}$, para algún n. Sea $f \in I$ no nula, existe n tal que $f \in k[x_1, \ldots, x_{2^n} - 1] = A_n$, luego $f \notin \mathfrak{p}_{y_m}$ para todo $m > n$. Como $I \cap A_m \subseteq \underset{i<m}{\cup} \mathfrak{p}_{y_i} \cap A_m$, existe $i < m$ tal que $I \cap A_m \subset \mathfrak{p}_i$, por el problema 19 del capítulo 2. Existe i tal que $I \cap A_m \subset \mathfrak{p}_{y_i}$, para todo m. Por tanto, $I \subseteq \mathfrak{p}_{y_i}$.

b) $\operatorname{Spec} A_S = \{z \in \operatorname{Spec} A : \mathfrak{p}_z \subset \underset{i \in \mathbb{N}}{\cup} \mathfrak{p}_{y_i}\} = \{z \in \operatorname{Spec} A : \mathfrak{p}_z \subset \mathfrak{p}_{y_i}, \text{ para algún } i \in \mathbb{N}\} = \underset{i \in \mathbb{N}}{\cup} \operatorname{Spec} A_{y_i}$.

c) A_{y_i} es localización de $k(x_1, \ldots, \widehat{x_{2^i}}, \ldots, \widehat{x_{2^{i+1}-1}}, x_{2^{i+1}}, \cdots)[x^{2^i}, \cdots, x^{2^{i+1}-1}]$, luego es noetheriano. Sea

$$I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

una cadena de inclusiones de ideales de A_S. Por el apartado a) sabemos que existe m, tal que $I \subset \mathfrak{p}_{y_n}$, para todo $n > m$. Luego, $(I_1)_{y_n} = A_{y_n}$, para todo $n > m$. Para cada $i \leq m$, existe n_i tal que $I_{n_i, y_i} = I_{n_i+1, y_i} = \cdots$, porque A_{y_i} es noetheriano. Sea $n = \max\{m, n_1, \ldots, n_m\}$. Entonces, la cadena estabiliza a partir de n, porque así sucede al localizar en todo ideal maximal de A_S. Por tanto, A_S es noetheriano.

d) $\dim A_S = \sup\{\dim A_{y_n}\}_{n \in \mathbb{N}} = \sup\{2^n\}_{n \in \mathbb{N}} = \infty$.

P7. Existe un morfismo finito inyectivo $k[x_1, \ldots, x_n] \hookrightarrow A$, por el lema de normalización de Noether. Sabemos que $\dim A = \dim k[x_1, \ldots, x_n] = n$. Si $n = \dim A = 0$, entonces $\dim_k A < \infty$. Si $n = \dim A > 0$, entonces $\dim_k A \geq \dim_k k[x_1, \ldots, x_n] = \infty$.

P8. Los ideales maximales de $\mathbb{C}[x_1, \ldots, x_n]$ y $\mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - 1)$ son racionales. Por tanto, $\operatorname{Spec}_{max} \mathbb{C}[x_1, \ldots, x_n] = \{(x_1 - \alpha_1, \ldots, x_n - \alpha_n), \forall\, \alpha_1, \ldots, \alpha_n \in \mathbb{C}\}$ y

$\mathrm{Spec}_{max}\,\mathbb{C}[x_1,\dots,x_n]/(x_1^2+x_2^2+x_3^2-1) = \{(\bar{x}_1-\alpha_1,\dots,\bar{x}_n-\alpha_n),\ \forall\,(\alpha_1,\dots,\alpha_n)\in\mathbb{C}^n$, tales que $\alpha_1^2+\alpha_2^2+\alpha_3^2-1=0\}$.

Por último tenemos que calcular los puntos de corte de las dos curvas planas $p(x,y)=x^2+y^2-1=0$ y $q(x,y)=x^3+y^3-1=0$. Vamos a "eliminar" la variable y. Este ejemplo puede servir como una introducción a la teoría de la eliminación. Consideremos los polinomios como polinomios en x, con coeficientes en $\mathbb{C}(y)$. Por el algoritmo de Euclides, sabemos calcular $a'(x),b'(x)\in\mathbb{C}(y)[x]$ tales que $a'p+b'q=1$. Multiplicando por un polinomio conveniente $((y^2-1)y^2)$ eliminamos denominadores y obtenemos $ap+bq=(y^2-1)y^2$. Por tanto, si (α,β) es un punto de corte de las dos curvas, entonces $(\beta^2-1)\beta^2=0$. Por tanto, $\beta=0$ (luego $\alpha=1$) o $\beta=1$ (luego $\alpha=0$). En conclusión,

$$\mathrm{Spec}_{max}\,\mathbb{C}[x,y]/(x^2+y^2-1.x^3-y^3-1) = \{(\overline{(x-1,y)},\overline{(x,y-1)}.$$

P9. Sea $\mathfrak{m}\subset k[x_1,\dots,x_n]$ un ideal maximal. Consideremos la inclusión obvia

$$i\colon k[x_1]\hookrightarrow k[x_1,\dots,x_n].$$

Entonces $i^{-1}(\mathfrak{m})$ es un ideal maximal, luego $i^{-1}(\mathfrak{m})=(p(x_1))$ con $p(x_1)$ irreducible. Por inducción sobre n, $\bar{\mathfrak{m}}\subset k[x_1,\dots,x_n]/(p(x_1))=k[x_1]/(p(x_1))[x_2,\dots,x_n]$ está generado por $n-1$ elementos, luego $\mathfrak{m}$ por n. Si $\mathfrak{m}=(f_1,\dots,f_{n-1})$, entonces todas las componentes irreducibes de $\{\mathfrak{m}\}=(\mathfrak{m})_0=(f_1,\dots,f_{n-1})_0$ tienen dimensión mayor o igual que $n-(n-1)=1$, lo que es absurdo.

P10. $(y^2-x^2-y^3,x^2+y^3)=(y^2,x^2+y^3)=(y^2,x^2)$ y $\dim_{\mathbb{C}}\mathbb{C}[x,y]/(y^2,x^2)=4$.

P11. Dado un subconjunto $S\subset\mathrm{Spec}\,B$, denotemos $S_{rac}=S\cap\mathrm{Spec}_{rac}\,B$.

b) El morfismo de k-álgebras $A\otimes A\to B$, $a\otimes a'\mapsto f(a)\cdot g(a')$, induce un morfismo $(f^*,g^*)\colon X\to Y\times Y$, tal que $(f^*,g^*)(x)=(f^*(x),g^*(x))$ para todo punto racional $x\in X_{rac}$. El epimorfismo de k-álgebras $A\otimes_k A\to A$, $a\otimes a'\mapsto aa'$, induce un morfismo $i\colon Y\hookrightarrow Y\times Y$, tal que $i(y)=(y,y)$ para todo punto racional $y\in Y_{rac}$. Entonces,

$$C=[(f^*,g^*)^{-1}(i(Y))]_{rac}$$

que es un cerrado de X_{rac}, porque $i(Y)$ es un cerrado de $Y\times Y$. Evidentemente $f^*(c)=g^*(c)$, para todo $c\in C$, luego f^* coincide con g^* sobre $\bar{C}$. Cualquier otro cerrado D de X sobre el que coincidan f^* y g^*, cumple que $D_{rac}\subset C$, luego $D\subset\bar{C}$.

b) $(f^*,g^*)^{-1}(i(Y))_{rac}=X_{rac}$, luego $(f^*,g^*)^{-1}(i(Y))=X$ y $(f^*,g^*)=i\circ j$, para cierto morfismo de variedades algebraicas $j\colon X\to Y$. Consideremos las dos proyecciones $\pi_1,\pi_2\colon Y\times Y\to Y$ (que son las aplicaciones inducidas en espectros por los

dos morfismos $A \to A \otimes A$, $a \mapsto a \otimes 1, 1 \otimes a$). Observemos que $\pi_1 \circ (f^*, g^*) = f^*$ y $\pi_2 \circ (f^*, g^*) = g^*$. Entonces, $f^* = \pi_1 \circ (f^*, g^*) = \pi_1 \circ i \circ j = j = \pi_2 \circ i \circ j = \pi_2 \circ (f^*, g^*) = g^*$. Considerando los morfismos entre los anillos, en vez de los inducidos en espectros, estamos diciendo que $f = g$.

P12. No supongamos $\operatorname{Spec} A$ irreducible. Por el lema de normalización de Noether existe un morfismo finito inyectivo $k[x_1, \ldots, x_n] \hookrightarrow A$, luego tenemos un morfismo finito e inyectivo $K[x_1, \ldots, x_n] \hookrightarrow A \otimes_k K$ y $\dim A = n = \dim(A \otimes_k K)$.

El morfismo $i : A \to A \otimes_k K$ es un morfismo plano. Si $\mathfrak{p}$ es un ideal primo minimal de $A \otimes_k K$, por el teorema del descenso $\mathfrak{q} = i^{-1}(\mathfrak{p})$ es un ideal primo minimal de A.

Supongamos ya que $\operatorname{Spec} A$ es irreducible. Podemos suponer que A es íntegro (haciendo cociente por los nilpotentes). Sea $\mathfrak{p} \subset A \otimes_k K$ un ideal primo minimal.

Supongamos que K es una k-álgebra de tipo finito. Sea $x_1, \ldots, x_n$ una base de trascendencia de K. $A \otimes_k k(x_1, \ldots, x_n)$ es íntegro porque es localización del anillo íntegro $A \otimes_k k[x_1, \ldots, x_n] = A[x_1, \ldots, x_n]$. $A \otimes_k k(x_1, \ldots, x_n) \hookrightarrow (A \otimes_k K)/\mathfrak{p}$ es un morfismo finito e inyectivo, luego $\dim(\mathfrak{p})_0 = \dim(A \otimes_k k(x_1, \ldots, x_n)) = \dim A = n$.

Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos minimales de $A \otimes_k K$. Existe una k-subextensión de tipo finito Σ de K, de modo que $\mathfrak{q}_i = \mathfrak{p}_i \cap (A \otimes_k \Sigma) \neq \mathfrak{p}_j \cap (A \otimes_k \Sigma) = \mathfrak{q}_j$, para todo $i \neq j$. Sea U_a un abierto básico incluido en $(\cup_{j \neq 1} (\mathfrak{q}_j)_0)^c$ y el morfismo natural $\pi \colon \operatorname{Spec}(A \otimes_k K) = \operatorname{Spec}(A \otimes_k \Sigma) \otimes_\Sigma K \to \operatorname{Spec}(A \otimes_k \Sigma)$. Entonces, $\dim(\mathfrak{p}_1)_0 = \dim \pi^{-1}(U_a) = \dim U_a = \dim((\mathfrak{q}_1)_0) = n$.

