Álgebra

Pedro Sancho de Salas

20-1-2004

Índice General

Capítulo 0

Introducción

Una definición de Matemáticas podría ser: "La Matemática estudia el concepto de espacio, es Geometría". Desde este punto de vista, la Topología es el estudio de los espacios topológicos, de las variedades topológicas, la Geometría Diferencial es el estudio de las variedades diferenciales, la asignatura de Variable Compleja el estudio de las variedades analíticas y el Álgebra el estudio de las variedades algebraicas. El análisis del espacio se funda en las funciones del espacio considerado. Así el fundamento de la Topología es el anillo de funciones continuas, de la Geometría Diferencial el anillo de las funciones infinito diferenciables, el de la Variable compleja el anillo de funciones analíticas o conformes y el del Álgebra el anillo de funciones algebraicas.

Una definición del Álgebra podría ser: "El estudio de los espacios definidos por sistemas de ecuaciones algebraicas". Así el primer problema que nos planteamos es ¿qué es un sistema de ecuaciones algebraicas? Podríamos responder que es dar r-polinomios $p_1(x_1,\dots,x_n),\cdots,p_r(x_1,\dots,x_n)\in\mathbb{C}[x_1,\dots,x_n]$ y escribimos el sistema

$$\begin{array}{l} p_1(x_1,\dots,x_n)=0\\ \cdots\\ p_r(x_1,\dots,x_n)=0 \end{array}$$

De modo inconsciente identificamos el sistema de ecuaciones algebraicas con el conjunto de soluciones del sistema de ecuaciones algebraicas, con "la variedad de soluciones". Por ello decimos que si al sistema de ecuaciones algebraicas anterior añadimos la ecuación $a_1\cdot p_1(x_1,\dots,x_n)+\cdots+a_rp_r(x_1,\dots,x_n)=0$ obtenemos el mismo sistema de ecuaciones algebraicas. En definitiva una definición mejor adaptada a nuestros propósitos inconscientes debería ser: "Un sistema de ecuaciones algebraicas es un ideal $(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))\subseteq\mathbb{C}[x_1,\dots,x_n]$"

Surgen, ahora, varias preguntas: ¿Todo ideal de $\mathbb{C}[x_1,\dots,x_n]$ está generado por un número finito de elementos? ¿Están los ideales de $\mathbb{C}[x_1,\dots,x_n]$ determinados por su variedad de soluciones?

La respuesta a la primera pregunta es afirmativa. Los anillos cuyos ideales son finito generados se denominan anillos noetherianos y, como decimos, los anillos de polinomios son anillos noetherianos, que estudiaremos en el curso.

La respuesta a la segunda pregunta es "no, pero casi sí". Observemos que las soluciones (sobre $\mathbb{C}$) del sistema $x_1=0$ son las mismas que $x_1^2=0$. Obviamente, dado un ideal $I\subseteq\mathbb{C}[x_1,\dots,x_n]$ si consideramos el ideal $r(I):=\{q\in\mathbb{C}[x_1,\dots,x_n]$, tales que $q^m\in I$, para algún $m\}$, entonces la variedad de soluciones de I es la misma que la de $r(I)$. El teorema de los ceros de Hilbert afirma que I e I' tienen la misma variedad de soluciones si y sólo si $r(I)=r(I')$, es decir, salvo "nilpotencias" los ideales están determinados por su variedad de soluciones. Decimos que un ideal I es radical si $r(I) = I$. Como $r(r(I)) = r(I)$, tenemos que hay correspondencia biunívoca entre variedades de soluciones e ideales radicales. Dado I, resulta que $r(I)$ es el ideal de todas los polinomios que se anulan en la variedad de soluciones de I.

Llamemos variedad algebraica a la variedad de soluciones de un ideal (radical). En el estudio de las variedades algebraicas un primer resultado inmediato es que una variedad V es irreducible, es decir, no es unión propia de dos variedades algebraicas, si y sólo si el ideal de todas las funciones que se anulan en V es un ideal primo. En general, toda variedad algebraica V es unión de un número finito de variedades algebraicas irreducibles. En términos de ideales, todo ideal radical es intersección de un número finito de ideales primos.

Puede parecernos que dado un ideal I es siempre mejor considerar $r(I)$ en vez de I. Pongamos un ejemplo sencillo en el que nos interese el ideal I: Consideremos el ideal $(x, y^2 - x)$ o el sistema

$$\begin{aligned} &x = 0 \\ &y^2 - x = 0 \end{aligned}$$

la variedad de soluciones de este sistema es el punto $x = 0, y = 0$. Tenemos que $I = (x, y^2 - x) = (x, y^2)$ y $r(I) = (x, y)$. Podemos pensar la variedad de soluciones dada, como el conjunto de puntos de corte de la recta $x = 0$ con la parábola $y^2 - x = 0$, y como esta recta es tangente a la parábola nos gustaría afirmar que la variedad de soluciones es "el origen contado dos veces". De esta afirmación "queda rastro" en el ideal I pero no en $r(I)$. En conclusión, cuando estudiamos el sistema de ecuaciones definido por I, si consideramos sólo el conjunto de soluciones del sistema de ecuaciones (o equivalentemente, consideramos sólo $r(I)$) perdemos información que puede ser esencial, sobre todo en una teoría fina de intersección de variedades.

El ideal $(x, y^2 - x)$ es el ideal de polinomios p tales que $p(0,0) = 0$ y $\frac{\partial p}{\partial y}(0,0) = 0$, que hemos expresado de modo más impreciso como ideal de funciones que se anulan dos veces en el origen. En general, demostraremos que los ideales I son los ideales de polinomios que se anulan en ciertas variedades irreducibles y cumplen ciertas condiciones infinitesimales (no preciso este concepto) a lo largo de estas variedades irreducibles. Si llamamos ideal primario al ideal de funciones que se anula en una variedad irreducible y cumple ciertas condiciones infinitesimales a lo largo de ella, el resultado fundamental de la teoría de descomposiciones primarias afirma que todo ideal es intersección de un número finito de ideales primarios. En conclusión, dar un sistema de ecuaciones algebraicas equivale a dar un número finito de variedades algebraicas irreducibles y condiciones infinitesimales a lo largo de ellas. Euclides se habría sorprendido si hubiese sabido que su Teorema de Euclides era la punta del iceberg de un teorema geométrico.

Una vez que hemos profundizado en el concepto de variedad algebraica surgen las preguntas ¿cuántas variedades algebraicas hay? ¿cómo distinguir dos variedades algebraicas? Nos planteamos la clasificación de las variedades algebraicas.

Un invariante obvio de las variedades algebraicas es la dimensión. Se dice que una variedad algebraica es de dimensión n si existe una cadena (de inclusiones estrictas) de subvariedades irreducibles $\emptyset = C_0 \subset C_1 \subset \cdots \subset C_n$ de longitud n y no existe ninguna otra de longitud mayor. Probaremos que la dimensión de una variedad algebraica es m si existe una proyección de fibras finitas y no vacías de la variedad en un espacio afín $\mathbb{A}^m(\mathbb{C})$. Veremos que el concepto de dimensión en variedades algebraicas irreducibles es local, y aún más, que todas las cadenas irrefinables de subvariedades irreducibles tienen la misma longitud. Por último, veremos que las hipersuperficies $f = 0$ de una variedad algebraica irreducible de dimensión m son de dimensión $m - 1$ y que todo punto de la variedad es (localmente) la solución de un sistema de m ecuaciones algebraicas y no menos. Todos estos resultados serán expresados en términos de los anillos de funciones algebraicas de la variedad y sus ideales primos.

En segundo lugar una propiedad geométrica distintiva de las variedades algebraicas es la existencia de puntos singulares. Por ejemplo el cono $x^2 + y^2 - z^2 = 0$ tiene como único punto singular el vértice y la esfera $x^2 + y^2 + z^2 = 1$ no tiene puntos singulares, es decir, es "lisa". En el curso estudiamos los conceptos de lisitud, módulo de diferenciales, derivaciones, cono tangente en un punto y daremos distintos criterios que caractericen los puntos singulares de una variedad. En el último capítulo, hacemos un estudio más detallado de las singularidades de una curva plana y damos el procedimiento para su desingularización, es decir, la obtención de una curva lisa a partir de una curva no lisa, de modo que ambas sean iguales fuera de los puntos singulares.

Puede decirse que la Geometría Algebraica Local se mueve dentro del marco afín y que la Geometría Algebraica Global dentro del marco proyectivo. Por ejemplo, el Teorema de Bezout que afirma que dos curvas planas proyectivas de grados n y m se cortan en $n \cdot m$ puntos (contando multiplicidades), es obviamente un enunciado no local y pertenece a la Geometría Algebraica Proyectiva. En el curso, definiremos las variedades proyectivas, veremos que todos los conceptos afines (esencialmente locales), como descomposición en componentes irreducibles, dimensión, lisitud etc, se extienden a las variedades proyectivas.

Capítulo 1

Anillos

1.1 Introducción

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

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

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

Desde Descartes, imaginamos tres ejes de coordenadas y todo punto del espacio viene definido por tres coordenadas. Los puntos vienen determinados por los valores de las funciones coordenadas en ellos. Además los objetos del espacio, por ejemplo un paraboloide, los solemos definir en implícitas. Dos objetos serán iguales si no los sabemos distinguir, es decir, con nuestra terminología, si no existe una función que valore distintamente en los dos objetos. Gauss, con la introducción de las coordenadas curvilíneas, permitió independizarnos de la elección arbitraria de las coordenadas cartesianas (inexistentes).

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

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

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

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

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

El lugar geométrico de un sistema de ecuaciones, como conjunto de soluciones del sistema, no recoge toda la información geométrica deseable, pero que sin embargo, sí que está en el anillo de funciones del objeto que define (o en el ideal definido).

Por ejemplo, si consideramos el sistema

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

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

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

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

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

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

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

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

Abundando en lo mismo, demos otro punto de vista. Observemos que las soluciones del sistema de ecuaciones $(*)$, con valores en una $\mathbb{R}$-álgebra A, se corresponden con los morfismos de $\mathbb{R}$-álgebras $\mathbb{R}[x_1, x_2, x_3]/I \to A$:

$$\begin{array}{rcl} \left\{ \begin{array}{c} \text{Soluciones } (a_1, a_2, a_3) \text{ del sistema} \\ p_1(x_1, x_2, x_3) = \cdots = p_r(x_1, x_2, x_3) = 0 \end{array} \right\} & \to & \mathrm{Hom}_{\mathbb{R}-\mathrm{alg}}(\mathbb{R}[x_1, x_2, x_3]/I, A) \\ (a_1, a_2, a_3) & \mapsto & \varphi\colon \bar{x}_i \mapsto a_i \end{array}$$

Si A es $\mathbb{R}$, se verifica que

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{R}-\mathrm{alg}}(\mathbb{R}[x_1, x_2, x_3]/I, \mathbb{R}) & = & \left\{ \begin{array}{c} \text{Ideales maximales de} \mathbb{R}[x_1, x_2, x_3]/I \\ \text{de cociente } \mathbb{R} \end{array} \right\} \\ \varphi & \mapsto & \mathrm{Ker}\, \varphi \end{array}$$

Si A es $\mathbb{C}$, se verifica que los morfismos de $\mathbb{R}$-álgebras de $\mathbb{R}[x_1, x_2, x_3]/I$ en $\mathbb{C}$, "salvo conjugación", se corresponden con los ideales maximales de $\mathbb{R}[x_1, x_2, x_3]/I$ (no lo vemos ahora). De nuevo, vemos la relación estrecha entre los ideales maximales de $\mathbb{R}[x_1, x_2, x_3]/I$ y el lugar geométrico de los puntos del sistema de ecuaciones $(*)$.

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

Tomamos como espacio todos los ideales primos y no sólo los maximales, por razones que se aclararán a lo largo del capítulo. Digamos ahora sólo que los ideales primos recogen mejor el concepto de primo (en el sentido del Lema de Euclides), que todo morfismo de anillos induce un morfismo entre los espectros (lo que no sucedería en general si sólo tomamos los ideales maximales) y que si una función se anula en todo primo entonces es nilpotente (lo que no sucede en general si sólo tomamos los ideales maximales). Además, hay una razón de índole topológica: Así como todo espacio topológico puede suponerse T_0, es decir, puede asignársele, de modo natural, un espacio T_0, también a todo espacio topológico puede asignársele un espacio topológico en el que cada cerrado irreducible (cerrados que no son unión de dos cerrados) es el cierre de un punto. Esto último es lo que hacemos en Geometría Algebraica cuando consideramos $\operatorname{Spec} A$ y no sólo el conjunto de los ideales primos maximales.

La teoría de ideales inicia el cumplimiento del sueño de Kronecker: la unificación de la Aritmética y la Geometría. Desde esta perspectiva los elementos de cualquier anillo conmutativo pueden entenderse como funciones sobre el espectro primo del anillo. Así, por ejemplo, los números enteros, los enteros de Gauss, etc., son verdaderas funciones y podemos aplicarles intuiciones y recursos geométricos. Los números primos podrán ser interpretados geométricamente como los puntos o subvariedades irreducibles de un espacio, etc.

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

1.2 Anillos. Ideales

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

1. Definición: Un anillo A es un conjunto con dos operaciones $A \times A \xrightarrow{+} A$, $(a, a') \mapsto a + a'$, $A \times A \xrightarrow{\cdot} A$, $(a, a') \mapsto a \cdot a'$, que denominamos suma y producto[1], tales que

1. A es un grupo abeliano con respecto a la suma (luego cumple la propiedad asociativa, tiene un elemento cero, que se denota por 0, y cada $a \in A$ tiene un opuesto que se denota por $-a$).

2. La multiplicación es asociativa ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$) y distributiva ($a \cdot (b + c) = a \cdot b + a \cdot c$).

   Además, sólo consideraremos anillos conmutativos con unidad, es decir, verificando

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

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

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

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

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

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

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

3. Definición : Una aplicación $f\colon A \to B$ 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. $f(1) = 1$.

4. Ejemplo : 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 $\tilde{\phi}\colon C(Y) \to C(X)$, $f \mapsto f \circ \phi$ es un morfismo de anillos.

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

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

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

Como I es un subgrupo de A, podemos considerar el grupo cociente A/I, donde

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

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

Dado un morfismo $f\colon A \to B$ de anillos, el núcleo de f, $\operatorname{Ker} f := \{a \in A \colon f(a) = 0\}$, es un ideal. Si $J \subseteq A$ es un ideal incluido en $\operatorname{Ker} f$, entonces existe un único morfismo de anillos $\bar{f}\colon A/J \to B$ (definido por $\bar{f}(\bar{a}) = f(a)$) de modo que el diagrama

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B \\ & A/J \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

es conmutativo, siendo π el morfismo de paso al cociente, $\pi(a) = \bar{a}$.

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. Es inmediata la proposición siguiente.

6. Proposición : *Sea $I \subseteq A$ un ideal y $\pi\colon A \to A/I$, $a \mapsto \bar{a}$ el morfismo de paso al cociente. Se verifica la correspondencia biunívoca*

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

$$J \longrightarrow \pi(J)$$

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

Sea S un sistema multiplicativo de A (es decir, $1 \in S$ y si $s, s' \in S$ entonces $s{\cdot}s' \in S$). Consideremos la localización de A por S, A_S, es decir,

$$A_S = \{\frac{a}{s},\ a \in A \text{ y } s \in S\colon\ \frac{a}{s} = \frac{a'}{s'} \text{ si existen un } t, t' \in S \text{ tales que } ta = t'a' \text{ y } ts = t's'\}^2$$

Con la suma y producto ordinarios de fracciones A_S es un anillo. Al morfismo natural de anillos $A \to A_S$, $a \mapsto \frac{a}{s}$ se le denomina morfismo de localización por S. El cual verifica la propiedad universal:

$$\mathrm{Hom}_{\text{Anillos}}(A_S, B) = \{f \in \mathrm{Hom}_{\text{Anillos}}(A, B)\colon\ f(s) \text{ es invertible en } B, \text{ para todo } s \in S\}$$

Ejemplos de localización son los cuerpos $\mathbb{Q} = \mathbb{Z}_{\mathbb{Z}-\{0\}}$ y $\mathbb{Q}(x) = \mathbb{Q}[x]_{\mathbb{Q}[x]-\{0\}}$.

Todo ideal de A_S es el ideal generado por la imagen de un ideal (o más) de A, pues $(\frac{a}{s}) = (\frac{a}{1})$.

7. Ejercicio : Probar que $I \subset A$ es un ideal que corta con el sistema multiplicativo S si y sólo si el ideal generado por la imagen de I en A_S es A_S.

1.3 Módulos

Los espacios vectoriales son el ejemplo más sencillo y usual de espacio geométrico. Muchos problemas se resuelven linealizándolos, lo que permite aplicarles además la intuición geométrica. Añadamos, que muchas de las estructuras usuales en Matemáticas son estructuras de espacios vectoriales.

Si I es un ideal de un anillo A, es un grupo conmutativo respecto de la suma de A y el producto de A define una aplicación $A \times I \to I$ que verifica todos los axiomas de espacio vectorial, salvo la condición de que los escalares formen un cuerpo; lo que resumiremos diciendo que I es un A-módulo. En esta sección iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (submódulos, cocientes, sumas y productos directos, producto tensorial, etc.) pueden generalizarse para los A-módulos; aunque la frecuente existencia de módulos que no admiten bases introduzca grandes modificaciones en la teoría de módulos. La posibilidad de efectuar muchas operaciones (cocientes, sumas directas, productos tensoriales, etc.) que carecen de sentido en los ideales hace que la teoría de módulos sea mucho más flexible y natural, que una teoría restringida únicamente a los ideales. Esta generalidad no complica las demostraciones, sino que la posibilidad de usar las operaciones básicas del Álgebra Lineal las aclara y simplifica.

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

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

Es decir, dada una aplicación $A \times M \xrightarrow{\cdot} M$, $(a,m) \mapsto a \cdot m$, 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. Los tres últimos puntos expresan que la aplicación $\phi\colon A \to \operatorname{End}(M)$, $\phi(a) = a\cdot$, es morfismo de anillos (donde $\operatorname{End}(M)$ son los endomorfismos de grupos del grupo conmutativo M). Recíprocamente, si M es un grupo conmutativo, cada morfismo de anillos $\phi\colon A \to \operatorname{End}(M)$ define una estructura de A-módulo en M tal que $a \cdot m := \phi(a)(m)$.