P13. Supondremos que $\operatorname{Spec} B$ es unión de variedades irreducibles de dimensión n. El morfismo $A \to B$ es plano, luego por el teorema del descenso, f^* aplica los puntos genéricos de las componentes irreducibles de $\operatorname{Spec} B$ en puntos genéricos de las componentes irreducibles de $\operatorname{Spec} A$, luego la imagen de cada componente irreducible de $\operatorname{Spec} B$ es densa en una componente irreducible de $\operatorname{Spec} A$. Sea $a_1 \in A$ tal que a_1 se anule en y y no se anule en ninguna componente irreducible. El morfismo $A/(a_1) \to B/(f(a_1))$ es plano, luego por el teorema del descenso, f^* aplica los puntos genéricos de las componentes irreducibles de $(f(a_1))_0 = f^{*-1}((a_1)_0)$ en puntos genéricos de las componentes irreducibles de $(a_1)_0$, luego la imagen de cada componente irreducible de $(f(a_1))_0$ es densa en una componente irreducible de $(a_1)_0$. Sea ahora $a_2 \in A$ tal que a_2 se anule en y y no se anule en ninguna componente irreducible de $(a_1)_0$, entonces $f(a_2)$ no se anula en ninguna de las componentes irreducibles de $(f(a_1))_0 = f^{*-1}((a_1)_0)$. El morfismo de anillos $A/(a_1, a_2) \to B/(f(a_1), f(a_2))$ es plano, luego por el teorema del descenso, f^* aplica los puntos genéricos de las componentes irreducibles de $(f(a_1), f(a_2))_0 =$

$f^{*-1}((a_1,a_2)_0)$ en puntos genéricos de las componentes irreducibles de $(a_1,a_2)_0$, luego la imagen de cada componente irreducible de $(f(a_1),f(a_2))_0$ es densa en una componente irreducible de $(a_1,a_2)_0$. Así se procede $m=\dim \operatorname{Spec} A$ veces, obtenemos $(a_1,\ldots,a_m)_0=\{y=y_1,\ldots,y_r\}$ puntos cerrados, y $f^{*-1}(y_1,\ldots,y_r)$ es unión de variedades irreducibles de dimensión $\dim \operatorname{Spec} B-m$.

P14. Escribamos $\bar{X}=\operatorname{Spec}_{rac} A$, $\bar{Y}=\operatorname{Spec}_{rac} B$, luego $\bar{X}\times\bar{Y}=\operatorname{Spec}_{rac}(A\otimes_k B)$. Sea $f\in A\otimes_k B$ y C el conjunto de puntos $\alpha\in\bar{X}$ tales que $f_{|\alpha\times\bar{Y}}=0$. Observemos que si $f_{|\alpha\times\bar{Y}}\neq 0$, entonces existe un punto $\beta\in\bar{Y}$, tal que $f(\alpha,\beta)\neq 0$, luego existe un entorno abierto (básico) $\bar{U}_\alpha$ de α tal que para todo $\alpha'\in\bar{U}_\alpha$ se cumple que $f(\alpha',\beta)\neq 0$; por tanto, $f_{|\alpha'\times\bar{Y}}\neq 0$. En conclusión, C es un cerrado de $\bar{X}$. Sea $g\in A\otimes B$ y D el conjunto de puntos $\alpha\in\bar{X}$ tales que $g_{|\alpha\times\bar{Y}}=0$. Si $f\cdot g=0$, entonces para cada punto cerrado $\alpha\in\bar{X}$, tenemos que $f_{|\alpha\times\bar{Y}}\cdot g_{|\alpha\times\bar{Y}}=0$, luego $f_{|\alpha\times\bar{Y}}=0$ o $g_{|\alpha\times\bar{Y}}=0$, es decir, $\alpha\in C\cup D$. En conclusión, $\bar{X}=C\cup D$ lo que implica que $\bar{X}=C$ (luego f es nilpotente) o que $\bar{X}=D$ (luego g es nilpotente). Luego, $\operatorname{Spec} A$ es irreducible por el problema 24 del capítulo 2.

P15. Sea $\bar{k}$ el cierre algebraico de k. $X\times_k\bar{k}=\cup_i X_i$ es uníón de componentes irreducibles de dimensión $n=\dim X$ y $Y\times_k\bar{k}=\cup_j Y_j$ es uníón de componentes irreducibles de dimensión $m=\dim Y$. Entonces, $(X\times Y)\times_k\bar{k}=(X\times_k\bar{k})\times_{\bar{k}}(Y\times_k\bar{k})$ es unión de las componentes irreducibles $X_i\times_{\bar{k}} Y_j$, que son de dimensión $n+m$.

Sea $X\times Y=\cup_r Z_r$ unión de componentes irreducibles, con $\dim Z_r=n_r$. Entonces, $Z_r\times_k\bar{k}=\cup_s Z_{rs}$, con Z_{rs} es irreducible de dimensión n_r, cuyo punto genérico se proyecta en el punto genérico de Z_r. Luego, $\cup_{rs} Z_{rs}=\cup_{i,j}(X_i\times Y_j)$ y $Z_{rs}=X_i\times Y_j$ para ciertos i,j, y $r=\dim Z_{rs}=\dim X_i\times Y_j=n+m$.

P16. Sigamos las notaciones de la solución del problema 14. Nos falta probar que $A\otimes_k B$ es reducido. Sean $\Sigma=A_{A\setminus\{0\}}$ y $\Sigma'=B_{B\setminus\{0\}}$. Como el morfismo de anillos $A\otimes_k B\hookrightarrow\Sigma\otimes_k\Sigma'$ es inyectivo, basta probar que $\Sigma\otimes_k\Sigma'$ es reducido. Se concluye por el problema 17 del capítulo 1.

P17. Sean $f=\sum_i a_i\otimes\lambda_i$, $g=\sum_j a'_j\otimes\mu_j\in A\otimes_k K$, tales que $f\cdot g=0$. Sea $B:=k[\lambda_i,\mu_j]_{i,j}\subset K$. Como $f,g\in A\otimes_k B$ y $f\cdot g=0$, entonces $f=0$ o $g=0$.

P18. Tenemos que comprobar si $\bar{g}\in(\bar{f})\subset\mathbb{C}[x,y]/(x^2+y^2-9)$, o equivalentemente, si

$$\begin{aligned}0=\bar{g}\in\mathbb{C}[x,y]/(x^2+y^2-9,f)&=\mathbb{C}[x,y]/(x^2+y^2-9,(y-3)(x-5))\\&=\mathbb{C}[x,y]/(x^2+y^2-9,y-3)\times\mathbb{C}[x,y]/(x^2+y^2-9,x-5)=\mathbb{C}[x]/(x^2)\times\mathbb{C}[y]/(y^2+16)\end{aligned}$$

Tenemos que $\bar{g}=(25\bar{x},0)\neq 0$.

Los puntos de la curva plana donde se anula f son $\{(0,3),(5,\pm 4i)\}$, los puntos donde se anula g son $\{(0,\pm 3),(5,\pm 4i)\}$. Por tanto, g es nula en todo punto cerrado de $(f)_0$ y existe n tal que $g^n \in (f)$, es decir, f divide a una potencia de g. Sí, porque la igualdad o no de (g^n, f) con (f) es estable por cambio de cuerpo base

P19. Sea $\Delta := (x_1 - x_1', \ldots, x_n - x_n')_0 \subset \operatorname{Spec} k[x_1,\ldots,x_n,x_1',\ldots,x_n'] = \mathbb{A}^n \times_k \mathbb{A}^n$ y consideremos el cerrado obvio $Y \times Y' \subset \mathbb{A}^n \times \mathbb{A}^n$. Se cumple que $Y \cap Y' = \Delta \cap (Y \times Y')$. Por el teorema del ideal principal de Krull (por el problema 15 todas las componentes irreducibles de $Y \times Y'$ son de de dimensión $\dim Y + \dim Y'$), todas las componentes irreducibles Z de $Y \cap Y'$ cumplen $\dim Z \geq \dim(Y \times Y') - n = \dim Y + \dim Y' - n$ y se concluye.

P20. Sea $A = k[x_1,\ldots,x_n]/I$, luego $A \otimes_k \bar{k} = \bar{k}[x_1,\ldots,x_n]/(I)$. El morfismo $A \to A \otimes_k \bar{k}$ es inyectivo y entero. Entonces la aplicación inducida $\operatorname{Spec}(A \otimes_k \bar{k}) \to \operatorname{Spec} A$ es epiyectiva. Entonces, $p(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$ pertenece a I si y solo si se anula en todos los puntos de $\operatorname{Spec}(A \otimes_k \bar{k})$, que equivale a que se anula en todos los puntos $\bar{k}$-racionales de $\operatorname{Spec}(A \otimes_k \bar{k})$, es decir, se anula en el conjunto de las soluciones del sistema $\{f_i = 0\}_{i \in I}$ con valores en $\bar{k}$.

P21. Supongamos que A es íntegro. y que $\{j_1,\ldots,j_s\}$ es cualquier subconjunto tal que el morfismo $R = k[x_1,\ldots,x_s] \hookrightarrow A$ es inyectivo. Entonces, el cuerpo de fracciones de R se inyecta en el de A, luego tomando grados de trascendencia $s \leq \dim A$. Ahora en general. Reordenando las variables, podemos suponer que $\{j_1,\ldots,j_r\} = \{1,\ldots,r\}$. Como el morfismo dado es inyectivo, en espectros es denso, luego existe un ideal primo $\mathfrak{p} \subset A$, tal que $\mathfrak{p} \cap k[x_1,\ldots,x_r] = 0$. Por tanto, la composición $R = k[x_1,\ldots,x_r] \hookrightarrow A \to A/\mathfrak{p}$ es inyectiva, luego $r \leq \dim A/\mathfrak{p} \leq \dim A$. Para cada x_s, con $s > r$, tenemos que existe un polinomio $p_s(x_1,\ldots,x_r,x_s)$ tal que $\overline{p_s(x_1,\ldots,x_r,x_s)} = 0$. Si $\mathfrak{p}$ es un ideal primo de A, $\dim A/\mathfrak{p} \leq r$, porque el grado de trascendencia del cuerpo de fracciones de $A/\mathfrak{p}$ es menor o igual que r. Por lo tanto, $\dim A = \max\{\dim A/\mathfrak{p}_x, \forall x \in \operatorname{Spec} A\} \leq r$. Luego, $\dim A = r$.

P22. Por cambio de coordenadas, podemos suponer $\alpha = 0$, luego $\mathfrak{m}_\alpha = (\bar{x}_1,\ldots,\bar{x}_n)$. Escribamos $p = p_r + \cdots + p_{r+s}$, con p_i homogéneos de grado i y $p_r \neq 0$. Como $p(\alpha) = 0$, entonces $r > 0$. Si $r > 1$, $A_X/\mathfrak{m}_\alpha^2 = k[x_1,\ldots,x_n]/(x_i x_j)_{1 \leq ij \leq n}$ y $\dim_k \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 = n$. Si $r = 1$, entonces $A_X/\mathfrak{m}_\alpha^2 = k[x_1,\ldots,x_n]/(p_1, x_i x_j)_{1 \leq ij \leq n}$ y $\dim_k \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 = n - 1$. Por otra parte, $(\frac{\partial p}{\partial x_1}(\alpha),\ldots,\frac{\partial p}{\partial x_n}(\alpha)) \neq 0$ si solo si $r > 1$. Probemos el último «si y solo si». $\Rightarrow$) Es consecuencia del lema de Nakayama. $\Leftarrow$) Sea $m = \dim_k \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$. Evidentemente, $m \leq n-1$. Si $m < n-1$, entonces $(x_1,\ldots,x_n) = (f_1,\ldots,f_m,p) \subset k[x_1,\ldots,x_n]_\alpha$, pero todas las componentes irreducibles de $(f_1,\ldots,f_m,p)_0 \subset \mathbb{A}^n$ son de dimensión

mayor o igual que $n-m-1 \geq 1$, y la que pasa por $\alpha = 0$ es α,que tiene dimensión 0.

P23. Si B es invertible entonces $c_{AB}(x) = c_{BABB^{-1}}(x) = c_{BA}(x)$.

El conjunto de matrices cuadradas de orden n se identifica con los puntos racionales de $M := \operatorname{Spec} k[x_{ij}]_{1\leq i,j\leq n}$ y el de las matrices invertibles con los puntos racionales de $U := U_{\det(x_{ij})}$. El conjunto de polinomios de grado menor o igual que n se identifica con los puntos racionales de $P = \operatorname{Spec} k[x_1,\ldots,x_{n+1}]$. El morfismo $c : M_{rac} \times M_{rac} \to P_{rac}, c(A,B) := c_{AB}(x) - c_{BA}(x)$ es constantemente nulo sobre $M_{rac} \times U_{rac}$ y es el inducido por un morfismo $M \times M \to P$ que ha de ser constantemente nulo sobre $M \times U$, luego es constantemente nulo sobre $M \times M$, luego c es constantemente nulo.

P24. 2. El conjunto de polinomios mónicos de grado n es biyectivo con el conjunto de los puntos racionales de $P = \mathbb{A}^n$: $(a_1,\ldots,a_n) \mapsto x^n + a_1x^{n-1} + \cdots + a_n$. Consideremos el morfismo $\pi\colon \mathbb{A}^n \to P$, $(\alpha_1,\ldots,\alpha_n) \mapsto (x-\alpha_1)\cdots(x-\alpha_n)$, el morfismo inducido por el morfismo finito $k[a_1,\ldots,a_n] \to k[x_1,\ldots,x_n]$, $a_i \mapsto (-1)^i \prod_{|\alpha|=i} x^\alpha$. Sea $C = \bigcup_{i\neq j}(x_i - x_j)_0$. Entonces, $\pi(C)$ es un cerrado de P de dimensión $n-1$ y los puntos racionales de $V = P - \pi(C)$ se corresponden con los polinomios mónicos de grado n sin raíces múltiples. Sea U la variedad algebraica del problema anterior, cuyos puntos racionales se corresponden biyectivamente con las matrices cuadradas de orden n invertibles. Sea $c\colon U \to P$ el morfismo de variedades algebraicas que sobre los puntos racionales asigna a cada matriz invertible A su polinomios característico $c_A(x)$. Entonces, el conjunto de puntos racionales de $W = c^{-1}(V)$ se corresponde con matrices cuadradas invertibles diagonalizables.

3. Si la matriz (a_{ij}) es diagonal, es fácil comprobar que $c(a_{ij})((a_{ij})) = 0$. Como $c_{BAB^{-1}}(x) = c_A(x)$ y $p(BAB^{-1}) = Bp(A)B^{-1}$, para todo $p(x) \in k[x]$, es fácil probar que $c_{(a_{ij})}((a_{ij})) = 0$, para toda matriz diagonalizable. Sea $M_n = \operatorname{Spec} k[x_{ij}]_{1\leq i,j\leq n}$, cuyos puntos racionales se corresponden biyectivamente con las matrices cuadradas de orden n y $c\colon U \to M_n$ el morfismo de variedades algebraicas que sobre los puntos racionales es la asignación $A \mapsto c_A(A)$. Como c es nula sobre los puntos racionales de W, entonces es nula sobre W, luego es nula.

P25. a) El morfismo inverso de $k[x,y]/(y^2 - x^2 - x^3) \to k[t]$, $x \mapsto t^2 - 1$, $y \mapsto t^3 - t$, en los cuerpos de fracciones, es $t \mapsto \frac{y}{x}$. La longitud del lazo es

$$\int_{-1}^{1} \sqrt{x'^2 + y'^2}\cdot dt = \int_{-1}^{1} \sqrt{4t^2 + (3t^2-1)^2}\cdot dt$$

b) El morfismo inverso es $t = \frac{y}{x}$, entre los cuerpos de fracciones.

Solución de los problemas del capítulo cuarto

P1. a) Veamos que la composición de los morfismos naturales

$$\mathrm{Proj}R \hookrightarrow \mathrm{Spec}R \to \mathrm{Spec}\, R_0,$$

que asigna a cada ideal primo homogéneo $\mathfrak{p} \subset R$ el ideal primo $[\mathfrak{p}]_0 := \mathfrak{p} \cap R_0$, es el homeomorfismo buscado. Observemos que el ideal primo $\mathfrak{p} \subset R$ está determinado por sus elementos homogéneos de grado cero: un elemento homogéneo $g \in R$ de grado m pertenece a $\mathfrak{p}$ si y solo si g^r/f^m pertenece a $[\mathfrak{p}]_0$. Por tanto, $\mathrm{Proj}R \to \mathrm{Spec}R_0$ es inyectivo. Si $\mathfrak{q} \subset R_0$ es un ideal primo, veamos que $\mathfrak{p} := \oplus_m \mathfrak{p}_m$, donde definimos $\mathfrak{p}_m := \{g \in R_m \,|\, g^r \cdot f^{-m} \in \mathfrak{q}\}$, 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 $\mathfrak{p} \cap R_0 = \mathfrak{q}$. En conclusión, $\mathrm{Proj}R \to \mathrm{Spec}R_0$ 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.

b) $U_f^h = \mathrm{Proj}R_f = \mathrm{Spec}[R_f]_0$.

c) $\mathrm{Spec}[R_f]_0 = U_f^h = \mathrm{Proj}R - (f)_0^h = \emptyset$, luego $[R_f]_0 = 0$, entonces $R_f = 0$ y f es nilpotente.

P2. $\Rightarrow$) Los ideales primos minimales son homogéneos, luego han de contener al ideal irrelevante, luego $R_n \subset \mathrm{rad}R$, para todo $n \neq 0$.

$\Leftarrow$) Todo ideal primo homogéneo contiene a toda $f_n \in R_n$, para todo $n \neq 0$, luego contiene al irrelevante y $\mathrm{Proj}R = \emptyset$.

P3. a) $C \cap U_{x_0}^h = (x_0^2 + x_1^2 + x_2^2)_0^h \cap U_{x_0}^h = (\frac{x_0^2}{x_0^2} + \frac{x_1^2}{x_0^2} + \frac{x_2^2}{x_0^2}{}_0$. Es decir, $C \cap U_{x_0} \equiv 1 + x^2 + y^2 = 0$, con $x = \frac{x_1}{x_0}$ e $y = \frac{x_2}{x_0}$.

$C \cap U_{x_1}^h = (x_0^2 + x_1^2 + x_2^2)_0^h \cap U_{x_1}^h = (\frac{x_0^2}{x_1^2} + \frac{x_1^2}{x_1^2} + \frac{x_2^2}{x_1^2}{}_0$. Es decir, $C \cap U_{x_1} \equiv \bar{x}^2 + 1 + \bar{y}^2 = 0$, con $\bar{x} = \frac{x_0}{x_1}$ y $\bar{y} = \frac{x_2}{x_1}$.

$C \cap U_{x_2}^h = (x_0^2 + x_1^2 + x_2^2)_0^h \cap U_{x_2}^h = (\frac{x_0^2}{x_2^2} + \frac{x_1^2}{x_2^2} + \frac{x_2^2}{x_2^2}{}_0$. Es decir, $C \cap U_{x_2} \equiv \bar{x}'^2 + \bar{y}'^2 + 1 = 0$, con $x' = \frac{x_0}{x_2}$ y $y' = \frac{x_1}{x_2}$.

b) $x = \frac{x_1}{x_0}$ e $y = \frac{x_2}{x_0}$. Luego, homogeneizando (multiplicando por x_0^2) la curva $y + x^2$ en el plano afín $U_{x_0}^h$, obtenemos $x_2 x_0 + x_1^2 = 0$. La recta afín $x = 0$ es la recta

proyectiva $x_1 = 0$ (cortada con $U^h_{x_0}$) y la recta del infinito es $x_0 = 0$. Entonces, el punto de corte de $x_0 = 0$, $x_1 = 0$, $x_2x_0 + x_1^2 = 0$ es $[0,0,1]$. La respuesta es sí.

P4. Escribamos $p(x,y) = \sum_{i=0}^{n} p_i(x)y^i$ (con $p_n(x) \neq 0$). Sabemos por el ejemplo 3.5.19 del capítulo 3, que el morfismo es finito si y solo si $\operatorname{gr} p_n(x) = 0$. Veamos que las asíntotas verticales de $p(x,y) = 0$ son las rectas $x - \alpha = 0$, donde α es raíz de $p_n(x)$: Sea $m = \operatorname{gr} p(x,y)$. Consideremos las coordenadas homogéneas x_0, x_1, x_2 ($x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$). tenemos que calcular las tangentes a $x_0^m \cdot p(\frac{x_1}{x_0}, \frac{x_2}{x_0}) = 0$ en el punto $(0,0,1)$ (distintas de $x_0 = 0$). Es decir, las tangentes en $(0,0) \in U^h_{x_2} = \operatorname{Spec} k[\frac{x_0}{x_2}, \frac{x_1}{x_2}]$ de la curva

$$0 = (\frac{x_0}{x_2})^m \cdot p(\frac{x_1}{x_0}, \frac{x_2}{x_0}) = \bar{x}^m \cdot p(\frac{\bar{y}}{\bar{x}}, \frac{1}{\bar{x}}) = \bar{x}^m \cdot \sum_{i=0}^{n} p_i(\frac{\bar{y}}{\bar{x}})(\frac{1}{\bar{x}})^i$$

(donde $\bar{x} = \frac{x_0}{x_2}$ y $\bar{y} = \frac{x_1}{x_2}$). La parte homogénea de menor grado es $\bar{x}^{m-n} \cdot p_n(\frac{\bar{y}}{\bar{x}}) = \bar{x}^r \cdot \prod_i (\bar{y} - \alpha_i \bar{x})$, donde $\{\alpha_i\}$ son las raíces de $p_n(x)$.