2. Ejemplo : 1. Todo ideal $I \subset A$ es un A-módulo, pues con la suma definida en A y con el producto por los elementos de A ya definido en A, I tiene estructura de A-módulo. En particular, A es un A-módulo.

2. Si A es un cuerpo, entonces los A-módulos son los A-espacios vectoriales.
3. Si G es un grupo abeliano, entonces es un $\mathbb{Z}$-módulo de modo natural: $n \cdot g = g + \overset{n}{\ldots} + g$ si $n \in \mathbb{N}^+$, $n \cdot g = (-g) + \overset{-n}{\ldots} + /(-g)$ 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.

Sea $\{M_i\}_{i\in I}$ una familia de A-módulos con índices en un conjunto I. Su producto directo se denotará $\prod\limits_{i\in I} M_i$, mientras que $\bigoplus\limits_{i\in I} M_i$ denotará el subconjunto de $\prod\limits_{i\in I} M_i$ 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 $\prod\limits_{i\in I} M_i$ como $\bigoplus\limits_{i\in I} M_i$ son A-módulos con la siguiente suma y producto por elementos de A:

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

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

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

4. Definición : Una aplicación $f\colon M \to M'$ entre A-módulos M, M', diremos que es un morfismo de A-módulos si cumple

1. $f(m+n) = f(m) + f(n)$, para todo $m,n \in M$.

2. $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

El conjunto de los elementos de un módulo M, que por un morfismo de A-módulos $f\colon M \to M'$ van al cero, se denomina núcleo de f y denota por $\operatorname{Ker} f$. Se cumple que $\operatorname{Ker} f$ es un submódulo de M y que f es inyectiva si y sólo si $\operatorname{Ker} f = 0$. El conjunto de los elementos de la imagen, $\operatorname{Im} f$, forman un submódulo de M'. Cuando f sea biyectiva diremos que f es un isomorfismo de A-módulos.

Denotaremos por $\operatorname{Hom}_A(M, N)$ al conjunto de morfismos de A-módulos de M en N. Con las definiciones de suma de morfismos y producto por elementos de A naturales:

$$(f+g)(m) := f(m) + g(m)$$
$$(af)(m) := a(f(m))$$

tenemos que $\operatorname{Hom}_A(M, N)$ es un A-módulo.

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

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

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

5. Ejercicio : Dado un epimorfismo $\pi\colon M \to M'$ de A-módulos, si π tiene sección (es decir, existe $s\colon M' \to M$ de modo que $\pi \circ s = \mathrm{Id}$) entonces $M \simeq \operatorname{Ker} \pi \oplus M'$. (Pista: Los morfismos $\operatorname{Ker} \pi \oplus M' \to M$, $(m, m') \mapsto (m + s(m'))$ y $M \to \operatorname{Ker} \pi \oplus M'$, $m \mapsto (m - s(\pi(m)), \pi(m))$ son inversos entre sí).

Dado un morfismo $i\colon N \to M$ inyectivo, si i tiene retracto (es decir, existe $r\colon M \to N$ de modo que $r \circ i = \mathrm{Id}$) entonces $M \simeq N \oplus M/N$. (Pista: Los morfismos $M \to N \oplus M/N$, $m \mapsto (r(m), \bar{m})$ y $N \oplus M/N \to M$, $(n, \bar{m}) \mapsto n + (m - r(m))$ son inversos entre sí).

6. Teorema : *Sea $f\colon M \to M'$ un morfismo de A-módulos. Sea $N \subseteq \operatorname{Ker} f$ un A-submódulo. Existe un único morfismo $\bar{f}\colon M/N \to M'$ (que vendrá definido por $\bar{f}(\bar{m}) = f(m)$) de modo que el diagrama*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\pi"'] & & M' \\ & M/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

es conmutativo, siendo π el morfismo de paso al cociente.

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

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & M' \\ M/\operatorname{Ker} f \arrow[r, equal, "\bar{f}"] & \operatorname{Im} f \arrow[u, hook, "i"'] \end{tikzcd}$$

donde $\pi(m) = \bar{m}$, $\bar{f}(\bar{m}) = f(m)$ (que está bien definida) e $i(m') = m'$, es conmutativo, $\bar{f}$ es un isomorfismo, π es epiyectiva e i inyectiva.

Demostración. Al lector. □

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

$$\sum_{i\in I} M_i = \{m \in M\colon m = \sum_{i\in I} m_i \\ \text{con } m_i \in M_i \text{ nulos para casi todo } i \in I\}$$

que es el menor submódulo de M que contiene a los submódulos M_i. Diremos que dos submódulos M_1, M_2 de M están en suma directa si $M_1 \cap M_2 = 0$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo. Se dice que M es la suma directa de dos submódulos M_1, M_2 si $M_1 \cap M_2 = 0$ y $M_1 + M_2 = M$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo.

Dado un conjunto $\{m_i\}_{i\in I}$ de elementos de un módulo M, denotaremos por

$$\langle m_i\rangle_{i\in I} = \{m \in M\colon m = \sum_{i\in I} a_i m_i, \\ \text{con } a_i = 0 \text{ para todo } i \text{ salvo un número finito}\}$$

que es el menor submódulo de M que contiene a $\{m_i\}_{i\in I}$. Diremos que $\{m_i\}_{i\in I}$ es un sistema generador de M si $\langle m_i\rangle_{i\in I} = M$. Evidentemente, todo módulo tiene sistemas generadores, por ejemplo el formado por todos los elementos de M. Si I es además finito diremos que el módulo es finito o finito generado. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M, si es un sistema generador y si $\sum_i a_i m_i = 0$ entonces $a_i = 0$ para todo i.

Denotaremos $M^{(I)} = \underset{i\in I}{\oplus} M_i$, siendo $M_i = M$. Se dice que un módulo es libre si es isomorfo a $A^{(I)}$. Si denotamos $1_j = (a_i)_{i\in I} \in A^{(I)}$, donde $a_i = 0$ para todo $i \neq j$ y $a_j = 1$, entonces $\{1_j\}_{j\in I}$ forma una base de $A^{(I)}$. Los morfismos de $A^{(I)}$ en un A-módulo M se corresponden con conjuntos $\{m_i\}_{i\in I}$ de M. Sea $\{m_i\}_{i\in I}$ un conjuntos de elementos de M, y definamos el morfismo

$$\phi\colon A^{(I)} \to M, (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i$$

Se cumple que ϕ es epiyectivo si y sólo si $\{m_i\}_{i\in I}$ es un sistema generador de M, ϕ es inyectivo si y sólo si $\{m_i\}_{i\in I}$ son linealmente independientes. Por tanto, ϕ es isomorfismo si y sólo si $\{m_i\}_{i\in I}$ es una base de M. En consecuencia, todo módulo es cociente de un libre y un módulo es libre si y sólo si tiene bases.

Sea pues, un epimorfismo $\pi\colon A^{(I)} \to M$. Igualmente, dado $\operatorname{Ker}\pi$ podemos definir un epimorfismo $A^{(J)} \to \operatorname{Ker}\pi$. Componiendo este último morfismo con la inclusión natural $\operatorname{Ker}\pi \hookrightarrow A^{(I)}$, tenemos un morfismo natural $s\colon A^{(J)} \to A^{(I)}$, de modo que la sucesión

$$A^{(J)} \xrightarrow{s} A^{(I)} \xrightarrow{\pi} M \to 0$$

es exacta. Es decir M es isomorfo a $\operatorname{Coker} s$, por tanto, el estudio de M se reduce al estudio de s, que es una aplicación A-lineal entre módulos libres.

El lema de Nakayama nos va a permitir calcular, mediante Álgebra Lineal, sistemas generadores.

Si M es un A-módulo e $I \subseteq A$ es un ideal, denotaremos por $I \cdot M = \{m \in M\colon m = \sum a_i m_i$, con $a_i \in I$ y $m_i \in M\}$, que es un A-submódulo de M. Se cumple que el A-módulo M/IM es de modo natural un A/I-módulo: $\bar a \cdot \bar m = a \cdot \bar m$. Es obvio que $M' \subseteq M/IM$ es un A-submódulo de M/IM, si y sólo si es un A/I-submódulo, y que $\bar m_1,\dots,\bar m_r \in M/IM$ es un sistema A-generador de M/IM si y sólo si es un sistema A/I-generador de M/IM. En el caso de que $I=\mathfrak{m}$ sea un ideal maximal, tendremos que $\bar m_1,\dots,\bar m_r\in M/\mathfrak{m}M$ es un sistema A-generador de $M/\mathfrak{m}M$ si y sólo si es un sistema generador del $A/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}M$.

8. Lema de Nakayama: *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y M un módulo finito generado. Se cumple que*

$$\mathfrak{m}M = M \iff M = 0$$

Como consecuencia se obtiene que $m_1,\dots,m_n\in M$ es un sistema generador de M, si sus clases $\bar m_1,\dots,\bar m_n$ en $M/\mathfrak{m}M$ son un sistema generador.

Demostración. Sea $n_1,\dots,n_r$ un sistema generador de M con el menor número posible de elementos. Si $\mathfrak{m}M=M$ tendremos que $n_1=\sum_{i=1}^r a_in_i$, con $a_i\in\mathfrak{m}$. Entonces $(1-a_1)n_1=\sum_{i=2}^r a_in_i$. Como $(1-a_1)$ no se anula en el único ideal maximal de $\mathcal{O}$, es invertible. Por tanto, $n_1=\frac{\sum_{i=2}^r a_in_i}{1-a_1}$, y $\langle n_2,\dots,n_r\rangle = M$, lo que es contradictorio salvo que $r=0$, es decir, $M=0$.

El recíproco es trivial.

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

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

$$M_S=\left\{\begin{array}{l}\dfrac{m}{s},\ m\in M \text{ y } s\in S\colon \dfrac{m}{s}=\dfrac{m'}{s'} \text{ si existen } s_1,s_2\in S \text{ tales que las fracciones}\\ \qquad\qquad\qquad\qquad \dfrac{s_1m}{s_1s},\dfrac{s_2m'}{s_2s'} \text{ tienen el mismo numerador y denominador}\end{array}\right\}^3$$

Con las operaciones (bien definidas)

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

M_S tiene estructura de A_S-módulo y diremos que es la localización de M por S. La aplicación canónica

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

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

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

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

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

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

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

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

Demostración. El morfismo $(\operatorname{Ker} f)_S \to M_S$, $\frac{m}{s}\mapsto\frac{m}{s}$ valora en $\operatorname{Ker} f_S$, pues $f_S(\frac{m}{s}) = \frac{f(m)}{s} = \frac{0}{s} = 0$ (para $m\in\operatorname{Ker} f$ y $s\in S$). Tenemos que comprobar que el morfismo $(\operatorname{Ker} f)_S\to\operatorname{Ker} f_S$, $\frac{m}{s}\mapsto\frac{m}{s}$ es un isomorfismo.

Inyectivo: si $\frac{m}{s}=0$ en $\operatorname{Ker} f_S\subseteq M_S$ entonces existe un $s'\in S$ de modo que $s'm=0$, luego $\frac{m}{s}=0$ en $(\operatorname{Ker} f)_S$. Epiyectivo: Dado $\frac{m}{s}$ en $\operatorname{Ker} f_S$, entonces $f_S(\frac{m}{s})=0$, luego $\frac{f(m)}{s}=0$. Por tanto, existe un $s'\in S$ de modo que $s'f(m)=0$, es decir, $f(s'm)=0$. Luego $\frac{m}{s}=\frac{s'm}{s's}$ con $s'm\in\operatorname{Ker} f$ y concluimos la epiyectividad.

Dejamos como ejercicio el probar que $(\operatorname{Im} f)_S = \operatorname{Im} f_S$. □

Una consecuencia de esta proposición es que la localización respeta los morfismos inyectivos y epiyectivos.

10. Proposición : *Sea S un sistema multiplicativo de A y sea*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

una sucesión exacta de A-módulos. Entonces es exacta la sucesión

$$M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$$

Demostración. Si $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión exacta de A-módulos entonces $\operatorname{Ker} g = \operatorname{Im} f$. Por tanto, $\operatorname{Ker} g_S = (\operatorname{Ker} g)_S = (\operatorname{Im} f)_S = \operatorname{Im} f_S$ (explícitamente, $\frac{m}{s}\mapsto\frac{m}{s}$) y $M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$ es exacta. □

11. Ejercicio : Probar

1. $(M/N)_S = M_S/N_S$.
2. $(M\oplus N)_S = M_S\oplus N_S$.
3. $(M+N)_S = M_S+N_S$.
4. $(M\cap N)_S = M_S\cap N_S$.

Uno de los procesos geométricos más básicos es el de localizar la atención en un entorno de un punto. Una propiedad es local cuando sólo depende del comportamiento en un entorno de cada punto. Por ejemplo, la continuidad de las funciones consideradas en Topología, la derivabilidad de las funciones consideradas en Análisis, la conexión local o compacidad local de los espacios topológicos, etc., son propiedades locales. Por el contrario, una propiedad es global cuando no es local, es decir, depende de todo el espacio considerado. Por ejemplo el concepto de función acotada no es local, ni el de espacio compacto o conexo.

Un resultado central de este capítulo será demostrar que la anulación de un módulo es una cuestión local y que por tanto, también son locales todos los problemas que puedan reducirse a la anulación de un módulo.

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

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

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

Dado un elemento $m \in M$, llamaremos anulador de $m \in M$ al ideal anulador del módulo $\langle m\rangle = \{am, a \in A\}$. Es decir, el ideal anulador de m es

$$\operatorname{Anul}(m) = \{a \in A \colon am = 0\}$$

El epimorfismo de A-módulos $A \to \langle m\rangle$, $a \mapsto am$, tiene de núcleo el ideal anulador de m. Por tanto, por el teorema de isomorfía $A/\operatorname{Anul}(m) \simeq \langle m\rangle$.

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

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

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

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

$$\operatorname{Sop} M = (\operatorname{Anul} M)_0$$

Como consecuencia se tiene que la condición necesaria y suficiente para que un módulo M (finito generado o no) sea cero es que $M_x = 0$, para todo punto cerrado $x \in \operatorname{Spec} A$.

Demostración. Empecemos probando que si $M = \langle m_1, \dots, m_r\rangle$ es un A-módulo finito generado, entonces $M_S = 0$ si y sólo si existe un $s \in S$ de modo que $sM = 0$: Si $M_S = 0$ entonces $\frac{m_i}{1} = 0$ para todo i, luego existen $s_i \in S$ de modo que $s_i m_i = 0$. Por tanto, $s = s_1 \cdots s_r \in S$ cumple que $sM = 0$. Recíprocamente, si existe $s \in S$ de modo que $sM = 0$, entonces $\frac{m}{s'} = 0$ para todo $\frac{m}{s'} \in M_S$ y $M_S = 0$.

Ahora ya, dado $x \in \operatorname{Spec} A$, tendremos que $M_x \neq 0$ si y sólo si $\operatorname{Anul}(M) \cap (A - \mathfrak{p}_x) = \emptyset$, es decir, $\operatorname{Anul}(M) \subseteq \mathfrak{p}_x$. Luego $\operatorname{Sop}(M) = (\operatorname{Anul} M)_0$.

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

□

15. Proposición :
1. *Una inclusión $N \subseteq M$ de módulos es una igualdad si y sólo si $N_x = M_x$, para todo punto cerrado $x \in \operatorname{Spec} A$.*
2. *Dos submódulos N, N' de un módulo M son iguales si y sólo si $N_x = N'_x$, para todo punto cerrado $x \in \operatorname{Spec} A$.*

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

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

□

16. Definición : Diremos que una sucesión de morfismos de A-módulos

$$\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \cdots$$

es exacta cuando $\operatorname{Im} f_n = \operatorname{Ker} f_{n+1}$ para todo n.

Casos concretos:

1. $0 \to N \xrightarrow{i} M$ es una sucesión exacta si y sólo si i es inyectiva.
2. $M \xrightarrow{\pi} M'' \to 0$ es una sucesión exacta si y sólo si π es un epimorfismo.
3. $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ es exacta si y sólo si i es inyectiva, π es epiyectiva y $\operatorname{Ker} \pi = \operatorname{Im} i$.

17. Teorema : *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión de morfismos de A-módulos. Las siguientes condiciones son equivalentes*

1. $M' \xrightarrow{f} M \xrightarrow{g} M''$ *es una sucesión exacta.*
2. $M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$ *es exacta para todo punto* $x \in \operatorname{Spec} A$.
3. $M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$ *es exacta para todo punto cerrado* $x \in \operatorname{Spec} A$.

Demostración. La implicación $1 \Rightarrow 2$ es un caso particular de 1.3.10. La implicación $2 \Rightarrow 3$ es evidente.

Veamos que $3 \Rightarrow 1$. Si la sucesión es exacta en todo punto cerrado x entonces $\operatorname{Ker} g_x = \operatorname{Im} f_x$. Luego $(\operatorname{Ker} g)_x = (\operatorname{Im} f)_x$. Por tanto, por la proposición anterior, $\operatorname{Ker} g = \operatorname{Im} f$ y la sucesión del punto 1. es exacta. □

Como corolario, dado que los morfismos inyectivos y epiyectivos son casos concretos de sucesiones exactas, tendremos que un morfismo es inyectivo (o epiyectivo) si y sólo si lo es localmente, para todo punto cerrado del espectro del anillo.

1.4 Anillos y módulos noetherianos

La introducción de los módulos la justificábamos con diversas razones. La primera que dábamos es que los ideales son módulos. Decíamos además que las operaciones básicas como producto tensorial, cocientes etc., se realizan de un modo mucho más flexible y claro con los módulos, y que muchos de los objetos usuales en Matemáticas tienen estructura de módulo.

En Geometría Algebraica los espacios estudiados son objetos definidos por un número finito de ecuaciones (la finitud es una condición natural). Es decir, los ideales que se consideran son los generados por un número finito de funciones. Los anillos cuyos ideales son finito generados se denominan noetherianos. Como veremos los anillos que usualmente aparecen en Geometría Algebraica y la Aritmética son noetherianos, de forma que estos anillos proporcionan el marco natural para desarrollar su estudio.

De nuevo, será natural comenzar estudiando los módulos finito generados, cuyos submódulos sean finito generados, en vez de limitarnos simplemente a los anillos cuyos ideales son finito generados.

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

2. Definición : ^{2} Un A-módulo M se dice que es noetheriano si toda cadena ascendente de submódulos de M

$$M_1 \subseteq M_2 \subseteq \cdots M_n \subseteq \cdots$$

estabiliza, es decir existe $m >> 0$ de modo que $M_m = M_{m+1} = \cdots$.

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

Demostración. **def**^{1} $\Rightarrow$ **def**^{2}: Sea una cadena ascendente de submódulos de M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$.

Sea $M' = \bigcup\limits_{i=1}^{\infty} M_i \subseteq M$. Como M' es un submódulo de M, es finito generado. Escribamos $M' = \langle m_1, \ldots, m_r \rangle$, con $m_j \in M_{i_j}$. Sea m el máximo de todos los i_j. Entonces trivialmente se obtiene que $M' = M_m$, luego $M_m = M_{m+1} = \cdots$.

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 $m_2 \in M' - M_1$. 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 $m \in \mathbb{N}$ tal que $\langle m_1, \ldots, m_m \rangle = M'$.

□

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

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

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

Demostración. Sea M noetheriano y $\pi\colon M \to M/N$ un cociente. Dado un submódulo $\bar{M} \subset M/N$, tenemos que $\pi^{-1}\bar{M} = \langle m_1, \ldots, m_r \rangle$. Por tanto, $\bar{M} = \langle \pi(m_1), \ldots, \pi(m_r) \rangle$. □

7. Proposición : *Sea*

$$0 \to M_1 \to M_2 \xrightarrow{\pi} M_3 \to 0$$

una sucesión exacta de A-módulos. Se verifica que M_2 es noetheriano $\Leftrightarrow$ M_1 y M_3 son noetherianos.

Demostración. $\Rightarrow$) Esto es lo que afirman las dos proposiciones anteriores.

$\Leftarrow$) Sea $M' \subseteq M_2$. El diagrama siguiente es conmutativo y las filas son exactas:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' \cap M_1 & \longrightarrow & M' & \longrightarrow & \pi(M') & \longrightarrow & 0 \\
 & & \cap & & \cap & & \cap & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \underset{\pi}{\longrightarrow} & M_3 & \longrightarrow & 0
\end{array}$$

Tenemos que $M' \cap M_1 = \langle m_1, \dots, m_r \rangle$ y que $\pi(M') = \langle \pi(n_1), \dots, \pi(n_s) \rangle$. Por tanto, tenemos la igualdad $M' = \langle m_1, \dots, m_r, n_1, \dots, n_s \rangle$.

□

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

9. Definición : Se dice que un anillo es noetheriano si como A-módulo es noetheriano, es decir si todo ideal es finito generado, o equivalentemente, si toda cadena ascendente de ideales estabiliza.

10. 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.

11. Corolario : *Si A es noetheriano entonces todo A-módulo finito generado es noetheriano.*

Demostración. Si A es noetheriano A^n es un A-módulo noetheriano, por el ejercicio que sigue a la proposición 1.4.7. Ahora bien, como todo módulo finito generado es cociente de un libre finito generado, concluimos que los módulos finitos son noetherianos.

□

Por tanto, sobre los dominios de ideales principales todo módulo finito generado es noetheriano.

12. Ejercicio : Si A es noetheriano A_S es noetheriano

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

1.5 Teorema de la base de Hilbert

1. Teorema de la base de Hilbert: *Si A es un anillo noetheriano entonces $A[x]$ es un anillo noetheriano.*

Demostración. Sea $I \subset A[x]$ un ideal. Tenemos que ver que es finito generado:

Sea $J \subseteq A$ el conjunto formado por los coeficientes de máximo grado de los $p(x) \in I$. Es fácil ver que J es un ideal de A. Observemos para ello, que si $p(x) = a_0x^n + \cdots + a_n$, $q(x) = b_0x^m + \cdots + b_m \in I$, entonces $x^m p(x) + x^n q(x) = (a_0 + b_0)x^{n+m} + \cdots \in I$, luego si $a_0, b_0 \in J$ entonces $a_0 + b_0 \in J$.

Por ser A noetheriano, $J = (b_1, \dots, b_r)$ es finito generado. Así, existen $p_1, \dots, p_r \in I$ cuyos coeficientes 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 $\operatorname{gr} p_i = m$.

Dado $p(x) = a_0x^n + \cdots + a_n \in I$. Supongamos que $n \geq m$. Escribamos $a_0 = \lambda_1 b_1 + \cdots + \lambda_r b_r$, con $\lambda_i \in A$ para todo i. Tenemos que $p(x) - \sum_i \lambda_i x^{n-m} p_i \in I$ y $\operatorname{gr}(p(x) - \sum_i \lambda_i x^{n-m} p_i) < \operatorname{gr} p(x)$.

Recurrentemente obtendré que

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

Ahora bien $I \cap \{A + Ax + \cdots + Ax^{m-1}\}$ es un A-módulo finito generado ya que es submódulo de $\{A + Ax + \cdots + Ax^{m-1}\}$, que es un A-módulo noetheriano. En conclusión, si escribimos $I \cap \{A + Ax + \cdots + Ax^{m-1}\} = (q_1, \dots, q_s)_A$, tenemos que $I = (p_1, \dots, p_r, q_1, \dots, q_s)$.

□

2. Definición : Dado un morfismo de anillos $f\colon A \to B$ se dice que B es una A-álgebra. Se dice que B es una A-álgebra de tipo finito si existen $\xi_1, \ldots, \xi_n \in B$ que generen A-algebraicamente B, es decir, si el morfismo

$$A[x_1, \ldots, x_n] \to B, \quad \sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto \sum_{\alpha_1,\ldots,\alpha_n} f(a_{\alpha_1,\ldots,\alpha_n}) \xi_1^{\alpha_1} \cdots \xi_n^{\alpha_n}$$

es epiyectivo.

3. Corolario : *Sea k un cuerpo. Toda k-álgebra de tipo finito es noetheriana.*

Demostración. Todo cuerpo es un anillo noetheriano, luego k es noetheriano. Por el teorema de la base de Hilbert $k[x_1]$ es noetheriano. De nuevo, por el teorema de la base de Hilbert, $k[x_1, x_2]$ es noetheriano. En conclusión $k[x_1, \ldots, x_n]$ es noetheriano y todo cociente $k[x_1, \ldots, x_n]/I$ también. Luego toda k-álgebra de tipo finito es noetheriana.

□

1.6 Espectro primo de un anillo

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

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. Por ejemplo, los cuerpos son anillos íntegros.

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

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

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

□

3. 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.

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

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

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

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

6. Corolario : *Todo ideal $I \underset{\neq}{\subset} A$ está incluido en un ideal maximal.*

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

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

$$J \longrightarrow \pi(J)$$

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

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

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

7. Proposición : *Un ideal $\mathfrak{m} \underset{\neq}{\subset} A$ es maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo. En particular, los ideales maximales son ideales primos, por la proposición* 1.6.2.

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

8. Definición : Sea k un cuerpo. Si $i\colon k \to A$ es un morfismo de anillos diremos que A es una k-álgebra. Seguiremos la notación $i(\lambda) \underset{Not.}{=} \lambda$. Si A y B son k-álgebras, diremos que un morfismo $\phi\colon A \to B$ de anillos es un morfismo de k-álgebras si $\phi(\lambda) = \lambda$, para todo $\lambda \in k$.

9. Definición : Diremos que un ideal $\mathfrak{m}$ de una k-álgebra A es racional, si $A/\mathfrak{m} \simeq k$ (como k-álgebras).

En particular, los ideales racionales son maximales.

10. Proposición : *Un ideal $\mathfrak{m}$ de $k[x_1, \dots, x_n]$ es racional si y sólo si $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$, $\alpha_i \in k$ para todo i.*

Demostración. Sea $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Veamos que $\mathfrak{m}$ es racional. El núcleo del morfismo de k-álgebras $k[x_1, \dots, x_n] \to k$, $p(x_1, \dots, x_n) \mapsto p(\alpha_1, \dots, \alpha_n)$, es $\mathfrak{m}$ (como puede comprobarse). Además el morfismo es epiyectivo, luego $k[x_1, \dots, x_n]/\mathfrak{m} \simeq k$.

Recíprocamente, sea un isomorfismo $\phi\colon k[x_1, \dots, x_n]/\mathfrak{m} \simeq k$ de k-álgebras. Consideremos la composición

$$k[x_1, \dots, x_n] \xrightarrow{\pi} k[x_1, \dots, x_n]/\mathfrak{m} \overset{\phi}{\simeq} k$$

donde π es el morfismo de paso al cociente. Sean $\alpha_i = \phi(\bar{x}_i)$. Por tanto, $\phi \circ \pi(p(x_1, \dots, x_n)) = p(\alpha_1, \dots, \alpha_n)$. Por un lado, como hemos visto más arriba, se cumple que $\operatorname{Ker}(\phi \circ \pi) = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Por otro lado, $\operatorname{Ker}(\phi \circ \pi) = (\phi \circ \pi)^{-1}(0) = \pi^{-1}(\phi^{-1}(0)) = \pi^{-1}(0) = \mathfrak{m}$. En conclusión, $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$.

□

Así pues, existe una correspondencia biunívoca entre los ideales racionales de $k[x_1,\dots,x_n]$ y los puntos $(\alpha_1,\dots,\alpha_n)$ del espacio afín $\mathbb{A}_n(k)$. Es decir, si "pensamos" $k[x_1,\dots,x_n]$ como las funciones algebraicas del espacio afín $\mathbb{A}_n(k)$, el modo de recuperar $\mathbb{A}_n(k)$ a partir de $k[x_1,\dots,x_n]$ es considerando sus ideales racionales. En general, por las razones esbozadas en la introducción, dado un anillo consideraremos el espacio formado por el conjunto de todos los ideales primos (y no sólo los ideales racionales).

11. Proposición : *Sea* $A = k[x_1,\dots,x_n]/I$ *e* $I = (p_1(x_1,\dots,x_n),\dots,p_m(x_1,\dots,x_n))$. *Se cumple que los puntos racionales de* $\operatorname{Spec} A$ *se corresponden biyectivamente con las soluciones del sistema de ecuaciones*

$$p_1(x_1,\dots,x_n) = 0,\dots,p_m(x_1,\dots,x_n) = 0$$

Demostración. Dar un punto racional de A equivale a dar un morfismo de k-álgebras $A \to k$, lo cual equivale a un morfismo de k-álgebras $k[x_1,\dots,x_n] \to k$ que se anule sobre I. Se concluye inmediatamente. □

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

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

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

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

13. 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,

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

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

15. Proposición : *Se verifican las siguientes igualdades:*

1. $(0)_0 = \operatorname{Spec} A$ *y* $(A)_0 = \emptyset$.
2. $(\sum_{j\in J} I_j)_0 = \underset{j\in J}{\cap} (I_j)_0$.
3. $(\overset{n}{\underset{j=1}{\cap}} I_j)_0 = \overset{n}{\underset{j=1}{\cup}} (I_j)_0$.

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 $(I_1 \cap I_2)_0 \subseteq (I_1)_0 \cup (I_2)_0$.

□

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

17. 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.

18. 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 $J \underset{\neq}{\subset} I$ 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 $\operatorname{Spec} A$.

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

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 $(\mathfrak{p}_x)_0 = (I)_0 = \bar{x}$.

□

20. Definición : Diremos que un espacio topológico es irreducible cuando no pueda descomponerse como unión de dos cerrados estrictamente menores. Llamaremos componentes irreducibles de un espacio topológico a los subespacios irreducibles maximales de X, es decir, los subespacios irreducibles no contenidos estrictamente en otro subespacio irreducible.

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

21. 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 $g \in I$. □

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

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

24. Ejemplo : Sea $X = [0, 1] \subset \mathbb{R}$ y $C(X)$ el anillo de funciones reales continuas definidas sobre X. Dado un punto $p \in X$, el ideal $\mathfrak{m}_p$ de funciones que se anulan en p es un ideal maximal, porque $C(X)/\mathfrak{m}_p \simeq \mathbb{R}$, $\bar{f} \mapsto f(p)$.

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

Si denotamos por $\operatorname{Spec}_m A$ el subespacio de $\operatorname{Spec} A$ formado por los ideales primos maximales, es fácil comprobar que la biyección

$$X = \operatorname{Spec}_m C(X),\ p \mapsto \mathfrak{m}_p$$

es un homeomorfismo. Dado un ideal I, denotemos $(I)_0^m = (I)_0 \cap \operatorname{Spec}_m A$. Bien, a través de la igualdad anterior, se cumple que $\{x \in X, \text{ tales que } f(x) = 0, \text{ para toda } f \in I\} = (I)_0^m$.

25. 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 $\underset{j}{\cap} C_j = \emptyset$ entonces

$$\emptyset = \underset{j}{\cap} (I_j)_0 = (\sum_j I_j)_0$$

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

26. Proposición : *Si A es un anillo noetheriano, entonces* $\operatorname{Spec} A$ *es un espacio topológico noetheriano. (Un espacio topológico se dice que es noetheriano si toda cadena descendente de cerrados estabiliza).*

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, $C_m = C_{m+1} = \cdots$.

□

27. Ejercicio : Demostrar

1. Todo espacio topológico noetheriano es compacto.
2. Todo abierto de un espacio topológico noetheriano es noetheriano.
3. Llamemos cerrado irreducible a todo cerrado que no es unión de dos cerrados propios. Todo espacio topológico noetheriano es unión de un número finito de cerrados irreducibles.

28. Ejercicio : Probar que en un anillo noetheriano el número de ideales primos minimales es finito.

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

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

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

Demostración. Consideremos los morfismos

$$A \xrightarrow{j} B$$
$$\operatorname{Spec} A \xleftarrow[j^*]{} \operatorname{Spec} B$$

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.

□

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

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

es biyectiva (usar el ejemplo 1.6.24 y que todo morfismo $C(X) \to C(X)$ induce un morfismo entre los espectros).

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

$$A \xrightarrow{\pi} A/I \qquad\qquad a \longrightarrow \bar{a}$$

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

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

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

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

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

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

que es justamente el morfismo

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

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

□

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

33. 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.

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

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

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

1.7 Fórmula de la fibra

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

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

1. 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 donde no se anula ninguna función de S:*

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

Demostración. Consideremos el morfismo de localización $j\colon A \to A_S$.

Las asignaciones

$$\begin{tikzcd}
\operatorname{Spec} A_S \arrow[r, equal] & \{\text{Ideales primos de } A \text{ que no cortan a } S\} \subseteq \operatorname{Spec} A \\
\mathfrak{p}' \arrow[r, "j^*"] & \mathfrak{p}' \cap A \\
\mathfrak{p} \cdot A_S & \mathfrak{p} \arrow[l]
\end{tikzcd}$$

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

□

Notación: Sea A un anillo. Si $f \in A$, denotaremos A_f la localización de A por el sistema multiplicativo $S = \{1, f, f^2, \dots, f^n, \dots\}$.

Si x es un punto de $\operatorname{Spec} A$, denotaremos por A_x la localización de A por el sistema multiplicativo $S = A - \mathfrak{p}_x$.

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

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

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

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

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

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

5. 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".

6. 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

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

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

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

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

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

Sea ahora $f \in \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$. Por el corolario 1.7.2, $\operatorname{Spec} A_f = \emptyset$. Por tanto, $A_f = 0$, es decir, $\frac{1}{1} = \frac{0}{1}$. Luego existe un $f^n \in \{1, f, f^2, \dots\}$, de modo que $f^n \cdot (1 \cdot 1 - 0 \cdot 1) = 0$. Entonces $f^n = 0$ y f es nilpotente. En conclusión $\operatorname{rad} A \supseteq \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$ y hemos terminado. □

8. Definición : Sea $I \subset A$ un ideal. Se llama radical de I, que denotaremos por $r(I)$ a la intersección de todos los ideales primos que contienen a I.

Si $\pi\colon A \to A/I$ es el morfismo de paso al cociente entonces $\pi^{-1}(\operatorname{rad}(A/I)) = r(I)$. Porque $\pi^{-1}(\bigcap_{x\in\operatorname{Spec} A/I} \mathfrak{p}_x) = \bigcap_{x\in\operatorname{Spec} A/I} \pi^{-1}(\mathfrak{p}_x) = \bigcap_{I\subset\mathfrak{q}_x} \mathfrak{q}_x$.

Por tanto, por 1.7.7, $a \in r(I)$ si y sólo si existe un $n \in \mathbb{N}$ tal que $a^n \in I$.

9. Corolario: *Sea A un anillo noetheriano. Si I es un ideal radical, es decir, $I = r(I)$ si y sólo si I es la intersección de un número finito de ideales primos.*

Demostración. Se cumple que el radical conmuta con intersecciones finitas, es decir, $r(I_1\cap\cdots\cap I_n)) = r(I_1)\cap\cdots r(I_n)$. Si $I = \mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n$, con $\mathfrak{p}_i$ ideales primos entonces $r(I) = r(\mathfrak{p}_1)\cap\cdots\cap r(\mathfrak{p}_n) = \mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n = I$.

Recíprocamente, $r(I)$ es la intersección de todos los ideales primos que contienen a I. Ahora bien, los ideales primos mínimos $\{\mathfrak{p}_i\}$ con la condición de contener a I son un número n finito, porque $\bar{\mathfrak{p}}_i \subset A/I$ son justamente los ideales primos minimales de A/I, que son un número finito. Por tanto, $r(I) = \mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n$.

□

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

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

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

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

Demostración.

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

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

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

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

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

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

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

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

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

1. Los puntos cerrados (α,β), es decir, los ideales primos $(x-\alpha, y-\beta)$.

2. Los puntos genéricos de las curvas irreducibles $(p(x,y))_0 \equiv p(x,y) = 0$, es decir, los ideales primos $(p(x,y))$, $p(x,y)$ irreducible.

3. El punto genérico del plano afín $(0)_0 \equiv \mathbb{A}_2(\mathbb{C})$, es decir, el ideal primo (0).

12. 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 $\operatorname{Spec}\mathbb{C}[x,y]/(q(x,y)) = (q(x,y))_0 = \overset{r}{\underset{i=1}{\cup}} (q_i(x,y))_0$ que son:

1. Los ideales maximales $(x-\alpha, y-\beta)$ tales que $(q(x,y)) \subseteq (x-\alpha, y-\beta)$. Es decir, con otras notaciones, los puntos (α,β) tales que $q(\alpha,\beta) = 0$.