P5. La ecuación homogénea de la circunferencia es $x_1^2 + x_2^2 - x_0^2 = 0$. Los puntos de corte con la recta del infinito $x_0 = 0$ son $x_1 = 1$ y $x_2 = \pm i$, es decir, los puntos $(0,1,\pm i)$. Las ecuaciones afines de la circunferencia en $x_2 \neq 0$, son $\bar{x}_1^2 + 1 - \bar{x}_2^2 = 0$ (donde $\bar{x}_1 = \frac{x_1}{x_2}$ y $\bar{x}_2 = \frac{x_0}{x_2}$). La recta tangente a la circunferencia en el punto $\bar{x}_1 = \frac{1}{i} = -i$ y $\bar{x}_2 = \frac{0}{i} = 0$, es $-2 \cdot i(\bar{x}_1 + i) + 2 \cdot 0 \cdot \bar{x}_2 = 0$, es decir, la recta $\bar{x}_1 + i = 0$, cuya ecuación homogénea es $x_1 + ix_2 = 0$, que en coordenadas afines es la recta $x + iy = 0$. La recta tangente a la circunferencia en el punto $\bar{x}_1 = \frac{1}{-i} = i$ y $\bar{x}_2 = \frac{0}{-i} = 0$, es $2 \cdot i(\bar{x}_1 - i) + 2 \cdot 0 \cdot \bar{x}_2 = 0$, es decir, la recta $\bar{x}_1 - i = 0$, cuya ecuación homogénea es $x_1 - ix_2 = 0$, que en coordenadas afines es la recta $x - iy = 0$. Éstas son las asíntotas.

P6. Supongamos $\alpha_0 \neq 0$. Entonces, $\{p(x_0,x_1,x_2) = 0\} \cap U^h_{x_0} \equiv q(x,y) = \frac{p(x_0,x_1,x_2)}{x_0^n} = 0$ (con $x = \frac{x_1}{x_0}$ y $y = \frac{x_2}{x_0}$). Observemos que $x_1 = xx_0$, luego $\frac{\partial p}{\partial x_1} = x_0^{n-1} \frac{\partial q}{\partial x}$ e igualmente $\frac{\partial p}{\partial x_2} = x_0^{n-1} \frac{\partial q}{\partial y}$. La recta (afín) tangente a la curva en $(\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0})$ es

$$\frac{\partial q}{\partial x}(\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0}) \cdot (x - \frac{\alpha_1}{\alpha_0}) + \frac{\partial q}{\partial y}(\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0}) \cdot (y - \frac{\alpha_2}{\alpha_0}) = 0.$$

Multipliquemos por $\alpha_0 x_0^n$ y obtenemos la ecuación homogénea de la recta proyectiva tangente

$$\frac{\partial p}{\partial x_1}(\alpha) \cdot (\alpha_0 x_1 - \alpha_1 x_0) + \frac{\partial p}{\partial x_2}(\alpha) \cdot (\alpha_0 x_2 - \alpha_2 x_0) = 0.$$

Como $x_0\frac{\partial p}{\partial x_0}+x_1\frac{\partial p}{\partial x_1}+x_2\frac{\partial p}{\partial x_2}=\mathrm{gr}(p)\cdot p$, entonces $\alpha_0\frac{\partial p}{\partial x_0}(\alpha)+\alpha_1\frac{\partial p}{\partial x_1}+\alpha_2\frac{\partial p}{\partial x_2}=0$. De esta igualdad obtenemos que la recta anterior es la recta

$$\frac{\partial p}{\partial x_0}(\alpha)\cdot x_0+\frac{\partial p}{\partial x_1}(\alpha)\cdot x_1+\frac{\partial p}{\partial x_2}(\alpha)\cdot x_2=0.$$

(ecuación del plano tangente al cono $p(x_0,x_1,x_2)=0$ en α, que pasa por el origen).

P7. Sea $X_i=\{(\lambda_0,\dots,\lambda_n)\in X:\lambda_i\neq 0\}$ y

$$U_i:=\{(\alpha_0,\dots,\hat{\alpha}_i,\dots,\alpha_n)\in\Sigma^n:\ p_1(\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n)=\cdots p_r(\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n)=0\}.$$

Establezcamos en U_i la relación de equivalencia $\sim$: $\alpha\sim\beta$ si existe $\tau\in\mathrm{Aut}_{k-alg}(\Sigma)$ tal que $\alpha=\tau(\mu)$ (donde $\tau(\mu_1,\dots,\mu_n)=(\tau(\mu_1),\dots,\tau(\mu_n))$.

Entonces, $U_i\times\Sigma^*=X_i$, $((\alpha_0,\dots,\hat{\alpha}_i,\dots,\alpha_n),\lambda)\mapsto\lambda\cdot(\alpha_0,\dots,\overset{i}{1},\dots,\alpha_n)$ es biyectivo y $X_i/\sim=U_i/\sim=U^h_{\tilde{x}_i}$.

P8. a) $\pi^{-1}(or)=(x,y)^h_0=\mathrm{Proj}\,A/(x,y)=\mathrm{Proj}\bigoplus_{n\in\mathbb{N}}(x,y)^n/(x,y)^{n+1}=\mathrm{Proj}\,k[x,y]=\mathbb{P}^1$.

b) $\pi^{-1}(U_x)=\mathrm{Proj}\,A_x=\mathrm{Proj}\bigoplus_{n\in\mathbb{N}}A_x=\mathrm{Proj}\,A_x[t]=\mathrm{Spec}\,A_x=U_x$. Igualmente, se tiene que $\pi^{-1}(U_y)=U_y$.

c) $A=k[x,y]\oplus(x,y)t\oplus\cdots\oplus(x,y)^nt^n\oplus\cdots\subset k[x,y,t]$, $\tilde{x}=xt$ y $A=k[x,y][xt,yt]$. $\mathrm{Proj}\,A_{xt}=\mathrm{Spec}\,A[\frac{yt}{xt}]=\mathrm{Spec}\,k[x,y/x]$.

P9. Si $V=\mathrm{Proj}\,k[x_0,\dots,x_n]/I$ denotemos $\hat{V}=\mathrm{Spec}\,k[x_0,\dots,x_n]/I$. $\hat{X}\cap\hat{Y}\neq\emptyset$ porque $or\in\hat{X}\cap\hat{Y}$ (donde $\mathfrak{m}_{or}=(x_0,\dots,x_n)\subset k[x_0,\dots,x_n]$). $\hat{Z}$ es una componente irreducible de $\hat{X}\cap\hat{Y}$, y por el problema 19 del capítulo 3,

$$\mathrm{codim}\,\hat{Z}\leq\mathrm{codim}\,\hat{X}+\mathrm{codim}\,\hat{Y}.$$

Se concluye porque $\dim\hat{Z}=\dim Z+1$, luego $\mathrm{codim}\,\hat{Z}=\mathrm{codim}\,Z$.

P10. El conjunto de rectas que pasan por (α,β) es el conjunto de rectas de ecuaciones $\lambda(x-\alpha)+\mu(y-\beta)=0$, donde la recta $\lambda(x-\alpha)+\mu(y-\beta)=0$ es la misma que $\gamma\lambda(x-\alpha)+\gamma\mu(y-\beta)=0$ (y no consideramos el caso $\lambda=\mu=0$). Así pues, el haz de rectas que pasa por (α,β) está en correspondencia biunívoca con los puntos racionales de $\mathrm{Proj}\,k[x,y]$.

P11. Si tres de los puntos están alineados, entonces toda cónica que pase por esos tres puntos contendrá a la recta r que pasa por los tres puntos, luego las cónicas que pasan por los cuatro puntos serán iguales a la recta r unión otra recta que

pasa por el cuarto punto. Luego, el conjunto de cónicas que pasan por los cuatros puntos está en correspondencia biunívoca con el haz de rectas que pasa por el cuarto punto.

Supongamos que ninguna terna de puntos de los cuatro están alienados. Si $p_2(x,y)=0$ y $q_2(x,y)=0$ son dos cónicas distintas que pasan por los cuatro puntos, y p es un punto punto que no pertence a ninguna de las cónicas, entonces existe (λ,μ) no nulo, único salvo multiplicación por invertibles, tales que $\lambda p_2+\mu q_2=0$ es una cónica que pasa por el punto p. Además existe una única cónica que pasa por los cuatro puntos y p (dos cónicas sin componente comunes se cortan en cuatro puntos). Así pues, el haz de cónicas que pasan por cuatro puntos, se corresponde biunívocamente con el haz de cónicas $\{\lambda p_2+\mu q_2=0\}$ que es biyectivo con los puntos racionales de $\operatorname{Proj} k[x,y]$.

P12. Tenemos dos puntos p_1,p_2 y una recta r que pasa por un tercer punto p_3. Si r pasa por p_1, entonces toda cónica del enunciado ha de contener a r, luego es la unión de r con una recta que pasa por p_2. Luego, el conjunto del enunciado está en correspondencia biunívoca con el haz de rectas que pasa por p_2.

Podemos suponer que r no pasa ni por p_1, ni por p_2. Sea r' la recta que pasa por p_1 y p_2, r_1 la recta que pasa por p_1 y p_3 y r_2 la recta que pasa por p_2 y p_3. Tenemos $r\cup r'\equiv p_2(x,y)=0$ y $r_1\cup r_2\equiv q_2(x,y)=0$. El conjunto del enunciado es el conjunto de cónicas de ecuaciones $\lambda p_2+\mu q_2=0$, que es biyectivo con los puntos racionales de $\operatorname{Proj} k[x,y]$.

P13. Estamos considerando el conjunto de ecuaciones $p(x_1,x_2,x_2)=0$ (salvo multiplicación por escalares), con $p(x_1,x_2,x_3)=\sum_{|\alpha|=n} x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$, que es biyectivo con los puntos racionales de $\operatorname{Proj} k[x_\alpha]_{|\alpha|=n}$.

P14. Sea $p(x_1,x_2)=0$ una curva plana de grado menor o igual que n, entonces $p(x_1,x_2)=\sum_{|\alpha|\le n} a_\alpha x^\alpha$, salvo multiplicación por escalares y además no se cumple que $a_\alpha=0$, para todo $\alpha\neq 0$. Luego, el conjunto es biyectivo con $\operatorname{Proj} k[x_\alpha]_{|\alpha|\le n}-p$, donde $p=[(\lambda_\alpha)]$ es el punto de coordenadas $\lambda_\alpha=0$, para todo $\alpha\neq 0$.