2. Los puntos genéricos de las curvas irreducibles $q_i(x,y) = 0$.

1.8 Problemas

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

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

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

4. Probar que $(A_S)_{S'} = A_{S\cdot S'}$.

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

6. Probar que $\mathbb{C}[x]_{\mathbb{R}[x]-0} \simeq \mathbb{C}(x)$. Probar que $\mathbb{Z}[x]_{\mathbb{Z}[x]-\{0\}} = \mathbb{Q}(x)$.

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

8. Probar que $A_{1+\mathfrak{m}_x} = A_x$.

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

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

11. Sea M un A-módulo noetheriano y N un A-módulo finito. Probar que $\operatorname{Hom}_A(N, M)$ es un A-módulo noetheriano.

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

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

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

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

16. Probar que $k[[x]]$ es un anillo noetheriano.

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

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

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

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

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

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

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

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

25. Sean $I, I' \subseteq A$ dos ideales. Probar que $(I)_0 = (I')_0$ si y sólo si $r(I) = r(I')$.

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

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

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

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

30. Calcular el morfismo $f \colon \mathbb{C}[x, y]/(x - 1) \to \mathbb{C}[x, y]/(y - x^3)$ que en espectros aplica cada punto (cerrado) (α, β) de la cúbica $y = x^3$ en el punto de la recta $x = 1$ que se obtiene como corte de la recta que pasa por el origen y (α, β), con la recta $x = 1$.

Capítulo 2

Variedades algebraicas afines

2.1 Introducción

Entendamos ahora las nociones de variedad y subvariedad desde un punto de vista puramente geométrico, es decir, como el conjunto de soluciones sobre un cuerpo algebraicamente cerrado, de un sistema de ecuaciones algebraicas. Queremos probar el teorema fuerte de los ceros de Hilbert, que dice que hay una correspondencia biunívoca, "salvo nilpotentes", entre los ideales del anillo de funciones algebraicas de una variedad algebraica y las subvariedades de las variedad algebraica. La descomposición primaria en anillos noetherianos, nos permitirá decir con todo rigor, que los ideales del anillo de funciones algebraicas de una variedad se corresponden con los conjuntos de funciones del anillo que se anulan en ciertas subvariedades algebraicas de la variedad y verifican ciertas condiciones infinitesimales a lo largo de un número finito de subvariedades de las subvariedades. En conclusión, tenemos una comprensión geométrica acabada de los ideales, es decir, de los sistemas de ecuaciones algebraicas.

El teorema central, que usaremos para la demostración del teorema de los ceros de Hilbert y el desarrollo de la teoría de la dimensión, será el lema de Noether, que afirma que toda variedad algebraica se proyecta con fibras finitas en un espacio afín. Esto nos llevará a estudiar con mayor profundidad los morfismos finitos.

2.2 Morfismos finitos

1. Definición: Un morfismo de anillos $f\colon A \to B$ se dice que es finito si B es un A-módulo finito, con la estructura natural de A-módulo que define f en B ($a \cdot b := f(a) \cdot b$). En este caso, también se dice que B es una A-álgebra finita.

2. Proposición: *La composición de morfismos finitos es finito.*

Demostración. Sean $A \overset{\text{finito}}{\longrightarrow} B \overset{\text{finito}}{\longrightarrow} C$. Es decir, $B = Ab_1 + \cdots + Ab_n$ y $C = Bc_1 + \cdots + Bc_m$. Luego,

$$C = (Ab_1 + \cdots + Ab_n)c_1 + \cdots + (Ab_1 + \cdots + Ab_n)c_m = \sum_{i=1,j=1}^{n,m} Ab_i c_j$$

En conclusión, $A \to C$ es un morfismo finito.

$\square$

3. Proposición : *Si $A \to B$ es un morfismo finito y $A \to C$ un morfismo de anillos, entonces $C = A \otimes_A C \to B \otimes_A C$ es un morfismo finito. "Los morfismos finitos son estables por cambio de base".*

Demostración. Inmediato. □

4. Corolario : *Si $A \to B$ es un morfismo finito, entonces $A_S \to B_S$ y $A/I \to B/I \cdot B$ son morfismos finitos*

5. Definición : Sea $A \to B$ un morfismo de anillos. Se dice que $b \in B$ es entero sobre A si verifica una relación del tipo

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0, \qquad \text{con}\, a_i \in A$$

El teorema de Hamilton-Cayley para los endomorfismos de espacios vectoriales también es cierto para los endomorfismos de módulos. Con precisión, sea $M = \langle m_1, \dots, m_r \rangle$ un A-módulo finito generado, $f\colon M \to M$, $f(m_i) = \sum\limits_j a_{ij} m_j$ un endomorfismo de A-módulos; si $p_c(x)$ es el polinomio característico de la matriz (a_{ij}), entonces $p_c(f) = 0$. En efecto, consideremos la matriz $B = (x_{ij})$ de coeficientes variables y el polinomio característico $P_c(X)$ de esta matriz. $P_c(X)$ es un polinomio con coeficientes en $\mathbb{Z}[x_{ij}] \subset \mathbb{Q}(x_{ij})$. Por el teorema de Hamilton-Cayley $P_c(B) = 0$. Por tanto, especializando a $x_{ij} = a_{ij}$, tendremos que $p_c(f) = 0$.

6. Proposición : *Sean $f\colon A \to B$ un morfismo de anillos y $b \in B$. Denotemos $A[b] = \{p(b) \in B,$ para $p(x) \in A[x]\}$. El morfismo $A \to A[b]$ es finito $\Leftrightarrow$ b es entero sobre A.*

Demostración. $\Rightarrow$) Consideremos el endomorfismo de A-módulos

$$\begin{aligned} A[b] &\xrightarrow{\cdot b} A[b] \\ p(b) &\longmapsto p(b) \cdot b \end{aligned}$$

Si (a_{ij}) es una matriz asociada a $\cdot b$ en un sistema generador de $A[b]$, entonces el polinomio característico de (a_{ij}) anula a $\cdot b$, luego anula a b, luego b es entero sobre A.

$\Leftarrow$) 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 $\bar{1}, \dots, \bar{x}^{n-1}$ se concluye. □

Observación: Para la demostración de $\Rightarrow$) sólo es necesario suponer que $A[b]$ está incluido en una A-álgebra finita.

7. Ejemplo : Si α es una raíz n-ésima de la unidad, entonces $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ es un morfismo finito.

8. Ejemplo : El morfismo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3) \to \operatorname{Spec} k[x]$ definido por $(\alpha, \beta) \mapsto \alpha$ es un morfismo finito.

9. Proposición : *Sea $f\colon A \to B$ 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 2.2.2, $A \to A[b_1, b_2]$ es un morfismo finito. Luego, por la observación anterior, todo elemento $p(b_1, b_2) \in A[b_1, b_2] \in B$, con $p(x,y) \in A[x,y]$, es entero sobre A.

□

10. Definición : Diremos que un anillo íntegro A es íntegramente cerrado en su cuerpo de fracciones Σ, si todo elemento de Σ entero sobre A pertenece a A. También se dice que A es un anillo normal.

Se dice que un morfismo de anillos $A \to B$ es entero si todo elemento de B es entero sobre A, es decir, si B es unión de A-subálgebras finitas.

Sea $A \to B$ un morfismo inyectivo de anillos. Llamaremos cierre entero de A en B al subanillo de B formado por todos los elementos de B enteros sobre A.

Dejamos que el lector pruebe que el cierre entero de un anillo íntegro en su cuerpo de fracciones es un anillo íntegramente cerrado.

11. Ejercicio : Demostrar que $\mathbb{Z}$ es un anillo íntegramente cerrado en $\mathbb{Q}$.

12. Proposición : *Si $f\colon A \hookrightarrow B$ es un morfismo finito e inyectivo, entonces el morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo.*

Con mayor generalidad, si $f\colon A \hookrightarrow B$ es un morfismo entero e inyectivo, entonces el morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo

Demostración. Supongamos que f es un morfismo finito. Dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to B_x$ es finito e inyectivo. Por Nakayama, $\mathfrak{p}_x B_x \neq B_x$, luego $\operatorname{Spec} B_x/\mathfrak{p}_x B_x \neq \emptyset$. Es decir, la fibra de x es no vacía, luego f^* es epiyectivo.

Ahora ya, si B es entero sobre A, entonces $B_x/\mathfrak{p}_x B_x \neq 0$ porque si $B_x/\mathfrak{p}_x B_x = 0$, para alguna subálgebra finita B_i se verificará que $(B_i)_x/\mathfrak{p}_x (B_i)_x = 0$ y llegaremos a contradicción con el párrafo anterior. De nuevo, tenemos que la fibra de x es no vacía y f^* es epiyectivo. □

13. Definición : Llamaremos dimensión de Krull de un anillo A, al supremo de las longitudes de las cadena de ideales primos de A, o equivalentemente, al supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$. Denotaremos a la dimensión (de Krull) de A por $\dim A$. Llamaremos dimensión de $\operatorname{Spec} A$ a la dimensión de Krull de A.

14. Ejercicio : Demostrar que la dimensión de Krull de $\mathbb{Z}$ y $k[x]$ es uno y la de $\mathbb{C}[x,y]$ dos.

15. Proposición : *Toda k-álgebra finita e íntegra es cuerpo.*

Demostración. Sea A una k-álgebras 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. □

16. 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. □

17. Teorema : *Sea $f\colon A \to B$ es un morfismo entero. El morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación cerrada de fibras de dimensión cero (y finitas si f es finito).*

Demostración. Sea $C = (J)_0$ un cerrado de $\operatorname{Spec} B$. Debemos demostrar que $f^*(C)$ es un cerrado de $\operatorname{Spec} A$. Consideremos los diagramas

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, dash] & B \arrow[d, dash] \\ A/(J\cap A) \arrow[r] & B/J \end{tikzcd} \qquad \begin{tikzcd} \operatorname{Spec} A & & \operatorname{Spec} B \arrow[ll, "f^*"'] \\ (J\cap A)_0 = \operatorname{Spec} A/(J\cap A) \arrow[u, hook] & & \operatorname{Spec} B/J = C \arrow[ll, "{f^*}_{|C}"] \arrow[u, hook] \end{tikzcd}$$

Como $A/J\cap A \hookrightarrow B/J$ es un morfismo entero inyectivo, por 2.2.12 ${f^*}_{|C}$ es epiyectiva y $f^*(C) = (J\cap A)_0$.

La fibra de un punto $x \in \operatorname{Spec} A$ es ${f^*}^{-1}(x) = \operatorname{Spec} B_x/\mathfrak{p}_x B_x$. Supongamos que f es un morfismo finito. Observemos que si ${f^*}^{-1}(x) \neq \emptyset$ entonces $B_x/\mathfrak{p}_x B_x$ es una $A_x/\mathfrak{p}_x$-álgebra finita. Por la proposición 2.2.16, concluimos que f^* es de fibras de dimensión cero y finitas. Si f entero es sencillo deducir que las fibras son de dimensión cero una vez que se sabe esto para los morfismos finitos. $\square$

18. Ejercicio: Probar que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

2.3 Teoremas de ascenso y descenso de ideales

1. Teorema del ascenso: *Sea $f\colon A \to B$ un morfismo entero. 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. El morfismo $A/\mathfrak{p}_x \to B/\mathfrak{p}_y$ es entero e inyectivo, luego epiyectivo entre espectros (2.2.12); es decir, $f^*\colon (\mathfrak{p}_y)_0 \to (\mathfrak{p}_x)_0$ es epiyectivo y existe $y' \in (\mathfrak{p}_y)_0$ tal que $f^*(y') = x'$. $\square$

Recordemos que la dimensión de Krull de un anillo A es el supremo de las longitudes de las cadena de ideales primos de A, o equivalentemente el supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$. Se denota $\dim A$ a la dimensión (de Krull) de A.

2. Corolario: *Si $f\colon A \hookrightarrow B$ es un morfismo entero 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 entre los espectros son de dimensión cero, por 2.2.17. 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 2.2.12). 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 $\dim A = \dim B$. $\square$

Si G es un grupo de automorfismos de un anillo A, de modo natural G es un grupo de homeomorfismos de $\operatorname{Spec} A$, definiendo $g\cdot x := {g^*}^{-1}(x)$, es decir, $\mathfrak{p}_{g\cdot x} = g(\mathfrak{p}_x)$.

Si G es un grupo de homeomorfismos de un espacio topológico X, entonces define una relación de equivalencia en X: $x \sim x'$ si y sólo si $x = g(x')$, para algún $g \in G$. Denotaremos el espacio topológico cociente $X/G := \{[x] \mid [x] = [x'] \text{ si y sólo si } x \sim x'\}$. Si $\pi\colon X \to X/G$ es el morfismo de paso al cociente, $U \subset X/G$ es un abierto si y sólo si $\pi^{-1}(U)$ es un abierto. Se verifica que π es una aplicación abierta, porque si V es un abierto de X, $\pi^{-1}(\pi(V)) = \underset{g\in G}{\cup} g(V)$, que es un abierto, luego $\pi(V)$ es un abierto de X/G. Del mismo modo, si G es finito, π es un morfismo cerrado. En este caso, si $\pi(x) = y$ e $y \in \bar{y'}$, entonces existe x' de modo que $x \in \bar{x'}$ y $\pi(x') = y'$: Las fibras de π son las órbitas por la acción de G y $\pi(\bar{x}) = \bar{y}$, luego $\pi^{-1}(\bar{y}) = \cup_{g\in G} \overline{gx}$. Dado x'' tal que $\pi(x'') = y'$, tendremos que $x'' \in \overline{gx}$ para algún $g \in G$. Entonces $x' := g^{-1}x''$ verifica que $x' \in \bar{x}$ y $\pi(x') = \pi(x'') = y'$.

3. Definición : Se dice que un morfismo de anillos $A \to B$ cumple el teorema del descenso de ideales si para cada par de ideales primos $\mathfrak{p}_{y'} \subseteq \mathfrak{p}_y \subseteq A$, y un ideal primo $\mathfrak{p}_x \subseteq B$ tal que $\mathfrak{p}_x \cap A = \mathfrak{p}_y$, entonces existe un ideal primo $\mathfrak{p}_{x'} \subseteq \mathfrak{p}_x$ tal que $\mathfrak{p}_{x'} \cap A = \mathfrak{p}_{y'}$.

4. Proposición : *Sea G un grupo finito de automorfismos de un anillo B. Se verifica que*

$$\operatorname{Spec} B^G = (\operatorname{Spec} B)/G$$

donde $B^G = \{b \in B \colon g(b) = b$, para todo $g \in G\}$.

En consecuencia, el morfismo natural $\pi \colon \operatorname{Spec} B \to \operatorname{Spec} B^G$ cumple el teorema del descenso de ideales.

Demostración. Empecemos observando que dada $f \in B$, el polinomio $\prod_{g\in G}(x - g(f))$ es un polinomio mónico con coeficientes en B^G. Por tanto, $B^G \hookrightarrow B^G[f]$ es un morfismo finito. Así pues, $B^G \hookrightarrow B$ es un morfismo entero, luego en espectros epiyectivo, cerrado y de fibras de dimensión cero.

Sólo nos falta ver que las fibras del morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$ son órbitas por la acción de G.

G actúa transitivamente sobre las fibras del morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$: Obviamente, dado un ideal primo $\mathfrak{p}_x \subset B$, $g(\mathfrak{p}_x)$ corta a B^G en el mismo ideal primo que $\mathfrak{p}_x$. Es decir, G actúa en las fibras. Sea $\mathfrak{p}_x$ es un ideal primo de B distinto de $g(\mathfrak{p}_{x'}) = \mathfrak{p}_{g(x')}$ para todo $g \in G$. Supongamos que x, x' tienen la misma imagen por el morfismo $\operatorname{Spec} B \to \operatorname{Spec} B^G$, digamos y. Por ser el morfismo $B^G \hookrightarrow B$ entero sabemos que $g(x') \notin \bar{x}$ para todo $g \in G$, luego existe una $f \in B$ que se anula en x y no se anula en ninguno de los $g(x')$. Entonces $N(f) := \prod_{g\in G} g(f) \in B^G$ se anula en x y no se anula en ninguno de los $g(x')$. Llegamos a contradicción, porque por un lado $N(f)$ ha de anularse en y y por el otro no.

□

5. Teorema del descenso de Cohen-Seidenberg : *Sea A un anillo íntegramente cerrado en su cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \Sigma'$ una extensión finita de cuerpos y A' una A-álgebra contenida en el cierre entero de A en Σ'. El morfismo $\operatorname{Spec} A' \to \operatorname{Spec} A$ es abierto y $A \hookrightarrow A'$ cumple el teorema del descenso de los ideales.*

Demostración. Sea Σ'' la envolvente normal de Σ' sobre Σ. Sea A'' el cierre entero de A en Σ''. Tenemos los morfismos

$$A \hookrightarrow A' \hookrightarrow A'', \quad \operatorname{Spec} A \leftarrow \operatorname{Spec} A' \leftarrow \operatorname{Spec} A''$$

Los morfismos inyectivos enteros, como los finitos, son epiyectivos en espectros. Por tanto, si $\operatorname{Spec} A'' \to \operatorname{Spec} A$ es abierto entonces $\operatorname{Spec} A' \to \operatorname{Spec} A$ es abierto. Igualmente, si $A \hookrightarrow A''$ cumple el teorema del descenso de ideales, entonces $A \hookrightarrow A'$ también. En conclusión, podemos suponer que $\Sigma \hookrightarrow \Sigma'$ es una extensión normal, digamos de grupo de automorfismos G. Sea $\bar{A}$ el cierre entero de A en Σ'^G. Es fácil ver que $\bar{A} = A'^G$. Por la proposición 2.3.4, el teorema es cierto para el morfismo $A'^G \hookrightarrow A'$. Para concluir, basta demostrar el teorema para

$$\begin{tikzcd} A \arrow[r] \arrow[d, dash] & \bar{A} \arrow[d, dash] \\ \Sigma \arrow[r] & \Sigma'^G \end{tikzcd}$$

Basta probar que $\operatorname{Spec} \bar{A} \to \operatorname{Spec} A$ es biyectiva. Como $\Sigma \to {\Sigma'}^G$ es puramente inseparable, para todo $b \in {\Sigma'}^G$, existe $n \in \mathbb{N}$ tal que $b^{p^n} \in \Sigma$ (donde $0 < p = \operatorname{car} \Sigma$). Por tanto, para todo $b \in \bar{A}$, existe $n \in \mathbb{N}$ tal que $b^{p^n} \in A$ (pues b^{p^n} es entero sobre A). Entonces $\operatorname{Spec} \bar{A} \to \operatorname{Spec} A$ es biyectiva, pues la aplicación $\operatorname{Spec} A \to \operatorname{Spec} \bar{A}$, $\mathfrak{p} \mapsto \mathfrak{p}' = \{b \in \bar{A} \colon b^{p^n} \in \mathfrak{p}$ para algún $n\}$, es su inversa. □

6. Proposición : *Sea $A \to B$ un morfismo finito e inyectivo entre anillos íntegros y A íntegramente cerrado. Sea $\mathfrak{p}_x \subset B$ un ideal primo y $\mathfrak{p}_y = \mathfrak{p}_x \cap A$. Entonces* $\dim B_x = \dim A_y$.