P15. Las curvas planas afines de grado n, $p(x_1,x_2)=\sum_{|\alpha|\le n} a_\alpha x^\alpha=0$ se corresponden con los puntos racionales del abierto de $\operatorname{Proj} k[x_\alpha]_{|\alpha|\le n}$, $U_n:=\cup_{|\alpha|=n}U^h_{x_\alpha}$, que es de dimensión $\binom{n+2}{2}-1$. Sea $n=r+r'$, $|\beta|=r$, $|\beta'|=r'$, $\alpha=\beta+\beta'$, $U^h_{x_\beta}\subset U_r$ y $U^h_{x_{\beta'}}=U_{r'}$ los abiertos obvios. El morfismo $U^h_{x_\beta}\times U^h_{x_{\beta'}}\to U^h_{x_\alpha}\subset U_n$, $(a_\gamma,b_{\gamma'})\mapsto(c_\alpha)$, donde $c_\alpha=\sum_{\gamma+\gamma'=\alpha}a_\gamma\cdot b_{\gamma'}$, en los puntos racionales, asigna a cada pareja de polinomios su producto. El cierre de la imagen, $C_{\beta,\beta'}$, es de dimensión menor o igual que

$\binom{r+2}{2}-1+\binom{s+2}{2}-1<\binom{n+2}{2}-1$. Por tanto, $U_n-\cup_{\beta,\beta'}C_{\beta,\beta'}$ es un abierto no vacío de U_n de "curvas irreducibles"

P16. Denotemos $m=\binom{n}{2}-1$.

a) Los puntos racionales de $\mathrm{Proj}\,k[a_{ijk}]_{i+j+k=n-2}=\mathbb{P}^m$ se corresponden biyectivamente con las curvas planas de grado $n-2$ o menos. Cada punto $p=(\alpha,\beta,\gamma)$ del plano define el hiperplano $H_p=(\sum\alpha^i\beta^j\gamma^k a_{ijk})_0$ de curvas planas de grado menor o igual que $n-2$ que pasa por p. La intersección de m hiperplanos es no vacía.

b) Tenemos que probar que en general los m hiperplanos considerados se cortan en un único punto. Es decir, que sus coordenadas son linealmente independientes. Tomemos todos los puntos, con coordenada $\gamma\neq 0$. Los puntos racionales del abierto $U_f\subset(\mathbb{A}^2)^m$ cumplen lo requerido, donde

$$f=\begin{vmatrix} x_1^{n-2} & x_1^{n-3}y_1 & x_1^{n-3} & \cdots & 1\\ \vdots & \vdots & \vdots & & \vdots\\ x_m^{n-2} & x_m^{n-3}y_m & x_m^{n-3} & \cdots & 1\end{vmatrix}$$

c) Sea $g\colon U_f\to\mathbb{P}^m$, la aplicación que asigna a $q=(p_1,\ldots,p_{m-1})\in U_f$ la única curva plana $c_q=0$ de grado $n-2$ que pasa por ellos. Tomando un abierto afín $V\subset U_f$ conveniente podemos suponer que $g_{|V}$ valora en $\mathbb{A}^m$. Sea $h\colon V\times\mathbb{A}^2\to\mathbb{A}^1$, $h(q,p)=c_q(p)$. Entonces, U_h es un abierto de $\binom{n}{2}$ puntos en posición general.

P17. Las rectas que pasan por el origen cortan a la curva (llamémosla C) cinco veces en el origen y en otro punto. Asignemos a cada recta del haz de rectas que pasa por el origen este otro punto. La recta $y=tx$ corta a la curva en $x^6-x^5t^3-x^5t^5=x^5(x-t^3-t^5)$, luego $x=t^5+t^3$ e $y=t^6+t^4$. La aplicación $\mathbb{A}^1-(t^5+t^3)_0\to C-\{(0,0)\}$, $t\mapsto(t^5+t^3,t^6+t^4)$ es isomorfismo. Los puntos de C de coordenadas (t^5+t^3,t^6+t^4) son los puntos racionales.

P18. a) La recta que pasa por el punto singular y otro punto, corta a la cónica en al menos tres puntos (contando grados y multiplicidades). Por el teorema de Bezout, la recta es una componente de la cónica.

b) La recta que pasa por los dos puntos singulares corta a la cónica en al menos cuatro puntos (contando grados y multiplicidades). Por el teorema de Bezout, la recta es una componente de la cúbica.

c) La cónica que pasa por los cuatro puntos singulares y un quinto punto corta a la cuártica en al menos nueve puntos (contando grados y multiplicidades). Por el teorema de Bezout, la cónica es una componente de la cuártica.

P19. Evidentemente $(0,0)$ es un punto singular. Si derivamos respecto de x y por y, obtenemos

$$y(x+y-2)+xy-2(x^2+y^2-2x-2y)(2x-2)=0$$
$$x(y+x-2)+xy-2(x^2+y^2-2x-2y)(2y-2)=0$$

Los tres puntos son soluciones de este sistema de ecuaciones, luego son singulares. La parte homogénea de grado mínimo de la cuártica es $-2xy-(2x+2y)^2=-4x^2-4y^2-10xy=-2(2x+y)(x+2y)$, luego las rectas tangentes a la cuártica en $(0,0)$ son $x+2y=0$ y $2x+y=0$. Consideremos el haz de cónicas que pasan por los puntos $(0,0)$, $(2,0)$ y $(0,2)$ y en el origen son tangentes a la recta $x+2y=0$:

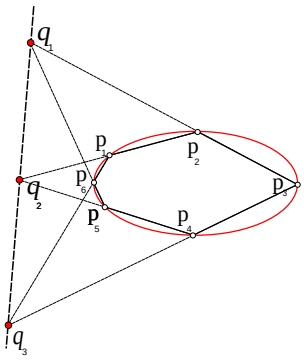
$$\{\lambda xy+\mu(x+y-2)(x+2y)=0\}$$

Cada cónica de este haz corta a la cuártica tres veces en $(0,0)$, dos veces en $(2,0)$, dos veces en $(0,2)$ y en un octavo punto (por el teorema de Bezout). Calculemos este octavo punto. Calculemos las soluciones de $\lambda xy+(x+y-2)(x+2y)=0$ y $xy(x+y-2)-(x^2+y^2-2x-2y)^2=0$. Considéremoslos como polinomios en x y calculemos el resto de dividir la cuártica por el primer polinomio. El cual es un polinomio en x de grado 1, podemos despejar (o eliminar) la x y calcular x e y. Obtendremos siete soluciones conocidas (con repeticiones) y la octava es

$$x=\frac{3(48+43\lambda+12\lambda^2+\lambda^3)}{(10+6\lambda+\lambda^2)^2}$$
$$y=\frac{-3(24+35\lambda+15\lambda^2+2\lambda^3)}{(10+6\lambda+\lambda^2)^2}$$

P20. Las dos circunferencias se cortan contando multiplicidades en cuatro puntos. No se cortan en ningún punto afín, luego se cortan en uno de los dos puntos del infinito de $x^2+y^2-1=0$ en los dos, y no pueden cortarse transversalmente.

P21. Teorema de Pascal.

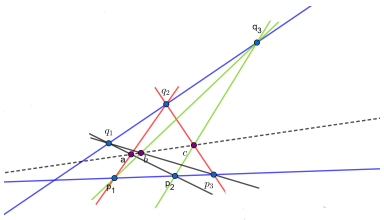


Sea $(q_2)_0^h=C_2$ la cónica, $p_1,\dots,p_6$ los seis vértices del hexágono, p_ip_j la recta que pasa por los puntos p_i y p_j, $(q_3)_0^h=C_3=p_1p_2\cup p_3p_4\cup p_5p_6$ y $(q_3')_0^h=C_3'=p_1p_6\cup p_2p_3\cup p_4p_5$. Podemos suponer que los vértices del hexágono están en el plano afín $U_{x_0}^h$. C_3 y C_2 se cortan transversalmente en los puntos $p_1,\dots,p_6$. Luego, $\mathfrak{m}_{p_i}\mathcal{O}_{\mathbb{P}^2,p_i}=(\frac{q_3}{x_0^3},\frac{q_2}{x_0^2})_{p_i}$. Por el teorema de Max Noether,

$$q_3'=a\cdot q_3+b\cdot q_2.$$

donde b es un polinomio de grado 1. $C_3\cap C_3'=\{p_1,\dots,p_6,q_1,q_2,q_3\}=C_3\cap(\{b=0\}\cup C_2)$, de lo que se deduce $\{q_1,q_2,q_3\}=p_1p_2\cap p_3p_4\cup p_2p_3\cap p_5p_5\cup p_1p_6\cap p_3p_4$ yacen en $\{b=0\}$.

P22. Teorema de Pappus.



Sea $(q_2)_0^h = R_1 \cup R_2$, $(q_3)_0^h = C_3 = R_{12} \cup R_{23} \cup R_{31}$ y $(q_3')_0^h = C_3' = R_{21} \cup R_{32} \cup R_{13}$. C_3 y C_2 se cortan transversalmente en los puntos $P = \{p_1, p_2, p_3, q_1, q_2, q_3\}$. Luego, $\mathfrak{m}_p \mathcal{O}_{\mathbb{P}^2,p} = (\frac{q_3}{x_0^3}, \frac{q_2}{x_0^2})_p$, para todo $p \in P$. Por el teorema de Max Noether,

$$q_3' = s \cdot q_3 + t \cdot q_2,$$

donde t es un polinomio homogéneo de grado 1.

$$P \coprod \{a,b,c\} = C_3 \cap C_3' = C_3 \cap (\{t=0\} \cup C_2),$$

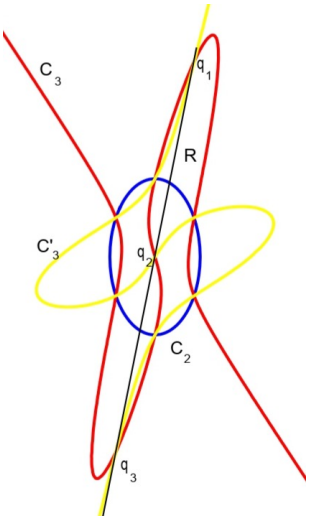
de lo que se deduce que $\{a,b,c\}$ yacen en $\{t=0\}$.

P23. La operación, denotemosla $*$, es conmutativa p_0 es el elemento neutro. Tenemos que probar que es asociativa. Denotemos aba' la recta que pasa por los puntos $a,b \in C$ y donde a' es el tercer punto de corte de abc con C. Para calcular $(a*b)*c$, realizamos las operaciones $R_1 = aba'$, $R_2 = a'p_0a''$, $R_3 = a''ca'''$, $a'''p_0a''''$ y $(a*b)*c = a''''$. Para calcular $a*(b*c)$, realizamos las operaciones $S_1 = bcb'$, $S_2 = b'p_0b''$, $S_3 = b''ab'''$, $b'''p_0b''''$. Tenemos que ver que $a'''' = b''''$, luego que $a''' = b'''$. Sea $C = (p_3)_0$, $C_3' = R_1 \cup R_3 \cup S_2 = (p_3')_0$ y $C_2 = S_1 \cup R_2 = (p_2)_0$. Por el teorema de Max Noether, $p_3' = \lambda p_3 + r \cdot p_2$, donde r es un polinomio homogéneo de grado 1. Entonces,

$$\begin{aligned} a+b+a'+b'+p_0+b''+a''+c+a''' = C_3' \cap C &= (\{r=0\} \cup C_2) \cap C \\ &= \{r=0\} \cap C + b + c + b' + a' + p_0 + a''. \end{aligned}$$

Luego, $\{r=0\} \cap C = a + b'' + a'''$, $\{r=0\} = S_3$ y $a''' = b'''$.

P24.



Sean $C_3=(p_3)_0$, $C_3'=(p_3')_0$ y $C_2=(q_2)_0$ la cónica. Denotemos $C_3\cap C_2=p_1+\cdots+p_6$ y $C_3\cap C_3'=p_1+\cdots+p_6+q_1+q_2+q_3$. Por el teorema de Max Noether $p_3'=ap_3+bq_2$, donde a es una constante y b es un polinomio homogéneo de grado 1. Sea $R=(b)_0$ Como

$$\begin{aligned}p_1+\cdots+p_6+q_1+q_2+q_3=C_3\cap C_3'&=C_3\cap(R\cup C_2)\\&=(C_3\cap R)+p_1+\cdots+p_6,\end{aligned}$$

se deduce que q_1,q_2,q_3 yacen en la recta R.

P25. Sea $C_3=(p_3)_0$ la cúbica. Sea $R=(a)_0$ la recta que pasa por los tres puntos alineados p_1,p_2,p_3 de C_3. Sea $T_i=(b_i)_0$ la tangente a C_3 en p_i y $C_3'=(b_1b_2b_3)_0=T_1\cup T_2\cup T_3$. $C\cap(a^2)_0=2p_1+2p_2+2p_3$. Por el teorema de Max Noether, $b_1b_2b_3=\lambda p_3+ba^2$, donde b es un polinomio homogéneo de grado 1. Entonces,

$$\begin{aligned}2p_1+2p_2+2p_3+q_1+q_2+q_3=C_3\cap C_3'&=C_3\cap(\{b=0\}\cup C_2)\\&=C_3\cap\{b=0\}+2p_1+2p_2+2p_3.\end{aligned}$$

Luego q_1,q_2,q_3 yacen en la recta $b=0$.

P26. Sean R_1, R_2, R_3 las rectas del triángulo, p_i los vértices del triángulo y T_i la tángente a la cónica en p_i. Sea $C_3=R_1\cup R_2\cup R_3=(p_3)_0$, $C_3'=T_1\cup T_2\cup T_3=(p_3')_0$ y $C_2=(p_2)_0$ la cónica. Por el teorema de Max Noether, $p_3=ap_3'+bp_2$, donde b es un polinomio homogéneo de grado 1. Entonces,

$$\begin{aligned}2p_1+2p_2+2p_3+q_1+q_2+q_3=C_3\cap C_3'&=C_3\cap(\{b=0\}\cup C_2)\\&=C_3\cap\{b=0\}+2p_1+2p_2+2p_3.\end{aligned}$$

y q_1,q_2,q_3 yacen en la recta $b=0$.

P27. Sean p_1,p_2 los dos puntos de inflexión, T_1 y T_2 las tangentes a la cúbica en p_1 y p_2 respectivamente y $R=(a)_0$ la recta que pasa por p_1 y p_2 (y corta en un tercer punto p_3). Sea $C_3=(p_3)_0$ la cúbica, $C_2=T_1\cup T_2=(p_2)_0$ y $C_3'=(a^3)_0$. Por el teorema de Max Noether, $a^3=\lambda p_3+bp_2$, donde b es un polinomio homogéneo de grado 1. Entonces,

$$3p_1+3p_2+3p_3=C_3\cap C_3'=C_3\cap(\{b=0\}\cup C_2)=C_3\cap\{b=0\}+3p_1+3p_2$$

Por tanto, $b=0$ es tangente a C_3 en p_3 y corta con multiplicidad 3.

P28. Sea $C_3=(p_3)_0$, $C_3'=(p_3')_0$ y $C_3''=(p_3'')_0$ las tres cúbicas. Sea $C_3'\cap C_3''=\{p_1,\dots,p_9\}$ y $\{p_1,\dots,p_8,q\}\subset C_3'\cap C_3$. Sea $R=(a)_0$ la recta tangente a C_3' en p_9 y $C_3'\cap R=2p_9+q'$. Por el teorema de Max Noether, $ap_3=a'p_3'+a''p_3''$, con a' y a'' polinomios homogéneos de grado 1. Entonces,

$$\begin{aligned}p_1+\cdots+p_8+q+2p_9+q' &= (C_3\cup R)\cap C_3' = (\{a''=0\}\cup C_3'')\cap C_3'\\ &= p_1+\cdots+p_9+\{a''=0\}\cap C_3'.\end{aligned}$$

Luego, $\{a''=0\}\cap C_3'=\{q,p,q'\}$ y $a''=a$ (salvo multiplicación por un escalar), entonces $a'=a$ (salvo multiplicación por un escalar). Por lo tanto, dividiendo por a, $p_3=\lambda p_3'+\mu p_3''$, con λ,μ constantes. Por tanto, $p_9\in C_3$.

P29. Escribamos $\{p_1,\dots,p_{dd'}\}=C_d\cap C_{d'}$. Denotemos $m=\binom{d+d'-k-1}{2}$ y según el enunciado suponemos que C_k pasa por $\{p_{m+1},\dots,p_{dd'}\}$. Sea $i\le m$ y $D=(q)_0$ la curva de grado $d+d'-k-3$ que pasa por $\{p_1,\dots,\widehat{p_i},\dots,p_m\}$, luego no pasa por p_i. Sea R una recta que pase por p_i y corte trnsversalmente a C_d, luego $C_d\cap R=p_i+q_1+\cdots+q_{d-1}$. Denotemos $C_j=(p_j)_0^h$ y $R=(p_1)_0^h$. Consideremos la curva $C_k\cup D\cup R$. Por el teorema de Max Noether $p_k\cdot q\cdot p_1=ap_d+bp_{d'}$, donde b es un polinomio homogéneo de grado $d-2$. Entonces,

$$\begin{aligned}p_1+\cdots+p_{dd'}+q_1+\cdots+q_{d-1}+\cdots &= (C_k\cup D\cup R)\cap C_d = \{b=0\}\cap C_d+(C_{d'}\cap C_d)\\ &= \{b=0\}\cap C_d+p_1+\cdots+p_{dd'}\end{aligned}$$

Entonces, $q_1,\dots,q_{d-1}\in\{b=0\}$ y por grados $R\cap\{b=0\}=R$. Por tanto, p_1 divide a b, luego a a y tenemos que $p_k\cdot q=a'p_d+b'p_{d'}$. Por tanto, p_i es un punto de C_k.

Solución de los problemas del capítulo quinto

P1. $(0)=(\bar{x})\cap(\bar{y})$, $(\bar{x})\subset A$ es irreducible porque $(0)\subset A/(\bar{x})=k[y]/(y^2)$ es irreducible, igualmente $(\bar{y})\subset A$ es irreducible. El ideal $(0)\subset A$ es primario porque su radical es un ideal maximal.

P2. Si el proceso no termina en número finito de pasos, entonces no termina en número finito de pasos para I_1 o I_2. Digamos que para I_1. Entonces, $I=J_1\cap J_2$, con J_1 y J_2 dos ideales estrictamente mayores que I_1. De nuevo, podemos decir que el proceso no termina en un número finito de pasos para J_1. Así sucesivamente obtenemos una cadena de inclusiones estrictas infinita $I\subset I_1\subset J_1\subset\cdots$, lo cual es contradictorio porque A es noetheriano.

P3. $(x)\cap(x,y)^2=(x)\cap(x^2,xy,y^2)=(x^2,xy)=(x)\cap(y,x^2)$. Hemos obtenido dos descomposiciones primarias reducidas distintas.

P4. Si $I = \mathfrak{p} \cap \mathfrak{m}^2$ fuese primario, entonces los primos asociados a I serían $\mathfrak{p}$ y $\mathfrak{m}$, por un lado y $r(I)$ por otro. Lo cual es contradictorio.

P5. $(60) = (5) \cap (2^2) \cap (3)$.

P6. Si $I \subset A$ es un ideal, entonces $(I) = I \oplus I \cdot X \oplus \cdots \oplus I \cdot x^n \oplus \cdots$ y $A[x]/(I) = A/I[x]$. Evidentemente, $(\mathfrak{p}) \subseteq r((\mathfrak{q}))$ y se tiene la igualdad porque $A[x]/(\mathfrak{p}) = A/\mathfrak{p}[x]$ es íntegro. Tenemos que probar que los divisores de cero de $A[x]/(\mathfrak{q}) = A/\mathfrak{q}[x]$ son nilpotentes. Podemos suponer que $\mathfrak{q} = 0$. Entonces, $\mathrm{rad}(A) = \mathfrak{p}$ y $\mathrm{rad}(A[x]) = (\mathfrak{p})$. Supongamos $(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{j=0}^{m} b_j x^j) = 0$, con $a_n, b_m \neq 0$. Como $A[x]/(\mathfrak{p})$ es íntegro, podemos suponer que $\sum_{j=0}^{m} b_j x^j \in (\mathfrak{p})$. Tenemos que probar que $\sum_{i=0}^{n} a_i x^i \in (\mathfrak{p})$. Observemos que $a_n \cdot b_m = 0$, luego $a_n \in \mathfrak{p}$. Sea $r \geq 0$ máximo tal que $a_n^r \cdot (\sum_i b_i x^i) \neq 0$. Entonces, $(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{j=0}^{m} a_0^r b_j x^j) = 0$ y $(\sum_{i=0}^{n-1} a_i x^i) \cdot (\sum_{j=0}^{m} a_0^r b_j x^j) = 0$. De nuevo, obtendremos que $a_{n-1} \in \mathfrak{p}$, etc.

P7. Obviamente, $r(\mathfrak{q}) = r(y^2, z^3) = (y, z) = \mathfrak{p}$. El ideal $(y^2, z^3) \subset k[y, z]$ es primario porque su radical es un ideal maximal, Por el problema 6, $\mathfrak{q}$ es primario. Evidentemente, $r((y^2, xy, z^3)) = \mathfrak{p}$ y $xy \in (y^2, xy, z^3)$, $x \notin \mathfrak{p}$ e $y \notin (y^2, xy, z^3)$, luego no es primario.