Demostración. Dada una cadena estricta de ideales primos de B

$$\mathfrak{m}_x \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_m$$

induce, cortando con A, una cadena de ideales primos $\mathfrak{m}_y \supset A \cap \mathfrak{p}_1 \supset \cdots \supset A \cap \mathfrak{p}_m$ cuyas inclusiones son estrictas, pues las fibras de un morfismo finito son de dimensión cero. Por tanto, $\dim B_x \leq \dim A_y$.

Por otra parte, sea

$$\mathfrak{m}_y \supset \mathfrak{p}'_1 \supset \cdots \supset \mathfrak{p}'_n$$

una cadena estricta de ideales primos de A. Por el teorema de descenso podemos construir una cadena de ideales primos de B

$$\mathfrak{m}_x \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_m$$

tal que $\mathfrak{p}'_i = A \cap \mathfrak{p}_i$. Por tanto, $\dim B_x \geq \dim A_y$ y $\dim B_x = \dim A_y$. □

2.4 Lema de Normalización de Noether. Teorema de los ceros de Hilbert

1. Definición : 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 $f \colon A \to B$ es un morfismo de k-álgebras, diremos que el morfismo inducido $f^* \colon \operatorname{Spec} B \to \operatorname{Spec} A$ es un morfismo de variedades algebraicas.

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

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

es inyectivo; es decir, cuando cualquier relación algebraica $\sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} \xi_1^{i_1} \ldots \xi_n^{i_n} = 0$, con coeficientes en k, tenga todos sus coeficientes nulos.

3. Lema de normalización de Noether : *Sea $A = k[\xi_1, \ldots, \xi_n]$ una k-álgebra de tipo finito. Supongamos que k tiene un número infinito de elementos*[1]*. Existe un morfismo finito e inyectivo*

$$k[x_1, \ldots, x_r] \hookrightarrow A$$

"Toda variedad algebraica afín se proyecta con fibras finitas en un espacio afín".

[1] Esta hipótesis no es necesaria, sólo la imponemos porque la demostración del lema es algo más sencilla.

Demostración. Vamos a hacerlo por inducción sobre n. Para $n=0$, no hay nada que decir. Supongamos que el teorema es cierto hasta $n-1$.

Si los $\{\xi_i\}$ son algebraicamente independientes entre sí, entonces $k[\xi_1,\ldots,\xi_n] = k[x_1,\ldots,x_n]$. Podemos suponer que existe $p(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$, no nulo, tal que $p(\xi_1,\ldots,\xi_n)=0$.

Escribamos $p(x_1,\ldots,x_n) = p_s(x_1,\ldots,x_n) + p_{s-1}(x_1,\ldots,x_n) + \ldots + p_0(x_1,\ldots,x_n)$ como suma de polinomios $p_i(x_1,\ldots,x_n)$ homogéneos de grado i. Sean $x_i = x_i' + \lambda_i x_n$, entonces

$$\begin{aligned}&p(x_1'+\lambda_1 x_n,\ldots,x_{n-1}'+\lambda_{n-1}x_n,x_n) = p_s(\lambda_1,\ldots,\lambda_{n-1},1)x_n^s +\\ &\text{polinomio en } x_1',\ldots,x_{n-1}',x_n \text{ de grado en } x_n \text{ menor que } s\end{aligned}$$

Así pues, si elegimos $\lambda_1,\ldots,\lambda_{n-1}\in k$ de modo que $p_s(\lambda_1,\ldots,\lambda_{n-1},1)\neq 0$, tendremos que ξ_n es entero sobre $k[\xi_1',\ldots,\xi_{n-1}']$, con $\xi_i' = \xi_i - \lambda_i\xi_n$. Por tanto, la composición

$$k[x_1,\ldots,x_r] \underset{\text{Hip.ind.}}{\overset{\text{finito}}{\hookrightarrow}} k[\xi_1',\ldots,\xi_{n-1}'] \overset{\text{finito}}{\hookrightarrow} k[\xi_1',\ldots,\xi_{n-1}',\xi_n] = k[\xi_1,\ldots,\xi_{n-1},\xi_n]$$

es un morfismo finito. □

4. Teorema de los ceros de Hilbert : *Sea A una k-álgebra de tipo finito y $\mathfrak{m}$ un ideal maximal. Entonces $A/\mathfrak{m}$ es una extensión finita de k. En particular, si k es algebraicamente cerrado, entonces $k = A/\mathfrak{m}$: "Todo punto cerrado de una variedad algebraica afín sobre un cuerpo algebraicamente cerrado es racional".*

Demostración. Obviamente $A/\mathfrak{m}$ es una k-álgebra de tipo finito sobre k. Por el lema de normalización de Noether, existe un morfismo finito inyectivo

$$k[x_1,\ldots,x_r] \hookrightarrow A/\mathfrak{m}$$

Por tanto, $k[x_1,\ldots,x_r]$ ha de tener dimensión cero, luego $r=0$ y concluimos. □

5. Ejercicio : Sean $X = \operatorname{Spec} A$ y $Y = \operatorname{Spec} B$ dos variedades algebraicas sobre un cuerpo algebraicamente cerrado k. Definamos $X \times_k Y := \operatorname{Spec} A \otimes_k B$. Probar que los puntos cerrados de $X\times_k Y$ son el producto cartesiano de los puntos cerrados de X y los puntos cerrados de Y.

6. Proposición : *Si $f^*\colon X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ es un morfismo entre variedades algebraicas afines, entonces la imagen de un punto cerrado es un punto cerrado.*

Demostración. Si x es un punto cerrado de X e y es su imagen por f^*, entonces $A/\mathfrak{p}_y \to B/\mathfrak{m}_x$ es inyectivo. Por el teorema de los ceros de Hilbert, $B/\mathfrak{m}_x$ es una extensión finita de k, por tanto $A/\mathfrak{p}_y$ es una k-álgebra finita e íntegra, luego es un cuerpo; es decir, y es un punto cerrado. □

7. Corolario : *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 $U_a \hookrightarrow X$. □

8. Definición : Diremos que $X = \operatorname{Spec} A$ es íntegra si A es un anillo íntegro. Diremos que $X = \operatorname{Spec} A$ es reducida si A es un anillo reducida.

9. Corolario (Forma fuerte de los ceros de Hilbert) : *Sea A una k-álgebra de tipo finito. Si $f \in A$ pertenece a todo ideal maximal, entonces es nilpotente. En particular, si $X = \operatorname{Spec} A$ es una variedad algebraica reducida sobre un cuerpo algebraicamente cerrado, entonces una función es nula si y sólo si se anula en todos los puntos racionales.*

Demostración. Por el corolario anterior, los ideales maximales de A_f, se corresponden con los ideales maximales de A que no contienen a f. Por tanto, si f pertenece a todo ideal maximal, entonces el espectro maximal de A_f es vacío, luego $A_f = 0$ y por tanto f es nilpotente. □

10. Corolario : *Dos subconjuntos cerrados de una variedad algebraica afín son iguales si y sólo si contienen los mismos puntos cerrados.*

Demostración. Una función se anula sobre todos los puntos de un cerrado de una variedad algebraica si y sólo si se anula sobre todos los puntos cerrados del cerrado, por el corolario anterior. Como todo cerrado son los ceros del ideal de todas las funciones que se anulan sobre él, hemos terminado. □

2.5 Ideales primarios. Interpretación geométrica

Queremos demostrar que todo ideal de un anillo noetheriano viene definido por condiciones infinitesimales en un número finito de puntos del espectro. Desde el punto de vista aritmético, esto puede entenderse como el teorema de Euclides para anillos noetherianos. Comencemos con los ideales primarios que serán los definidos por condiciones infinitesimales en un punto.

1. Definición : Sea A un anillo. Un ideal $\mathfrak{q} \neq A$ 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. Ejemplo :
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. Definición : Dado un ideal $I \subseteq A$, llamaremos radical de I, y lo denotaremos $r(I)$, a

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

Observemos que si $\pi \colon A \to A/I$ es el morfismo de paso al cociente, entonces el radical de I es la antimagen por π del radical de A/I. Por tanto, el radical de un ideal es la intersección de los ideales primos que lo contienen.

4. 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 $b \in \mathfrak{p}$. □

Sea $\mathfrak{q}$ un ideal primario. Diremos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario ó que $\mathfrak{p}$ es el ideal primo asociado a $\mathfrak{q}$ cuando $\mathfrak{p}$ es el radical de $\mathfrak{q}$. 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 : *Si $\mathfrak{m}$ es un ideal maximal, entonces todo ideal de radical $\mathfrak{m}$ es primario. En particular, todas las potencias $\mathfrak{m}^n$ 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 $A = \mathbb{C}[x_1, \dots, x_n]$, si consideramos el ideal maximal $\mathfrak{m}$ formado por todos los polinomios que se anulan en cierto punto racional $(a_1, \dots, a_n)$ y ponemos $t_i = x_i - a_i$, entonces

$$A/\mathfrak{m}^r = \mathbb{C}[t_1, \dots, t_n]/(t_1, \dots, t_n)^r = \begin{bmatrix} \text{Polinomios de grado} \\ < r \text{ en } t_1, \dots, t_n \end{bmatrix}$$

y la reducción módulo $\mathfrak{m}^r$ de cualquier polinomio coincide con el clásico desarrollo de Taylor hasta el orden $r-1$ en el punto $(a_1, \dots, a_n)$. Por tanto, el ideal $\mathfrak{m}$-primario $\mathfrak{q}$ está formado por todas las funciones $f \in A$ cuyo desarrollo de Taylor $\bar{f} \in A/\mathfrak{m}^r$, en el punto definido por $\mathfrak{m}$, satisface las relaciones impuestas por cierto ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}^r$. Por ello diremos que los ideales primarios de radical maximal $\mathfrak{m}_x$ son los ideales definidos por condiciones infinitesimales en el punto cerrado x.

Una base del $\mathbb{C}$-espacio vectorial dual de $A/\mathfrak{m}^r$, la constituyen las formas lineales

$$\omega_\alpha = \frac{\partial^{|\alpha|}}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n}$$

con $\alpha = (\alpha_1, \dots, \alpha_n)$ y $|\alpha| = \alpha_1 + \cdots + \alpha_n < r$, definidas por $\omega_\alpha(\bar{f}) = \frac{\partial^{|\alpha|} f}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n}(a_1, \dots, a_n)$. Por tanto, todo ideal de $A/\mathfrak{m}^r$ está definido por un sistema de s-ecuaciones

$$\sum_\alpha \lambda_{i,\alpha} \omega_\alpha(\bar{f}) = 0, \quad 1 \leq i \leq s$$

Es decir, los ideales $\mathfrak{m}$-primarios son ideales formados por las funciones f que verifican un sistema de s-ecuaciones

$$\sum_\alpha \lambda_{i,\alpha} \frac{\partial^{|\alpha|} f}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n}(a_1, \dots, a_n) = 0, \quad 1 \leq i \leq s$$

(variando s,$\lambda_{i,\alpha}$ se obtienen todos los ideales $\mathfrak{m}$-primarios)

Por tanto, cada ideal $\mathfrak{m}$-primario viene definido por ciertas relaciones entre las derivadas parciales iteradas en el punto $(a_1, \dots, a_n)$.

6. Proposición : *Sea S un sistema multiplicativo de un anillo A y sea $\mathfrak{q}$ un ideal $\mathfrak{p}_x$-primario.*

1. *Si $\mathfrak{p}_x$ corta a S, entonces $\mathfrak{q}A_S = A_S$.*
2. *Si $\mathfrak{p}_x$ no corta a S, entonces $\mathfrak{q}A_S$ es un ideal $\mathfrak{p}_x A_S$-primario y $\mathfrak{q} = A \cap (\mathfrak{q}A_S)$. En particular:*

$$\mathfrak{q} = A \cap (\mathfrak{q}A_x)$$

Por tanto, dos ideales $\mathfrak{p}_x$-primarios coinciden si coinciden al localizar en x.

Demostración. 1. Si $s \in S \cap \mathfrak{p}_x$, entonces $\mathfrak{q}$ contiene alguna s^n, que es invertible en A_S; luego $\mathfrak{q}A_S = A_S$.

2. Si $S \cap \mathfrak{p}_x = \emptyset$, entonces $\mathfrak{p}_x A_S$ es un ideal primo de A_S y es fácil comprobar que $\mathfrak{q}A_S$ es un ideal $\mathfrak{p}_x A_S$-primario. Por último, veamos que $\mathfrak{q} = A \cap (\mathfrak{q}A_S)$. Si $f \in A \cap (\mathfrak{q}A_S)$, entonces $sf \in \mathfrak{q}$ para algún $s \in S$. Ninguna potencia de s está en $\mathfrak{q}$, luego $f \in \mathfrak{q}$. Por tanto, $A \cap (\mathfrak{q}A_S) \subseteq \mathfrak{q}$. La inclusión contraria es evidente. □

Sea $\mathfrak{p}_x$ el ideal primo de un punto $x \in \operatorname{Spec} A$. Denotemos $\mathfrak{m} = \mathfrak{p}_x A_x$. Los ideales de A_x de radical $\mathfrak{m}$ son precisamente los ideales $\mathfrak{m}$-primarios, porque $\mathfrak{m}$ es maximal (estos ideales deben llamarse ideales de <u>condiciones</u> <u>infinitesimales</u> en el punto x, pues en el caso noetheriano vienen determinados por los ideales de los anillos $A_x/\mathfrak{m}^r A_x$). Por tanto, si $\mathfrak{q}$ es un ideal $\mathfrak{p}_x$-primario y A es noetheriano, existe un r y un ideal $\bar{\mathfrak{q}}$ de $A_x/\mathfrak{p}_x^r A_x$ tal que

$$\mathfrak{q} = \pi^{-1}(\bar{\mathfrak{q}})$$

siendo $\pi\colon A \to A_x/\mathfrak{p}_x^r A_x$ el morfismo natural. Recíprocamente, si $\mathfrak{q} = \pi^{-1}(\bar{\mathfrak{q}})$, entonces $\mathfrak{q}$ es un ideal $\mathfrak{p}_x$-primario.

7. Ejemplo : Si un ideal primo $\mathfrak{p}$ no es maximal, pueden existir ideales de radical $\mathfrak{p}$ que no son primarios. Fijemos en un plano afín un punto racional p y una recta r que pase por él. Sea $\mathfrak{m}_p$ el ideal maximal del punto y $\mathfrak{p}_r$ el ideal primo del punto genérico de la recta. 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 sobre un cono en $\mathbb{A}^3$ 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 $\mathfrak{m}$ denota el ideal maximal del vértice del cono. En efecto, la ecuación del plano tangente al cono a lo largo de la generatriz está en $A \cap {\mathfrak{p}_{gt}}^2 A_{gt}$ pero no está en ${\mathfrak{p}_{gt}}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal ${\mathfrak{p}_{gt}}^2$ no es primario.

2.6 Existencia y unicidad de las descomposiciones primarias

1. Definición : Diremos que un ideal $\mathfrak{q}$ de un anillo A es <u>irreducible</u> 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 noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún n. Por tanto, $(\operatorname{Ker} b) \cap (\operatorname{Im} b^n) = 0$. Como $\mathfrak{q}$ es irreducible, debe ser $\operatorname{Ker} b = 0$ ó $\operatorname{Im} b^n = 0$. Por hipótesis $\operatorname{Ker} b \neq 0$, luego $\operatorname{Im} b^n = 0$ y por tanto b es nilpotente. □

3. Teorema de existencia : *Sea A un anillo noetheriano. Todo ideal $I \neq A$ es intersección finita de ideales irreducibles de A. Por tanto, todo ideal $I \neq A$ 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 $I \underset{\neq}{\subset} I'$ (pues con I' se repite el argumento y así sucesivamente y se concluye por noetherianidad). Si I no es irreducible, entonces es intersección de ideales propios: $I = I_1 \cap J_1$. Si I_1 es irreducible hemos terminado; si no, $I_1 = I_{11} \cap I_{12}$, luego $I = I_{11} \cap I_{12} \cap J_1$. Si la inclusión $I \subset I_{12} \cap J_1$ es estricta, tomamos $I_2 = I_{11}, J_2 = I_{12} \cap J_1$; si no, tomamos $I_2 = I_{12}$, $J_2 = J_1$. En ambos casos obtenemos de nuevo que $I = I_2 \cap J_2$, con $I \underset{\neq}{\subset} J_2$, además $I_1 \underset{\neq}{\subset} I_2$. Así sucesivamente, el proceso es finito por noetherianidad, luego para cierto n, $I = I_n \cap J_n$ con I_n irreducible e $I \underset{\neq}{\subset} J_n$ 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) ni componentes asociadas a un mismo ideal primo ($r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ 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. Teorema de unicidad de las componentes no-sumergidas : *Sea I un ideal de un anillo A y sea $\mathfrak{p}_x$ el ideal primo de las funciones que se anulan en una componente irreducible de $(I)_0$. Si $I = \bigcap_i \mathfrak{q}_i$ es una descomposición primaria reducida, entonces $\mathfrak{p}_x$ es el radical de una componente $\mathfrak{q}_i$ y*

$$\mathfrak{q}_i = A \cap (IA_x)$$

Por tanto, las componentes $\mathfrak{q}_i$ cuyos radicales son mínimos (entre los primos que contienen a I), son únicas.

Demostración. Es claro que $\mathfrak{p}_x$ es el radical de una componente $\mathfrak{q}_i$. Ahora, si $j \neq i$, entonces $\mathfrak{q}_j A_x = A_x$, porque $r(\mathfrak{q}_j)$ corta al sistema multiplicativo $A - \mathfrak{p}_x$. Por tanto

$$IA_x = \bigcap_{j=1}^{n} \mathfrak{q}_j A_x = \mathfrak{q}_i A_x$$

y, por 2.5.6, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_x) = A \cap (IA_x)$. □

Si $I = \cap_i \mathfrak{q}_i$ es una descomposición primaria reducida, las componentes $\mathfrak{q}_i$ cuyos radicales son mínimos se denominan componentes no sumergidas. Una componente $\mathfrak{q}_j$ está sumergida cuando sus ceros están contenidos estrictamente en los ceros de alguna otra componente: $(\mathfrak{q}_j)_0 \underset{\neq}{\subset} (\mathfrak{q}_i)_0$. Las componentes no-sumergidas corresponden a los puntos genéricos de las componentes irreducibles de $(I)_0$, mientras que las componentes sumergidas están asociadas a puntos más pequeños de $(I)_0$.

7. Corolario: *Si los ceros de un ideal I de un anillo noetheriano son puntos aislados, la descomposición primaria reducida de I es única salvo el orden.*

Las componentes sumergidas no son únicas pero sí lo son sus radicales, como vamos a demostrar. Sea $a \in A$ e $I \subset A$ un ideal. Denotaremos

$$(I \colon a) = \{b \in A \colon a \cdot b \in I\}$$

8. Proposición : *Sea* $\mathfrak{q} \subset A$ *un ideal* $\mathfrak{p}$*-primario. Se verifica*

$$(\mathfrak{q} \colon a) = \begin{cases} A & \text{si } a \in \mathfrak{q} \\ \mathfrak{q}' & \text{si } a \notin \mathfrak{q} \end{cases}$$

siendo $\mathfrak{q}'$ *un ideal* $\mathfrak{p}$*-primario que contiene a* $\mathfrak{q}$.

Demostración. Es una sencilla comprobación. □

9. Teorema : *Sea* A *un anillo noetheriano. Sea* $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *una descomposición primaria reducida de* I*. Un ideal primo* $\mathfrak{p}$ *es un ideal primo asociado a un primario de la descomposición primaria de* I *si y sólo si existe* $a \in A$ *de modo que* $(I \colon a) = \mathfrak{p}$.

En particular, los primos asociados a una descomposición primaria reducida de un ideal son independientes de la descomposición.

Demostración. Observemos que $(I \colon a) = (\overset{n}{\underset{i=1}{\cap}} \mathfrak{q}_i \colon a) = \overset{n}{\underset{i=1}{\cap}} (\mathfrak{q}_i \colon a)$. Por la proposición anterior, es fácil concluir que si $(I \colon a) = \mathfrak{p}$, entonces $\mathfrak{p}$ es un ideal primo asociado a la descomposición primaria.

Recíprocamente, supongamos $\mathfrak{p} = r(\mathfrak{q}_1)$. Sea $a \in \overset{n}{\underset{i=2}{\cap}} \mathfrak{q}_i$ y $a \notin \mathfrak{q}_1$; por la proposición anterior $(I \colon a) = (\mathfrak{q}_1 \colon a)$ y es un ideal $\mathfrak{p}$-primario. Si $(\mathfrak{q}_1 \colon a) \neq \mathfrak{p}$, sea $\mathfrak{p}^r$ la primera potencia contenida en $(\mathfrak{q}_1 \colon a)$ y sea $b \in \mathfrak{p}^{r-1}$, $b \notin (\mathfrak{q}_1 \colon a)$. Entonces $(I \colon ab) = \mathfrak{p}$. □

10. Definición : Sea A un anillo noetheriano. Llamaremos ideales primos asociados a un ideal I a los radicales de las componentes de cualquier descomposición primaria reducida de I.

Veamos ahora que los A-módulos $A/\mathfrak{p}_x$, $x \in \operatorname{Spec} A$, son los "ladrillos" de la categoría de los A-módulos noetherianos. El significado preciso viene dado por el siguiente teorema.

11. 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, $A/\alpha \simeq \langle m \rangle \subset M$. Existe $\bar{a} \in A/\alpha$ cuyo anulador es $\mathfrak{p}_1$, siendo $\mathfrak{p}_1$ un primo asociado a α. Luego $A/\mathfrak{p}_1 \subset M$. 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 $M_2 = \pi^{-1}(A/\mathfrak{p}_2)$, siendo $\pi \colon M \to M/M_1$ el morfismo de paso al cociente; así sucesivamente se concluye por noetherianidad.

□

Hasta ahora, hemos desarrollado la descomposición primaria de los ideales de un anillo noetheriano. De modo totalmente análogo podemos desarrollar la descomposición primaria en módulos noetherianos. Indiquemos la línea argumental y dejemos al lector las demostraciones.

12. 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).

13. Definición : Un submódulo $M' \subseteq M$ diremos que es irreducible si no es intersección de dos submódulos estrictamente mayores de M.

14. Proposición : *Los submódulos irreducibles son primarios.*

15. Teorema : *Todo submódulo de un módulo noetheriano es intersección de un número finito de submódulos primarios.*

16. 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.

17. Proposición : *Si M_1,M_2 son submódulos $\mathfrak{p}$-primarios entonces $M_1 \cap M_2$ es $\mathfrak{p}$-primario.*

Por tanto, existen descomposiciones primarias reducidas de los submódulos de un módulo noetheriano.

Dados $m \in M$ y $M' \subset M$, denotaremos $(M' \colon m) = \{a \in A \colon am \in M'\}$.

18. Proposición : *Sea $M' \subset M$ un submódulo primario. Sea $\mathfrak{q}$ el anulador de M/M' y $\mathfrak{p}$ el radical de $\mathfrak{q}$. Se verifica*

$$(M' \colon m) = \begin{cases} A & si\ a \in M' \\ \mathfrak{q}' & si\ a \notin M' \end{cases}$$

siendo $\mathfrak{q}'$ un ideal $\mathfrak{p}$-primario, que contiene a $\mathfrak{q}$.

19. Proposición : *Sea $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida de M'. Un ideal primo $\mathfrak{p}$ es un ideal primo asociado a la descomposición primaria de M' si y sólo si existe $m \in M$ tal que $(M' \colon m) = \mathfrak{p}$.*

20. Teorema de unicidad de las componentes no-sumergidas : *Sea M' un submódulo de un módulo noetheriano M y $M' = M_1 \cap \cdots \cap M_n$ una descomposición primaria reducida. Sea $\mathfrak{p}_x$ un ideal primo minimal entre los ideales primos asociados a la descomposición primaria de M'. Entonces*

$$M_i = M \cap M'_x$$

21. Ejercicio : Probar que los ideales primos minimales asociados a un submódulo M' de un módulo noetheriano M, coinciden con los ideales primos minimales asociados al ideal anulador de M/M'.

2.7 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 primo asociado. Denotemos por J la intersección de los $\mathfrak{q}_i$ contenidos en $\mathfrak{p}_x$. Entonces*

$$J = A \cap I_x$$

Por tanto, el ideal J no depende de la descomposición primaria escogida.

Demostración. Se deduce de la Proposición 2.5.6 □

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 verifica*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}'_j \cap \mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$$

para todo j. En consecuencia, si $\mathfrak{q}_i''$ son ideales $\mathfrak{p}_{x_i}$-primarios, y cada uno de ellos aparece en alguna descomposición primaria de I, entonces

$$I = \mathfrak{q}_1'' \cap \cdots \cap \mathfrak{q}_n''$$

Demostración. Reordenado, podemos suponer que $\mathfrak{q}_i \subseteq \mathfrak{p}_{x_j} \Leftrightarrow i \leq j$. Por la proposición anterior $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} = \mathfrak{q}_1' \cap \cdots \cap \mathfrak{q}_{j-1}'$ para todo j. Por tanto,

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}_j' = \mathfrak{q}_1' \cap \cdots \cap \mathfrak{q}_{j-1}' \cap \mathfrak{q}_j' = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

Cortando con $\mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$ concluimos. □

3. Proposición : *Sea A un anillo noetheriano. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m \subset A$ una descomposición primaria reducida de radicales $\mathfrak{p}_{x_i}$. Sea $n_i \in \mathbb{N}$ tal que $\mathfrak{p}_{x_i}^{n_i} \subseteq \mathfrak{q}_i$ y denotemos $\alpha_i^{n_i}$ el ideal $\mathfrak{p}_{x_i}$-primario antimagen de $(I_{x_i} + \mathfrak{p}_{x_i}^{n_i}) \cdot A_{x_i}$ por el morfismo de localización $A \to A_{x_i}$. Entonces*

$$I = \mathfrak{q}_1 \cap \cdots \cap \alpha_i^{n_i} \cap \cdots \cap \mathfrak{q}_m$$

Demostración. Denotemos por J la intersección de los $\mathfrak{q}_j$ distintos de $\mathfrak{q}_i$. Como $I \subseteq \alpha_i^{n_i} \subseteq \mathfrak{q}_i$,

$$I = I \cap J \subseteq \alpha_i^{n_i} \cap J \subseteq \mathfrak{q}_i \cap J = I$$

luego las inclusiones son igualdades y concluimos.

□

El ideal $\alpha_i^{n_i}$ es el ideal de funciones de A cuyo desarrollo de Taylor de orden n_i en x_i coincide con el desarrollo de Taylor de orden n_i en x_i de alguna función de I.

Procedamos a ver que entre las descomposiciones primarias de I hay una canónica. Siguiendo las notaciones anteriores, para cada i, sea n_i el mínimo tal que $\alpha_i^{n_i}$ aparezca en alguna descomposición primaria de I. Entonces

$$I = \alpha_1^{n_1} \cap \cdots \cap \alpha_m^{n_m}$$

Demos un método de cálculo. Procedemos recurrentemente. Dado $\mathfrak{p}_{x_j}$, supongamos que ya tenemos calculados los $\alpha_i^{n_i}$, para todo $\mathfrak{p}_{x_i}$ contenido en $\mathfrak{p}_{x_j}$. Reordenando, supongamos que son $\alpha_1^{n_1}, \dots, \alpha_{j-1}^{n_{j-1}}$. Entonces n_j es el mínimo número natural tal que $\alpha_1^{n_1} \cap \cdots \cap \alpha_{j-1}^{n_{j-1}} \cap \mathfrak{p}_{x_j}^{n_j} \subseteq I_{x_j}$.

Así sucesivamente vamos determinando los n_j y obteniendo la descomposición primaria canónica

$$I = \alpha_1^{n_1} \cap \cdots \cap \alpha_m^{n_m}$$

Del mismo modo obtenemos descomposiciones primarias canónicas para los submódulos de un módulo noetheriano. Las demostraciones de las siguientes proposiciones se pueden copiar de sus equivalentes en el caso de ideales.

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 primo asociado. 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 $\{L_i\}_{1\leq i\leq n}$ son submódulos $\mathfrak{p}_{x_i}$-primarios y cada uno de ellos aparece en alguna descomposición primaria de M', entonces

$$M' = L_1 \cap \cdots \cap L_n$$

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'.

2.8 Teoría de la dimensión en variedades algebraicas

Vamos a desarrollar la teoría de la dimensión en variedades algebraicas apoyándonos fundamentalmente en el lema de normalización de Noether.

1. Definición: Una extensión de cuerpos $K \to K'$ se dice algebraica si todo elemento de K' es entero sobre K.

Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos y $\xi_1, \dots, \xi_n \in \Sigma$. Diremos que ξ_n es algebraico sobre $\xi_1, \dots, \xi_{n-1}$ si ξ_n es entero sobre $k(\xi_1, \dots, \xi_{n-1})$.

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

3. Teorema: *Sea $k \hookrightarrow \Sigma$ una extensión de cuerpos, generada por un número finito de elementos. Existen bases de trascendencia de Σ sobre k y todas tienen el mismo número de elementos, llamado <u>grado de trascendencia</u> de Σ sobre k.*

Demostración. Sea $\Sigma = k(\xi_1, \dots, \xi_r)$. Reordenando los generadores si fuera preciso, podemos suponer que $\xi_1, \dots, \xi_n$ son algebraicamente independientes sobre k y ξ_i es algebraico sobre $\xi_1, \dots, \xi_n$ para todo $i > n$. Por 2.2.2, Σ es una extensión algebraica de $k(\xi_1, \dots, \xi_n)$, luego $\{\xi_1, \dots, \xi_n\}$ es una base de trascendencia de Σ sobre k.

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

$$k(\xi_1, \dots, \xi_i, y_{i+1}, \dots, y_m) \hookrightarrow k(\xi_1, \dots, \xi_{i-1}, \xi_i, y_i, \dots, y_m) \underset{\text{Inducción}}{\hookrightarrow} \Sigma$$

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

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

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

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

6. Teorema : *Sea A una k-álgebra de tipo finito íntegra. La dimensión de Krull de A coincide con el grado de trascendencia de su cuerpo de fracciones.*

Demostración. Vamos a demostrarlo por inducción sobre el grado de trascendencia. Si el grado de trascendencia del cuerpo de fracciones es cero, entonces es una extensión finita de k, luego A es una k-álgebra finita íntegra. Por tanto, A es un cuerpo y su dimensión de Krull es cero.

Por el lema de Noether, existe un morfismo finito $k[x_1,\dots,x_n]\hookrightarrow A$, que induce un morfismo finito entre sus cuerpos de fracciones (pruébese)

$$k(x_1,\dots,x_n)\to\Sigma$$

luego $\operatorname{gr}\operatorname{tr}\Sigma=\operatorname{gr}\operatorname{tr}k(x_1,\dots,x_n)=n$. Por otra parte, $\dim k[x_1,\dots,x_n]=\dim A$, por 2.3.2. Por tanto, podemos suponer que $A=k[x_1,\dots,x_n]$ y tenemos que ver que su dimensión de Krull es n. Sea

$$0\subset\mathfrak{p}_1\subset\cdots\subset\mathfrak{p}_m$$

una cadena irrefinable de ideales primos de $k[x_1,\dots,x_n]$. Sea $p\in\mathfrak{p}_1$, no nulo e irreducible. Como $k[x_1,\dots,x_n]$ es un dominio de factorización única (p) es un ideal primo, luego $(p)=\mathfrak{p}_1$. El anillo $k[x_1,\dots,x_n]/(p)$ es íntegro y su cuerpo de fracciones es de grado de trascendencia $n-1$. Por inducción sobre el grado de trascendencia, las cadenas de ideales primos en $k[x_1,\dots,x_n]/(p)$ son de longitud menor o igual que $n-1$. Haciendo cociente por (p), la cadena anterior define una cadena

$$\bar{0}\subset\bar{\mathfrak{p}}_2\subset\cdots\subset\bar{\mathfrak{p}}_m$$

luego $m-1\leq n-1$ y $\dim A\leq n$. Por otra parte

$$0\subset(x_1)\subset(x_1,x_2)\subset\cdots\subset(x_1,\dots,x_n)$$

es una cadena de longitud n, luego $\dim A\geq n$. En conclusión A tiene dimensión de Krull n. □

Observemos que $\dim A=\dim A_{\text{red}}$. Por tanto, la dimensión de una variedad irreducible $\operatorname{Spec}A$ coincide con la dimensión de $\operatorname{Spec}A_{\text{red}}$, que es una variedad algebraica íntegra. En general, toda variedad algebraica es unión de variedades algebraicas irreducibles y la dimensión de la variedad es el máximo de las dimensiones de sus componentes irreducibles.

7. Ejercicio : Sean $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $X \times_k Y := \operatorname{Spec} A \otimes_k B$ variedades algebraicas. Demostrar que

$$\dim(X \times_k Y) = \dim X + \dim Y$$

8. Ejercicio : Sea $f\colon X \to Y$ un morfismo entre variedades algebraicas irreducibles. Sea $C \subset X$ un cerrado. Demostrar que

$$\dim C \geq \dim \overline{f(C)}$$

9. Teorema del ideal principal de Krull : *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra. Sea $f \in A$, no nula ni invertible. Entonces*

$$\dim(f)_0 = \dim X - 1$$

Es más, todas las componentes irreducibles de $(f)_0$ son de dimensión $\dim X - 1$.

Demostración. Si $X = \operatorname{Spec} k[x_1, \ldots, x_n]$ 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 $k[x_1, \ldots, x_n]/(p_i)$ 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 2.8.6, $\dim X = \dim U_a$ 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 $(f)_0 = C_1$.

Consideremos, por el lema de normalización de Noether, un morfismo finito $k[x_1, \ldots, x_n] \hookrightarrow A$. La inclusión $i\colon k[x_1, \ldots, x_n][f] \hookrightarrow A$ es un morfismo finito inyectivo. Además, $i^{*-1}((f)_0) = (f)_0$, por tanto la dimensión de $(f)_0$ en $\operatorname{Spec} k[x_1, \ldots, x_n][f]$ es la misma que la de $(f)_0$ en $\operatorname{Spec} A$. Por tanto, podemos suponer que $A = k[x_1, \ldots, x_n][f]$.

Sea $p(x_1, \ldots, x_n, x_{n+1})$ un polinomio irreducible tal que $p(x_1, \ldots, x_n, f) = 0$. El epimorfismo

$$k[x_1, \ldots, x_{n+1}]/(p(x_1, \ldots, x_n, x_{n+1})) \to k[x_1, \ldots, x_n][f],\ \bar{x}_{n+1} \mapsto f$$

es un isomorfismo, porque $k[x_1, \ldots, x_{n+1}]/(p(x_1, \ldots, x_n, x_{n+1}))$ es un anillo de dimensión n, íntegro y si hubiese núcleo la dimensión de $k[x_1, \ldots, x_n][f]$ sería menor que n.

En conclusión $A = k[x_1, \ldots, x_{n+1}]/(p(x_1, \ldots, x_n, x_{n+1}))$ y $f = x_{n+1}$. Por tanto,

$$\begin{aligned}\dim(f)_0 &= \dim A/(f) = \dim k[x_1, \ldots, x_{n+1}]/(p(x_1, \ldots, x_n, x_{n+1}), x_{n+1}) \\ &= \dim k[x_1, \ldots, x_n]/(p(x_1, \ldots, x_n, 0)) = n-1\end{aligned}$$

□

10. Definición : Una cadena de cerrados irreducibles diremos que es maximal si no está incluida en ninguna otra mayor.

11. Corolario : *Todas las cadenas maximales de cerrados irreducibles de una variedad algebraica irreducible tienen la misma longitud, que es la dimensión de Krull de la variedad.*

Demostración. Sea $X = \operatorname{Spec} A$ la variedad algebraica irreducible. Como $\operatorname{Spec} A = \operatorname{Spec} A_{\text{red}}$, podemos suponer que la variedad algebraica es íntegra. Demostraremos el corolario por inducción sobre la dimensión de Krull.