P8. Sea r tal que $\mathfrak{m}_x^r \subset \mathfrak{q}_1$. $I_x = \mathfrak{q}_{1,x}$, luego

$$A/(I + \mathfrak{m}_x^{r+1}) = (A/(I + \mathfrak{m}_x^{r+1}))_x = A_x/(\mathfrak{q}_{1,x} + \mathfrak{m}_x^{r+1} A_x) = A_x/\mathfrak{q}_{1,x}$$

y $\overline{\mathfrak{m}_x^r} = 0$ en $A/(I + \mathfrak{m}_x^{r+1})$.

Si $\overline{\mathfrak{m}_x^r} = 0$ en $A/(I + \mathfrak{m}_x^{r+1})$, entonces $\overline{\mathfrak{m}_x^r} = \overline{\mathfrak{m}_x^{r+1}}$ en A/I, luego en $(A/I)_x = A_x/\mathfrak{q}_{1,x}$. Luego, $\overline{\mathfrak{m}_x^r} = \overline{\mathfrak{m}_x^N} = 0$ en $A_x/\mathfrak{q}_{1,x}$. Entonces, $\mathfrak{m}_x^r A_x \subset \mathfrak{q}_{1,x}$, $(I + \mathfrak{m}_x^r)_x \subset \mathfrak{q}_{1,x}$ y $I + \mathfrak{m}_x^r \subset \mathfrak{q}_1$. Por tanto, $I = (I + \mathfrak{m}_x^r) \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$.

P9. $(I)_0 = (xy)_0 \cap (-y + x^2 + y^2)_0 = [(x)_0 \cap (-y + x^2 + y^2)_0] \cup [(y)_0 \cap (-y + x^2 + y^2)_0] = (x, -y + x^2 + y^2)_0 \cup (y, -y + x^2 + y^2)_0 = (x, -y + y^2)_0 \cup (y, x^2)_0 = \{(x, y), (x, y - 1)\}$. Por lo tanto, $I = (I + (x, y)^r) \cap (I + (x, y - 1)^s)$. Calculemos

Denotemos $A = \mathbb{C}[x, y]/(x, y-1)^2$. Luego, $\mathbb{C}[x, y]/I + (x, y-1)^2 = A/(xy, -y+x^2+y^2) = A/(x, -y + x^2 + y^2) = A/(x, y(y - 1)) = A/(x, y - 1)$. Por lo tanto, $\overline{(x - y - 1)} = 0$ en $\mathbb{C}[x, y]/I + (x, y - 1)^2$ y $s = 1$.

Denotemos $A = \mathbb{C}[x, y]/(x, y)^4$. Entonces, $\mathbb{C}[x, y]/I + (x, y)^4 = A/(-y + x^2 + y^2, xy) = A/(-y+x^2+y^2, xy, -yx+x^3+xy^2, -y^2+yx^2+y^3) = A/(-y+x^2+y^2, xy, x^3, -y^2+y^3) =$

$A/(-y+x^2+y^2, xy, -y^2+y^3, x^3, x^2y, xy^2, y^3)$, luego $\overline{(x,y)^3}=0$ en $\mathbb{C}[x,y]/I+(x,y)^4$ y $r=3$. En conclusión, $I=(x,y-1)\cap(I+(x,y)^3)$.

P10. a) $(x,y)\cdot(x,y-1)=(x,y)\cap(x,y-1)$ porque son iguales al localizar en todo punto cerrado.

b) $(x)\cdot(x,y)=(x^2,xy)=(x)\cap(x,y)^2$. Igualmente, $(x)\cdot(x,y-1)=(x)\cap(x,y-1)^2$. Por tanto, $(x)\cdot(x,y)\cap(x,y-1)=(x^2,xy)=(x)\cap(x,y)^2\cap(x,y-1)^2$, porque son iguales al localizar en todo punto cerrado.

P11. a) $(xy)+(x+y+1)=(xy,x+y+1)=(x,x+y+1)\cap(y,x+y+1)$ porque localmente son iguales.

b) $(x^2)+(y)=(x^2,y)$ que es primario.

c) $(x^2+y^2-1,x)=(y^2-1,x)=(y-1,x)\cap(y+1,x)$ porque localmente son iguales.

d) $(x^2+y^2-1,xy)=(x^2+y^2-1,x)\cap(x^2+y^2-1,y)=(x,y-1)\cap(x,y+1)\cap(y,x-1)\cap(y,x+1)$ porque localmente son iguales.

e) $(x^2+y^2-1,x^2)=(x^2,y^2-1)=(x^2,y-1)\cap(x^2,y+1)$ porque localmente son iguales.

P12. a) $\bar{b}\cdot\bar{J}=0$ si y solo si $b\cdot J\subset I$.

b) Sea $\frac{a}{s}\in(I:J)_S$, con $a\in(I:J)$ y $s\in S$. Entonces, $a\cdot J_S=(a\cdot J)_S\subset I_S$ y $\frac{a}{s}\cdot J_S\subset I_S$ y $\frac{a}{s}\in(I_S:J_S)$. Si $\frac{a}{s}\in(I_S:J_S)$, entonces $a\cdot J\subset I_S$, entonces para ciert $s'\in S$, $s'a\cdot J\subset I$, luego $s'a\in(I:J)$ y $\frac{a}{s}=\frac{s'a}{s's}\in(I:J)_S$.

c) Es obvio. d) Obviamente, $(b_1,\ldots,b_r)+Kera\cdot\subseteq(I:a)$. Si $b\in(I:a)$, entonces $ba\in I\cap(a)$ y $ba=\sum_i ab_ic_i$. Luego, $a(b-\sum_i b_ic_i)=0$, $b-\sum_i b_ic_i\in(0:a)$ y $b\in(b_1,\ldots,b_r)+(0:a)$.

e) Si $i\leq m$, entonces $(\mathfrak{p}_i:\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m)=A$, Si $i>m$, observemos que $\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m\not\subseteq\mathfrak{p}_i$, porque en caso contrario $\mathfrak{p}_i\in(\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m)_0=\cup_{j\leq m}(\mathfrak{p}_j)_0$ y para algún $j\leq m$, $\mathfrak{p}_j\subseteq\mathfrak{p}_i$. Entonces $(\mathfrak{p}_i:\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m)=\mathfrak{p}_i$. Por tanto,

$$(\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n:\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m)=\bigcap_{i=1}^{n}(\mathfrak{p}_i:\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_m)=\bigcap_{i=m+1}^{n}\mathfrak{p}_i$$

f) $I=\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n$, donde $\mathfrak{p}_i$ son ideales primos tales que $\mathfrak{p}_i\not\subseteq\mathfrak{p}_j$ para todo $i\neq j$. Como $(\mathfrak{p}_i:J)=A$ si y solo si $J\subseteq\mathfrak{p}_i$ (es decir, $(\mathfrak{p}_i)_0\subseteq(J)_0$) y en otro caso $(\mathfrak{p}_i:J)=\mathfrak{p}_i$, entonces

$$(I:J)=\bigcap_{i=1}^{n}(\mathfrak{p}_i:J)=\bigcap_{(\mathfrak{p}_i)_0\not\subseteq(J)_0}\mathfrak{p}_i$$

y $(I:J)_0=\bigcup_{(\mathfrak{p}_i)_0\not\subseteq(J)_0}(\mathfrak{p}_i)_0$.

Solución de los problemas del capítulo sexto

P1. En efecto, tenemos que $R(P'(x),Q'(x)) = ((-1)^n \cdot a_0^2)^m \cdot ((-1)^m \cdot b_0^2)^n \cdot \prod_{i,j}(x_i^2 - y_j^2) = a_0^m b_0^n \prod_{i,j}(x_i - y_j) \cdot a_0^m b_0^n \prod_{i,j}(x_i + y_j) = R(P(x),Q(x)) \cdot R(P(x),Q(-x)) \cdot (-1)^{nm}$.

P2. Sea $y = x + \frac{1}{x} = \frac{x^2+1}{x}$, es decir, $x^2 - yx + 1 = 0$. Consideremos el sistema

$$\left.\begin{aligned} P(x) &= 0 \\ Q(x) = x^2 - yx + 1 &= 0 \end{aligned}\right\}$$

Las soluciones del sistema son $x = \alpha_i$, $y = \alpha_i + \frac{1}{\alpha_i}$. Luego las raíces de $R(y) := R(P,Q)$ son $y = \alpha_i + \frac{1}{\alpha_i}$. Las raíces de $Q(x)$ son $x, 1/x$ (con $y = x + 1/x$). Luego

$$\boxed{R(y) = P(x) \cdot P(\frac{1}{x})}$$

haciendo el cambio $x + \frac{1}{x} = y$ (o sustituyendo $x = \frac{y+\sqrt{y^2-4}}{2}$ y $\frac{1}{x} = \frac{y-\sqrt{y^2-4}}{2}$).

P3. La ecuación $x^5 - 1 = 0$ tiene por soluciones las raíces quintas de 1:

$$\varepsilon^k = cos\,\frac{2k\pi}{5} + sen\,\frac{2k\pi}{5}$$

con lo que

$$cos\,\frac{2k\pi}{5} = \frac{1}{2}(\varepsilon^k + \overline{\varepsilon}^k) = \frac{1}{2}(\varepsilon^k + \frac{1}{\varepsilon^k})$$

así que el sistema es

$$\left.\begin{aligned} x^5 - 1 &= 0 \\ y = \frac{1}{2}(x + \frac{1}{x}) & \end{aligned}\right\}$$

Siguiendo el problema 2, la resultante queda:

$$R(y) = (x^5 - 1)(\frac{1}{x^5} - 1) = -(x^5 + \frac{1}{x^5}) + 2$$

haciendo el cambio $2y = x + x^{-1}$. Elevando $x + x^{-1}$ a 5 y a 3 y después de un pequeño cálculo se obtiene:

$$R(y) = 16y^5 - 20y^3 + 5y - 1$$

Igualmente sabríamos calcular el polinomio de raíces $sen\,\frac{2k\pi}{5}$, con $k = 1,\ldots,5$, ya que $sen\,\frac{2k\pi}{5} = \frac{1}{2i}(\varepsilon^k - \varepsilon^{-k})$ y se aplica el método del problema 3.

P4. Es el polinomio $R(y)=P(x)\cdot P(-\frac{1}{x})$, haciendo el cambio $y=x-\frac{1}{x}$ (es decir sustituyendo $x=\frac{y+\sqrt{y^2+4}}{2}$ y $-\frac{1}{x}=\frac{y-\sqrt{y^2+4}}{2}$).

P5. Si x es solución de la ecuación $y=ax+\frac{b}{x}$, entonces $\frac{b}{ax}$ también y se concluye como en los en los problemas 2 y 4, que el polinomio buscado es $R(y)=P(x)\cdot P(\frac{b}{ax})$ haciendo $ax+\frac{b}{x}=y$ (es decir sustituyendo $x=\frac{y+\sqrt{y^2-4ab}}{2a}$ y $\frac{b}{ax}=\frac{y-\sqrt{y^2-4ab}}{2a}$).