Sea $X \supset X_1 \supset \cdots \supset X_m$ una cadena de cerrados irreducibles maximal. Sea $f \in A$ una función no nula que se anule en X_1. Si $(f)_0 = Y_1 \cup \cdots \cup Y_r$ es la descomposición de $(f)_0$ en cerrados irreducibles, X_1 es una de las componentes de la descomposición. Por el teorema anterior $\dim X_1 = \dim X - 1$, luego por inducción sobre la dimensión $m - 1 = \dim X_1 = \dim X - 1$, y por tanto $m = \dim X$. □

12. 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.

13. 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. □

14. Proposición : *Si* $X = \operatorname{Spec} A$ *es una variedad algebraica irreducible y* $x \in X$ *un punto cerrado, entonces* $\dim X = \dim A_x$*.*

Demostración. La dimensión de Krull de A_x coincide con la máxima longitud de las cadenas de cerrados irreducibles de X que pasan por x. Ahora bien, todas las cadenas maximales de cerrados irreducibles tienen longitud $\dim X$.

□

15. 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* $f_1, \dots f_r$ *de* X *tales que una de las componentes irreducibles de* $(f_1, \dots, f_r)_0$ *sea* Y *es* $r = n - m$ *(puede imponerse además que todas las componentes sean de dimensión* m*).*

Demostración. Es fácil probar, aplicando recurrentemente el teorema del ideal principal de Krull, que todas las componentes irreducibles de $(f_1, \dots, f_r)_0$ tienen dimensión mayor o igual que $n - r$. Por tanto, tenemos que probar sólo la existencia de tales funciones para $r = n - m$.

Sea f_1 una función que se anule en todo Y y no en X. Escribamos $(f_1)_0 = \cup_i C_i$, donde C_i son cerrados irreducibles de dimensión $n-1$. 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.

□

16. Corolario: *Sea* X *una variedad algebraica irreducible de dimensión* n *y* $x \in X$ *un punto cerrado. El número mínimo de funciones* $f_1, \dots, f_r$ *tales que* $(f_1, \dots, f_r)_0 \cap U = \{x\}$*, en algún entorno abierto* U *de* x*, es* n*.*

17. Ejercicio : Sean Y, Y' subvariedades irreducibles de $\mathbb{A}^n$. Llamemos codimensión de Y en $\mathbb{A}^n$, que denotaremos $\operatorname{codim} Y$, a $n - \dim Y$. Supongamos que $Y \cap Y' \neq 0$. Demuéstrese que

$$\operatorname{codim} Y + \operatorname{codim} Y' \geq \operatorname{codim}(Y \cap Y')$$

18. Ejercicio : Sea $f \colon X \to Y$ un morfismo entre variedades algebraicas irreducibles. Sea $y \in f(X)$ un punto cerrado. Demuéstrese que

$$\dim f^{-1}(y) \geq \dim X - \dim \overline{f(X)}$$

2.9 Problemas

1. Definir el grupo multiplicativo G_m de los elementos no nulos de un cuerpo k, como variedad algebraica sobre k, así como los morfismos $G_m \times G_m \to G_m$ y $G_m \to G_m$ correspondientes al producto y paso al inverso. Análogamente para el grupo aditivo G_a de los elementos de k con la operación de la suma de k.

2. Sea $\mu_6 = \operatorname{Spec} k[x]/(x^6 - 1)$ el grupo de las raíces sextas de la unidad sobre un cuerpo k. Determinar si es una variedad íntegra o reducida, y calcular el número de componentes irreducibles cuando $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$.

   Definir los morfismos $\mu_6 \times \mu_6 \to \mu_6$, $\mu_6 \to \mu_6$ correspondientes a la noción intuitiva de producto y paso al inverso en este grupo. Definir el concepto de morfismo de grupos $\mu_6 \to \mu_6$ y del núcleo del mismo. Probar entonces que $\psi\colon \mu_6 \to \mu_6, \alpha \mapsto \alpha^2$, es morfismo de grupos y calcular el núcleo.

3. Sea X una variedad algebraica afín íntegra. Si dos morfismos de X en otra variedad algebraica afín coinciden en un abierto no vacío de X, probar que coinciden en X.

4. Sea $k \hookrightarrow K$ una extensión finita de cuerpos y $X = \operatorname{Spec} A$ una k-variedad algebraica. Probar que el morfismo natural $X_K = \operatorname{Spec} A \otimes_k K \to X = \operatorname{Spec} A$ de cambio de base es epiyectivo y cerrado.

5. Sea A un anillo íntegro y $a \in A$ no invertible, ni nula. Probar que el morfismo de localización $A \to A_a$ no es finito.

6. Sea $\pi\colon X = \operatorname{Spec} A \to \mathbb{A}^1 = \operatorname{Spec} k[x]$ un morfismo finito y supongamos que X es una variedad algebraica íntegra (de dimensión 1). Probar que el número de puntos (contando multiplicidades) de las fibras de π es constante.

7. Sea I un ideal de un anillo noetheriano. Probar que $I = r(I)$ si y sólo si I es intersección de un número finito de ideales primos.

8. Calcular los ideales maximales de $\mathbb{C}[x_1, \dots, x_n]$ y $\mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - 1)$.

9. Probar que si X e Y son variedades algebraicas íntegras sobre un cuerpo k algebraicamente cerrado, entonces $X \times_k Y$ es íntegra. (Indicación: Usar el teorema de los ceros de Hilbert).

10. Sea $X = \operatorname{Spec} A$ una variedad íntegra sobre un cuerpo k algebraicamente cerrado. Probar que para toda extensión $k \to K$, la variedad $X_K = \operatorname{Spec} A \otimes_k K$ es íntegra. (Póngase K unión de álgebras finito generadas).

11. Sea $\bar{k}$ el cierre algebraico de k. Probar que dos ideales primos $\mathfrak{p} = (f_i)_{i \in I}$, $\mathfrak{q} = (g_j)_{j \in J}$ de $k[x_1, \dots, x_n]$ son iguales si y sólo si las soluciones en $\bar{k}$ de los dos sistemas de ecuaciones $\{f_i = 0\}$, $\{g_j = 0\}$ son las mismas.

12. 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 <u>birracionales</u>. Diremos que X e Y son <u>birracionalmente equivalentes</u> 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 $y^2 = x^2 + x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcular el área del "ojo del lazo" definido por la curva $y^2 = x^2 + x^3$.

(b) Sea C la cúbica plana $y^2 = x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}^1 \to C$, $x = t^2$, $y = t^3$.

13. Supóngase conocido el siguiente resultado: "Si $k \hookrightarrow K$ es una extensión finita de cuerpos de característica cero, entonces existe un $\xi \in K$ de modo que $K = k(\xi)$". Demostrar que toda variedad algebraica íntegra, sobre $\mathbb{C}$, es birracionalmente isomorfa a una hipersuperficie de un espacio afín.

14. Probar que si A es un anillo íntegro entonces (0) es irreducible. Probar que los ideales primos son irreducibles.

15. Sea $A = k[x,y]/(x,y)^2$. Escribir el ideal (0) como intersección de ideales irreducibles ¿Es el ideal (0) un ideal primario?

16. Sea A un anillo noetheriano e $I \subseteq A$ un ideal. Si I no es irreducible, sean I_1 e I_2 dos ideales que contienen estrictamente a I tales que $I = I_1 \cap I_2$. Repitiendo este proceso con I_1 e I_2 y así sucesivamente, probar que este proceso termina en un número finito de pasos, obteniéndose I como intersección de un número finito de ideales irreducibles.

17. Probar que en $k[x,y]$ se cumple que $(x) \cap (x,y)^2 = (x) \cap (y, x^2)$ ¿Son las descomposiciones primarias únicas?

18. 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?

19. Probar que los ideales primos asociados al ideal cero de un anillo noetheriano A, son los ideales primos de A que coinciden con el anulador de algún elemento de A.

20. Sea $\mathcal{O}$ un anillo noetheriano local de ideal maximal $\mathfrak{m}$. Sea $I \subset \mathcal{O}$ un ideal tal que $r(I) = \mathfrak{m}$. Probar que $\mathfrak{m}^r \subseteq I$ precisamente cuando $\overline{\mathfrak{m}^r} \subseteq \bar{I}$ en $\mathcal{O}/\mathfrak{m}^{r+1}$.

21. Calcular la descomposición primaria de $I = (xy, -y + x^2 + y^2)$ en $\mathbb{C}[x,y]$.

22. Calcular una descomposición primaria reducida de los ideales

(a) $I = (x,y) \cdot (x, y-1)$ en $\mathbb{C}[x,y]$.

(b) $I = (x) \cdot (x,y) \cdot (x, y-1)$ en $\mathbb{C}[x,y]$.

23. Hallar la descomposición primaria del ideal generado en $\mathbb{C}[x,y]$ por las ecuaciones de:

(a) Un par de rectas y una recta.

(b) Una recta doble y una recta.

(c) Una cónica no singular y una recta.

(d) Una cónica no singular y un par de rectas.

(e) Una cónica no singular y una recta doble.

24. Calcular la multiplicidad de intersección en el origen de la curva $y^2 = x^2 + y^3$ con la curva $y^3 + x^2 = 0$. Es decir, calcular $\dim_{\mathbb{C}}(\mathbb{C}[x,y]/(y^2 - x^2 - y^3, y^3 + x^2))_x$, donde x es el origen.

25. Poner un ejemplo de variedad algebraica que sea la unión de dos componentes no disjuntas, una de dimensión 2, la otra de dimensión 1.

26. Sean $p(x,y)$ y $q(x,y)$ polinomios de $k[x,y]$ sin factores comunes. Demostrar que $k[x,y]/(p(x,y),q(x,y))$ es una k-álgebra finita.

27. Sea $\mathfrak{m} \subset k[x_1,\dots,x_n]$ un ideal maximal. Probar que $\mathfrak{m}$ está generado por n funciones ¿Puede estar generado por $n-1$ funciones?

28. Calcular la dimensión de Krull de $\mathbb{C}[x,y,z]/(x^2+y^2+z^2-1, y^2-x^3)$.

29. Sea $f\colon X \to Y$ un morfismo de imagen densa entre variedades algebraicas irreducibles. Probar que el conjunto de puntos $y \in Y$ tales que la dimensión de Krull de $f^{-1}(y)$ es igual a $\dim X - \dim Y$ contiene un abierto no vacío de Y.

Capítulo 3

Variedades proyectivas

3.1 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.

Del modo más simple, podemos decir que la Geometría Algebraica es el estudio de las soluciones de un sistema de ecuaciones polinómicas en un espacio proyectivo, es decir, el estudio de las variedades algebraicas proyectivas.

En Geometría Lineal el espacio proyectivo de dimensión n se define como el conjunto de rectas (que pasan por el origen) de un espacio vectorial de dimensión $n+1$. En Geometría Algebraica vamos a definir de modo equivalente, a partir de $\mathbb{A}^{n+1} = \operatorname{Spec} \mathbb{C}[x_0, \dots, x_n]$, 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. Así, las subvariedades homogéneas de dimensión mínima serán las rectas que pasan por el origen, que se corresponderán con los puntos cerrados del espacio proyectivo que queremos asociarle a $\mathbb{A}^{n+1}$.

Si $p(x_0, \dots, x_n) \in k[x_0, \dots, x_n]$ es una función que se anula en la variedad homogénea V, escribamos $p(x_0, \dots, x_n) = p_s(x_0, \dots, x_n) + \dots + p_m(x_0, \dots, x_n)$ 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

$$0 = p(\lambda a_0, \dots, \lambda a_n) = \lambda^s p_s(a_0, \dots, a_n) + \dots + \lambda^m p_m(a_0, \dots, a_n), \quad \text{para todo } \lambda$$

Por tanto, $p_i(a_0, \dots, a_n)$ se anula en V, para todo i. En conclusión, $V = (I)_0$, donde I es un ideal generado por polinomios homogéneos. Es fácil ver el recíproco, es decir, si $V = (I)_0$ donde I es un ideal generado por polinomios homogéneos, entonces V es una variedad homogénea.

Denotaremos por $\mathbb{P}^n = \operatorname{Proj} \mathbb{C}[x_0, \dots, x_n]$ el conjunto de ideales primos homogéneos (= generados por polinomios homogéneos) de $\mathbb{C}[x_0, \dots, x_n]$.

Si consideramos en $\mathbb{P}^n$ la topología inducida por $\mathbb{A}^{n+1}$, entonces los puntos cerrados de $\mathbb{P}^n$ se corresponden con las variedades homogéneas de $\mathbb{A}^{n+1}$ de dimensión mínima, que son justamente las rectas de $\mathbb{A}^{n+1}$ que pasan por el origen.

En Geometría Proyectiva se demuestra que $\mathbb{P}^n$ está recubierto por los subconjuntos $U_i = \{$rectas de $\mathbb{C}^{n+1}$ que pasan por el origen y no yacen en el hiperplano $x_i = 0\}$ y que éstos se corresponden con los puntos del espacio afín $\mathbb{A}^n$, del modo siguiente: El morfismo

$$\mathbb{A}^{n+1} - \{x_i = 0\} \to \mathbb{A}^n,\ (\alpha_0, \dots, \alpha_n) \mapsto (\frac{\alpha_0}{\alpha_i}, \dots, \frac{\alpha_n}{\alpha_i})$$

tiene por fibras las rectas que pasan por el origen y no yacen en el hiperplano $x_i = 0$, es decir, induce la igualdad

$$\begin{array}{ccc} U_i = \{\text{rectas } \lambda(\alpha_0, \dots, \alpha_n) \mid \alpha_i \neq 0\} & = & \mathbb{A}^n \\ & & \\ \lambda(\alpha_0, \dots, \alpha_n) & \longrightarrow & (\frac{\alpha_0}{\alpha_i}, \dots, \frac{\alpha_n}{\alpha_i}) \end{array}$$

En Álgebra Conmutativa, veremos que el conjunto $U_i = \{x \in \operatorname{Proj} \mathbb{C}[x_0, \dots, x_n]$ que no yacen en $(x_i)_0\}$ se identifica con $\operatorname{Proj} \mathbb{C}[x_0, \dots, x_n]_{x_i}$ (se dota a $\frac{1}{x_i}$ de grado -1), y la composición de los morfismos

$$\begin{array}{ccccc} U_i & \hookrightarrow & \mathbb{A}^{n+1} - (x_i)_0 & \longrightarrow & \mathbb{A}^n \\ & & (\alpha_0, \dots, \alpha_n) & \longrightarrow & (\frac{\alpha_0}{\alpha_i}, \dots, \frac{\alpha_n}{\alpha_i}) \\ & & \mathbb{C}[x_0, \dots, x_n]_{x_i} & \hookleftarrow & \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] \end{array}$$

induce un homeomorfismo $U_i = \operatorname{Proj} \mathbb{C}[x_0, \dots, x_n]_{x_i} \simeq \operatorname{Spec} \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$. Además se prueba que $\mathbb{P}^n = \underset{i}{\cup} U_i$.

3.2 Espectro proyectivo

Procedamos ahora con todo rigor y generalidad.

1. Definición : Diremos que un anillo $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ es un álgebra graduada, si los R_i son subgrupos de R con la suma y si para cada $r_i \in R_i$ y $r_j \in R_j$, entonces $r_i \cdot r_j \in R_{i+j}$. Diremos que $r_i \in R_i$ es un elemento homogéneo de grado i.

2. Definición : Sea $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo, si está generado por elementos homogéneos.

3. Ejercicio : Probar que un ideal $I \subseteq R$ es homogéneo si y sólo si $I = \underset{n}{\oplus} I_n$, siendo $I_n = I \cap R_n$.

4. Definición : Llamaremos ideal irrelevante de R al ideal $(\underset{n\neq 0}{\oplus} R_n)$.

5. Definición : Llamaremos espectro proyectivo de R, y lo denotaremos $\operatorname{Proj} R$, al conjunto de ideales primos homogéneos de R que no contienen al ideal irrelevante.

Evidentemente $\operatorname{Proj} R \subset \operatorname{Spec} R$. Consideraremos $\operatorname{Proj} R$ como espacio topológico con la topología inicial heredada de la topología de Zariski de $\operatorname{Spec} R$. Si denotamos $(f)_0^h$ a los ideales primos homogéneos que contienen a $f \in R$ y escribimos $f = f_n + f_{n+1} \cdots + f_m$, es obvio que $(f)_0^h = (f_n, \dots, f_m)_0^h = (f_n)_0^h \cap \cdots \cap (f_m)_0^h$. Por tanto, una base de abiertos de la topología de $\operatorname{Proj} R$ son los abiertos

$$U_f^h = \{x \in \operatorname{Proj} R, f \notin \mathfrak{p}_x\}, \quad (f \text{ homogéneo})$$

6. Definición : Llamaremos espacio proyectivo de dimensión n (sobre k) a

$$\mathbb{P}_k^n = \operatorname{Proj} k[x_0, \dots, x_n]$$

7. Definición : Diremos que un morfismo de álgebras $\phi\colon R \to R'$ graduadas es un morfismo graduado de grado $m \in \mathbb{N}$, si transforma funciones de grado n en funciones de grado $n \cdot m$.

Si $\phi\colon R \to R'$ es un morfismo graduado entonces el morfismo inducido $\phi^*\colon \operatorname{Spec} R' \to \operatorname{Spec} R$, aplica ideales primos homogéneos en ideales primos homogéneos. Si suponemos que la imagen del ideal irrelevante de R por ϕ, no está contenido en más ideal primo homogéneo que los que contengan al irrelevante de R', tenemos definido un morfismo

$$\phi^*\colon \operatorname{Proj} R' \to \operatorname{Proj} R, x \mapsto \phi^*(x), \text{ donde } \mathfrak{p}_{\phi*(x)} = \phi^{-1}(\mathfrak{p}_x)$$

8. Ejemplo : Sea $\phi\colon k[x_0, x_1, x_2] \to k[x_0, x_1, x_2]$, $\phi(x_i) = \sum\limits_j \lambda_{ij} x_j$, de modo que $\det(\lambda_{ij}) \neq 0$. Entonces ϕ es un isomorfismo graduado de grado 1, que induce un isomorfismo $\phi^*\colon \mathbb{P}^2 \to \mathbb{P}^2$. Diremos que ϕ es un cambio de coordenadas homogéneo.