P6. 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!).

P7. $R_0(x)=x^2+ax+b$, $R_1(x)=P'(x)=2x+a$, $R_2(x)=P(-\frac{a}{2})=-\frac{a^2}{4}+b$, luego $g_0=2,g_1=1,g_2=0$ y $d_0=1,d_1=2,d_2=-\frac{a^2}{4}+b$:

$$\Delta=(-1)^{\binom{2}{2}}\cdot R(P,P')=(-1)^{2\cdot1+1\cdot0}\cdot2^{2-0}(-\frac{a^2}{4}+b)^{1-0}=a^2-4b.$$

P8. $R_0(x)=x^3+px+q$, $R_1(x)=P'(x)=3x^2+p$, $R_2(x)=\frac{2}{3}px+q$ y por último $R_3(x)=R_2(-\frac{3}{2}\frac{q}{p})=\frac{3^3}{2^2}\frac{q^2}{p^2}+p$, luego $g_0=3,g_1=2,g_2=1,g_3=0$ y $d_0=1,d_1=3,d_2=\frac{2}{3}p,d_3=\frac{3^3}{2^2}\frac{q^2}{p^2}+p$:

$$\Delta=(-1)^{\binom{3}{2}}\cdot R(P,P')=-(-1)^{3\cdot2+2\cdot1+1\cdot0}\cdot3^{3-1}(\frac{2}{3}p)^{2-0}(\frac{3^3}{2^2}\frac{q^2}{p^2}+p)=-(4p^3+27q^2).$$

P9. Sea M el conjunto de los monomios de $k[x_1,\ldots,x_n]$. Para $n\gg0$, la aplicación $M\to\mathbb{N}^n$, $m\mapsto n\cdot(w_1(m),\ldots,w_n(m))$ es inyectiva, aditiva y el orden heredado en M, por el orden lexicográfico de $\mathbb{N}^n$ es el orden monomial definido en el problema.

El orden definido por $x_1,\ldots,x_n$ es el orden lexicográfico. El orden definido por $x_1+\cdot+x_n,x_1,x_2,\ldots,x_{n-1}$ es el orden lexicográfico homogéneo. El orden definido por $x_1+\cdot+x_n,x_1+\cdots+x_{n-1},\ldots,x_1$ es el orden lexicográfico inverso.

P10. a) $\langle g_1,\ldots,\hat{g}_i,\ldots,g_s\rangle\underset{\neq}{\subset}M$, si y solo si $\langle\text{máx}(g_1),\ldots,\hat{g}_i,\ldots,\text{máx}(g_s)\rangle\underset{\neq}{\subset}\text{máx}(M)$ y esto sucede si y solo si máx$(g_1),\ldots,$máx(g_s) es el sistema generador minimal de máx(M).

b) Sea $g_1,\dots,g_s$ una base de Gröbner minimal. Por el algoritmo de división de Buchberger, $g_i = \sum_{j\neq i} p_j\cdot g_j + r_i$, de modo que ningún término de r_i es divisible por ningún máx(g_j), para $j\neq i$ y máx(r_i) = máx(g_i). Entonces, $\{r_1,\dots,r_s\}$ es una base de Gröbner minimal reducida. Si hubiera otra $\{r'_1,\dots,r'_s\}$, podemos suponer máx(r'_i) = máx(r_i), para todo i, entonces todos los términos de $r_i - r'_i \in M$ no pertenecen a máx(M), luego $r_i - r'_i = 0$.

P11. a) $\bar{f} = \sum_i \bar{t}_i \in L/M$, donde t_i son términos que no pertenecen a máx$\,M$. Entonces, $f = g + \sum t_i$, con $g\in M$.

b) $0 = (g-g') + (r-r')$, entonces $g-g'\in M$ y máx$(g-g')$ = máx$(r'-r)\notin$ máx(M), esto es contradictorio, salvo que $g-g'=0$, luego $g=g'$ y $r=r'$.

P12. Calculemos la base de Gröbner del ideal $(y^3+xy+x^3, y^2x+2xy+3)$, con la ayuda del programa Mathematica:

GroebnerBasis[$\{y^3+xy+x^3, y^2x+2xy+3\},\{x,y\}$] =

$$\{y^9+6y^8+12y^7+8y^6-3y^5-12y^4-12y^3-27, 9x+y^7+4y^6+4y^5-3y^3-6y^2\}$$

El polinomio de Hilbert $h(n)$ de Spec$\,k[x,y]/(y^3+xy+x^3, y^2x+2xy+3)$ coincide con la función de Hilbert de Spec$\,k[x,y]/(y^9,y^7)$ = Spec$\,k[x,y](y^9)$. De la sucesión exacta

$$0\to k[x,y]\xrightarrow{y^7\cdot} k[x,y]\to k[x,y](y^7)\to 0$$

se tiene que $h(n) = h_{k[x,y]}(n) - h_{k[x,y]}(n-7) = \binom{n+2}{2} - \binom{n-5}{2} = 6n-9$. El polinomio de Hilbert $h(n)$ de Spec$\,k[x,y]/(y^3+xy+x^3, y^2x+2xy+3)$ coincide con $h_{k[x,y]/(x,y^9)} = 9$ y $h(n) = \dim_k k[x,y]/(y^3+xy+x^3, y^2x+2xy+3)$ para $n\gg 0$. Por tanto, el número de puntos de las dos curvas planas afines $y^3+xy+x^3=0$ y $y^2x+2xy+3=0$, contando grados y multiplicidades, es 9 (luego estás dos cúbicas no se cortan en ningún punto del infinito).

P13. Consideramos el ideal $(tI+(1-t)J)\subset k[t,x,y]$, entonces por la proposición 6.2.26, $I\cap J = (tI+(1-t)J)\cap k[x,y]$. Usando ahora el algoritmo de Buchberger obtenemos que $\{tx^2y, txy^2-xy^2, x^2y^2\}$ es una base de Gröbner de $(tI+(1-t)J)$ respecto del orden lexicográfico donde $t>x>y$. Luego, por la proposición 6.2.24, $\{x^2y^2\}$ es una base de Gröbner de $I\cap J = (tI+(1-t)J)\cap k[x,y]$ respecto del orden lexicográfico. Por consiguiente $I\cap J = (x^2y^2)$.

P14. Con la ayuda de la plataforma Singular, escribiendo

```
ring R = 0, (x,y,z), Dp;
ideal I = x^3*y-z^4, x^2-y^3;
std(I);
```

obtenemos que la base de Gröbner del ideal (x^3y-z^4, x^2-y^3) son los polinomios $\{y^3-x^2, x^3y-z^4, y^2z^4-x^5, yz^8-x^8, z^{12}-x^{11}\}$. El polinomio de Hilbert de la variedad algebraica afín coincide con el polinomio de Hilbert $h_A(n)$ de la variedad algebraica $\operatorname{Spec} k[x,y,z]/(y^3, x^3y, y^2z^4, yz^8, z^{12}) = \operatorname{Spec} A$. De la sucesión exacta

$$0 \to k[x,y,z]/(x^3, z^4, z^8, z^{12}) \xrightarrow{y^3\cdot} k[x,y,z]/(x^3y, y^2z^4, yz^8, z^{12}) \to A \to 0$$

obtenemos que $h_A(n) = h_{k[x,y,z]/(x^3y, y^2z^4, yz^8, z^{12})}(n) - h_{k[x,y,z]/(x^3, z^4)}(n-3)$. Por una parte,

$$h_{k[x,y,z]/(x^3,z^4)}(n) = h_{k[x,y,z]/(z^4)}(n) - h_{k[x,y,z]/(z^4)}(n-3) = \binom{n+3}{3} - \binom{n-1}{3} - \binom{n}{3} + \binom{n-4}{3}.$$

Por otra parte,

$$0 \to k[x,y,z]/(y) \xrightarrow{z^{12}\cdot} k[x,y,z]/(x^3y, y^2z^4, yz^8) \to k[x,y,z,w]/((x^3y, y^2z^4, yz^8, z^{12}) \to 0$$

obtenemos que $h_{k[x,y,z]/(x^3y, y^2z^4, yz^8, z^{12})}(n) = h_{k[x,y,z]/(x^3y, y^2z^4, yz^8)}(n) - h_{k[x,z]}(n-12) = h_{k[x,y,z]/(x^3y, y^2z^4, yz^8)}(n) - \binom{n-10}{2}$. Tenemos

$$h_{k[x,y,z]/((x^3y, y^2z^4, yz^8)}(n) = h_{k[x,y,z]/(x^3y, y^2z^4)}(n) - h_{k[x,y,z]/(x^3, y)}(n-9)$$

y $h_{k[x,y,z]/((x^3,y)}(n) = h_{k[x,z]}(n) - h_{k[x,z]}(n-3) = \binom{n+2}{2} - \binom{n-1}{2}$ y $h_{k[x,y,z]/(x^3y, y^2z^4)}(n) = h_{k[x,y,z]/(x^3y)}(n) - h_{k[x,y,z]/(x^3)}(n-6) = \binom{n+3}{3} - \binom{n-1}{3} - \binom{n-3}{3} + \binom{n-6}{3}$. Como la dimensión de la variedad algebraica es 1, entonces $h_A(n) = an + b$. Como $h_A(0) = -18$ y $h_A(1) = -6$ entonces $h_A(n) = -18 + 12n$.

Bibliografía

1. M.F. Atiyah, I.G. Macdonald. Introduction to Commutative Algebra,Addison-Wesley Series in Mathematics, Addison-Wesley Publishing Co., Inc., 1969.

2. D. Eisenbud, Commutative Algebra, with a View Toward Algebraic Geometry,GTM Springer, 1995.

3. R. Hartshorne, Algebraic Geometry. Graduate Texts in Mathematics, Springer-Verlag, New York, 1977.

4. S. Lang, Álgebra, Aguilar S.A. de ediciones, Madrid, 1971.

5. H. Matsumura. Commutative ring theory,Cambridge University Press, 1986.

6. J.S. Milne. Algebraic Geometry.http://www.jmilne.org/math/

7. J.A. Navarro. Álgebra Conmutativa Básica, Manuales UNEX, 19. Servicio de Publicaciones, Universidad de Extremadura, 1996. Versión on-line actualizada disponible en http://matematicas.unex.es/ navarro.

8. M. Reid. Undergraduate Commutative Algebra, London Mathematical Society, Students Texts 29, University Cambridge Press, 1995.

9. C. Sancho, P. Sancho. Álgebra Conmutatica. Geometría Algebraica. Manuales Uex online, 90. Servicio de Publicaciones, Universidad de Extremadura, 2013.

Índice alfabético

UNIVERSIDAD DE EXTREMADURA