Si $f \in R$ es un elemento homogéneo de grado m, entonces R_f es una álgebra graduada, diciendo que el grado de $\frac{g_n}{f^r}$ es $n - mr$, para cada $g_n \in R_n$. Dejamos que el lector demuestre la siguiente proposición.

9. Proposición : *1. El morfismo de localización $R \to R_f$ (f homogénea) es un morfismo de grado 1 que induce un isomorfismo*

$$\operatorname{Proj} R_f = U_f^h = \operatorname{Proj} R - (f)_0^h$$

2. Si I es un ideal homogéneo de R entonces R/I es un álgebra graduada homogénea, de modo que el morfismo $R \to R/I$ es un morfismo graduado de grado 1 que induce un isomorfismo

$$\operatorname{Proj}(R/I) = (I)_0^h$$

Dada un álgebra graduada R denotaremos por R_0 a la subálgebra de R formada por los elementos de grado cero.

Por sencillez, supondremos a partir de ahora que $R = R_0[\xi_0, \dots, \xi_n]$, donde cada ξ_i es de grado 1.

10. Teorema : *Sea $R = R_0[\xi_0, \dots, \xi_n]$. Denotemos U_i al abierto básico* $\operatorname{Proj} R - (\xi_i)_0^h$. *Entonces*

1. $\operatorname{Proj} R = \bigcup\limits_{i=0}^n U_i$.

2. *U_i es homeomorfo a* $\operatorname{Spec} R_0[\frac{\xi_0}{\xi_i}, \dots, \frac{\xi_n}{\xi_i}]$.

Diremos que U_i es un abierto afín de $\operatorname{Proj} R$. *Por tanto, el espectro proyectivo admite un recubrimiento por abiertos afines.*

Demostración. 1. $\operatorname{Proj} R = \bigcup\limits_{i=0}^n U_i$, ya que $\bigcap\limits_{i=0}^n (\xi_i)_0^h = (\xi_0, \dots, \xi_n)_0^h = \emptyset$, pues $(\xi_0, \dots, \xi_n)$ es el ideal irrelevante.

2. $R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$ es por definición el subanillo obvio de R_{ξ_i}. La composición de los morfismos naturales

$$\operatorname{Proj} R_{\xi_i} \hookrightarrow \operatorname{Spec} R_{\xi_i} \to \operatorname{Spec} R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$$

es el homeomorfismo buscado. En efecto, dicha aplicación transforma un ideal primo homogéneo $\mathfrak{p}$ de R_{ξ_i} en el ideal primo $\mathfrak{p}\cap R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$; es claro que todo primo homogéneo $\mathfrak{p}$ de R_{ξ_i} está determinado por sus elementos homogéneos de grado cero, es decir, por $\mathfrak{p}\cap R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, luego la aplicación es inyectiva. Además, es fácil comprobar que si $\mathfrak{p}'$ es un ideal primo de $R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, entonces $\mathfrak{p}'R_{\xi_i}$ es un ideal primo homogéneo de R_{ξ_i}, y esta es la asignación inversa. Finalmente, si $f\in R$ es homogénea de grado n, la biyección anterior transforma $(f)_0^h=(f/\xi_i^n)_0^h$ en $(f/\xi_i^n)_0$. Es decir, es un homeomorfismo.

□

Si C es un cerrado de $\operatorname{Proj} R$, entonces $C=(J)_0^h$, donde podemos suponer que J es un ideal homogéneo de R; de hecho el ideal I de todas las funciones de R que se anulan en C es homogéneo y $C=(I)_0^h$. Si C es irreducible, entonces $I=\mathfrak{p}_x$ es primo (y homogéneo) y C es el cierre de x en $\operatorname{Proj} R$.

Todo subespacio de un espacio noetheriano es noetheriano. Por tanto, si $R=k[\xi_0,\dots,\xi_n]$ entonces $\operatorname{Proj} R\subseteq \operatorname{Spec} R$, es un espacio noetheriano. En particular, $\operatorname{Proj} R$ es unión de un número finito de cerrados irreducibles, luego $\operatorname{Proj} R=\bar{x}_1\cup\dots\cup\bar{x}_r$, siendo $\mathfrak{p}_{x_1},\dots,\mathfrak{p}_{x_r}$ los ideales primos homogéneos minimales de R.

3.3 Dimensión en variedades proyectivas

1. Definición : Llamaremos dimensión de $\operatorname{Proj} R$ al máximo de las longitudes de sus cadenas de cerrados irreducibles, que coincide con el máximo de las longitudes de las cadenas de ideales primos homogéneos de R que no contengan al ideal irrelevante.

Si $\bar{x}_1\supset\dots\supset\bar{x}_m$ es una cadena de cerrados irreducibles de longitud máxima de $\operatorname{Proj} R$ y $x_m\in U^h_{\xi_i}\subseteq \operatorname{Proj} R$, entonces $\bar{x}_1\cap U^h_{\xi_i}\supset\dots\supset\bar{x}_m\cap U^h_{\xi_i}$ es una cadena de cerrados irreducibles en $U^h_{\xi_i}$. Como la dimensión de un abierto es siempre menor o igual que la del espacio, tenemos que

$$\dim \operatorname{Proj} R=\dim U^h_{\xi_i}=\dim k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$$

2. Definición : Llamaremos variedad proyectiva (sobre k) al espectro proyectivo de un álgebra graduada del tipo $k[\xi_0,\dots,\xi_n]=k[x_0,\dots,x_n]/I$, siendo I un ideal homogéneo. Es decir, una variedad proyectiva es un cerrado del espacio proyectivo $\mathbb{P}^n$. Si además es de dimensión 1, diremos que es una curva proyectiva.

3. Proposición : *Las variedades proyectivas son catenarias.*

Demostración. Dados dos cerrados irreducibles $\bar{x}_1\supset\bar{x}_2$, sea $U=U^h_{\xi_i}$ un abierto afín que contenga a x_2. Toda cadena maximal de cerrados irreducibles de extremos $\bar{x}_1$ y $\bar{x}_2$ induce, cortando con U, una cadena maximal en U (de extremos dados). Se concluye por 2.8.13, pues U es una variedad algebraica afín. □

3.4 Multiplicidad y multiplicidad de intersección

1. Definición : Si A es una k-álgebra finita. Diremos que $\dim_k A$ es el número de puntos de $\operatorname{Spec} A$ ("contando multiplicidades").

Si $C = \operatorname{Spec} k[x_1,\dots,x_n]/I$ y $C' = \operatorname{Spec} k[x_1,\dots,x_n]/I'$ son dos curvas afines sin componentes comunes, entonces $C \cap C' = \operatorname{Spec} k[x_1,\dots,x_n]/(I+I')$ está formado por un número finito de puntos cerrados $x_1,\dots,x_n$. Diremos que el número de puntos de la intersección de C con C', que denotaremos $\mu(C\cap C')$, es $\dim_k k[x_1,\dots,x_n]/(I+I')$.

2. Ejercicio : Calcular el número de puntos de corte de la recta $x=0$, con la curva $y^3+xy+x^3+1=0$.

3. Lema : *Sea A una k-álgebra de tipo finito de dimensión 1. Sean $f,g\in A$ no divisores de cero. Se cumple que*

$$\dim_k A/(fg) = \dim_k A/(f) + \dim_k A/(g)$$

Demostración. La sucesión

$$0 \to A/(f) \xrightarrow{g\cdot} A/(fg) \xrightarrow{\pi} A/(g) \to 0$$

con $(g\cdot)(\bar a) = \overline{ga}$ y $\pi(\bar a) = \bar a$, es exacta. En efecto, veamos sólo la inyectividad de $g\cdot$: si $\overline{ga}=0$, entonces $ga = fgh$ para un $h\in A$, luego $a = fh$ y $\bar a = 0$. Ahora ya es fácil concluir. □

4. Proposición : *Sean $C \equiv p(x,y)=0$ y $C'\equiv q(x,y)\cdot q'(x,y)=0$ dos curvas planas afines sin componentes comunes. Escribamos $C_1\equiv q(x,y)=0$ y $C_2\equiv q'(x,y)=0$. Se cumple que el número de puntos de intersección de C con C', es la suma del número de puntos de intersección de C con C_1 más el número de puntos de intersección de C con C_2.*

Demostración. Denotemos $A = k[x,y]/(p(x,y))$. Entonces el número de puntos de corte de C con C' es $\dim_k A/(q\cdot q')$, el número de puntos de corte de C con C_1 es $\dim_k A/(q)$ y el número de puntos de corte de C con C_1 es $\dim_k A/(q')$. Por el lema anterior se concluye. □

Por sencillez, vamos a suponer que k es un cuerpo algebraicamente cerrado.
Escribamos $\operatorname{Spec} k[x_1,\dots,x_n]/(I+I') = \{x_1,\dots,x_n\}$. Por **??**

$$k[x_1,\dots,x_n]/(I+I') = (k[x_1,\dots,x_n]/(I+I'))_{x_1}\times\cdots\times(k[x_1,\dots,x_n]/(I+I'))_{x_n}$$

Diremos que $\dim_k(k[x_1,\dots,x_n]/(I+I'))_x \underset{Not}{=} \mu_x(C\cap C')$ es la multiplicidad de intersección de C con C' en $x\in C\cap C'$.

5. Ejercicio : Calcular la multiplicidad de intersección en el origen de la curva $y^2 = x^2+y^3$ con la curva $y^3+x^2=0$.

6. Proposición : *El número de puntos de corte de dos curvas, sin componentes comunes, es igual a la suma de las multiplicidades de intersección en cada uno de los puntos de corte de las dos curvas, es decir,*

$$\mu(C\cap C') = \sum_{x\in C\cap C'} \mu_x(C\cap C')$$

Dada la curva plana afín $p(x,y)=0$, escribamos $p(x,y) = p_r(x,y)+p_{r+1}(x,y)+\cdots+p_n(x,y)$ como suma de polinomios homogéneos. Tenemos que

$$p_r(x,y) = x^r\cdot p_r(1,\frac{y}{x}) = x^r\cdot\prod_{i=1}^r(a_i\frac{y}{x}+b_i) = \prod_{i=1}^r(a_iy+b_ix)$$

Es decir, $p_r(x,y)$ es el producto de r rectas. Diremos que estas rectas son las tangentes de $p(x,y)=0$ en el origen y que la multiplicidad de $C \equiv p(x,y)=0$ en el origen es r, número que denotaremos por $\mu_{(0,0)}(C)$. Por traslaciones estas definiciones se pueden trasladar a todo punto p de $p(x,y)=0$. Si $\mu_p(C)=1$ diremos que p es no singular. Si $\mu_p(C)>1$ diremos que p es singular.

Si dos curvas planas son no singulares en un punto, no es difícil demostrar que la multiplicidad de intersección es uno si no son tangentes en el punto y mayor que uno si lo son. En el caso de que sean singulares, el cálculo de la multiplicidad de intersección es más difícil.

3.5 Teorema de Bézout

Sean $C \equiv p_n(x_0,x_1,x_2)=0$ y $C' \equiv p_m(x_0,x_1,x_2)=0$ dos curvas proyectivas planas, sin componentes comunes y $C \cap C'$ la intersección de las dos curvas planas.

Si $U_{x_0}^h$ es un abierto afín que contiene a $C\cap C'$, sean $x=\frac{x_1}{x_0}$ y $y=\frac{x_2}{x_0}$ coordenadas afines y escribamos $\frac{p_n(x_0,x_1,x_2)}{x_0^n}=p_n(1,x,y)=p(x,y)$ y $\frac{p_m(x_0,x_1,x_2)}{x_0^m}=p_m(1,x,y)=q(x,y)$. Entonces

$$C\cap C' = C\cap C' \cap U_{x_0}^h = \operatorname{Spec} k[x,y]/(p(x,y),q(x,y))$$

Diremos que el anillo $k[x,y]/(p(x,y),q(x,y))$ es el anillo de funciones de $C\cap C'$, también diremos que $\dim_k k[x,y]/(p(x,y),q(x,y))$ es el número de puntos en los que se cortan C y C'.

El anillo de funciones de $C\cap C'$ no depende del abierto afín $U_{x_0}^h$ (que contiene a $C\cap C'$) tomado: sea $U_{x_1}^h$ otro abierto afín que contiene a $C\cap C'$ y escribamos $x'=\frac{1}{x}=\frac{x_1}{x_0}$ y $y'=\frac{y}{x}=\frac{x_2}{x_0}$ y $p'(x',y')=\frac{p_n(x_0,x_1,x_2)}{x_1^n}=\frac{p(x,y)}{x^n}$ y $q'(x',y')=\frac{p_m(x_0,x_1,x_2)}{x_1^m}=\frac{q(x,y)}{x^m}$. Se cumple que $x=\frac{x_1}{x_0}$ es una función que no se anula en ningún punto de $C\cap C'\cap U_{x_0}^h$, e igualmente $x'=\frac{x_0}{x_1}$ es una función que no se anula en ningún punto de $C\cap C'\cap U_{x_1}^h$, luego

$$\begin{aligned} k[x,y]/(p(x,y),q(x,y)) &= (k[x,y]/(p(x,y),q(x,y)))_x = (k[x',y']/(p'(x',y'),q'(x',y')))_{x'} \\ &= k[x',y']/(p'(x',y'),q'(x',y')) \end{aligned}$$

1. Teorema de Bézout: *El número de puntos de intersección de dos curvas proyectivas planas $C\equiv p_n(x_0,x_1,x_2)=0$, $C'\equiv q_m(x_0,x_1,x_2)=0$ de grados n y m, sin componentes comunes, es $n\cdot m$.*

Demostración. La idea de la demostración es la siguiente: Supongamos que la recta del infinito $(x_0)_0^h$ no pasa por $C\cap C'$. Afínmente nuestras curvas se escribirán $p_n(1,x_1,x_2)=0$, $q_m(1,x_1,x_2)=0$ y la intersección es $C\cap C'=\operatorname{Spec} k[x_1,x_2]/(p_n(1,x_1,x_2),q_m(1,x_1,x_2))$ (nos conviene usar esta notación porque nos permite pensar afínmente las curvas C y C' como curvas en el plano $x_0=1$). El "cono", en $\mathbb{A}_3=\operatorname{Spec} k[x_0,x_1,x_2]$, que pasa por $C\cap C'$ y vértice $(0,0,0)$, es $\operatorname{Spec} k[x_0,x_1,x_2]/(p_n(x_0,x_1,x_2),q_m(x_0,x_1,x_2))$. Probaremos que los planos $x_0=\lambda$ cortan al cono en el mismo número de puntos. La intersección del cono con el plano $x_0=1$ es justamente $C\cap C'$. La intersección del cono con el plano $x_0=0$ es la intersección de $p_n(x_0,x_1,x_2)=0, x_0=0$, que son n rectas que pasan por el origen, con $q_m(x_0,x_1,x_2)=0, x_0=0$ que son m rectas que pasan por el origen. En conclusión, reducimos el problema del corte de dos curvas de grados n y m al problema del corte de n rectas con m rectas.

Por cambio de coordenadas homogéneo podemos suponer que $(x_0)_0^h\cap C\cap C'=\emptyset$. Tenemos que demostrar que

$$\dim_k k[x_1,x_2]/(p_n(1,x_1,x_2),q_m(1,x_1,x_2)) = n\cdot m$$

Sea $B=k[x_0,x_1,x_2]/(p_n(x_0,x_1,x_2),q_m(x_0,x_1,x_2))$.

Se verifica que B es un $k[x_0]$-módulo sin torsión: Si $p(x_0)\cdot b=0$, escribamos $p(x_0)=\sum\limits_{i=0}^{s} a_i x_0^i$ y $b=\sum\limits_{i=0}^{r} b_i(x_0,x_1,x_2)$ (siendo los $b_i(x_0,x_1,x_2)$ polinomios homogéneos de grado i). Entonces, $x_0^s\cdot b_r(x_0,x_1,x_2)=0$. Es decir, x_0 sería divisor de cero en B. Si $a\cdot x_0=0$ en B, entonces $a\cdot x_0=bp_n+cq_m$. Entonces, $0=b(0,x_1,x_2)p_n(0,x_1,x_2)+c(0,x_1,x_2)q_m(0,x_1,x_2)$. Como $p_n(0,x_1,x_2)$ y $q_m(0,x_1,x_2)$ son primos entre si, $c(0,x_1,x_2)\in(p_n(0,x_1,x_2))$. Es decir, $c\in(x_0,p_n)$, digamos $c=c_1x_0+c_2p_n$. Luego $(a-c_1q_m)x_0=(b+c_2)p_n$. Como x_0 y p_n son primos entre si, $a-c_1q_m\in(p_n)$. Luego $a\in(p_n,q_m)$ y x_0 no es divisor de cero en B.

El morfismo $B\hookrightarrow B_{x_0}$ es inyectivo. Denotemos $A=[B_{x_0}]_0$. Sabemos que $B_{x_0}=\bigoplus\limits_{n\in\mathbb{Z}} A\cdot x_0^n$. Denotemos $B_{x_0}^+=\bigoplus\limits_{n\in\mathbb{N}} A\cdot x_0^n$. Obviamente, $B_{x_0}^+$ es un $k[x_0]$-módulo finito y como B se inyecta en $B_{x_0}^+$ es también un $k[x_0]$-módulo finito. En conclusión, B es un $k[x_0]$-módulo finito sin torsión, luego libre. Escribamos $B=k[x_0]\oplus\overset{s}{\cdots}\oplus k[x_0]$. Por tanto,

$$\begin{aligned}\dim_k B/(x_0)&=\dim_k B\otimes_{k[x_0]}k[x_0]/(x_0)=s=\dim_k B\otimes_{k[x_0]}k[x_0]/(x_0-1)\\&=\dim_k B/(x_0-1)=\dim_k k[x_1,x_2]/(p_n(1,x_1,x_2),q_m(1,x_1,x_2))\end{aligned}$$

Así pues, tenemos que demostrar que $\dim_k B/(x_0)=n\cdot m$.

$$\begin{aligned}\dim_k B/(x_0)&=\dim_k k[x_1,x_2]/(p_n(0,x_1,x_2),q_m(0,x_1,x_2))\\&=\sum_{i,j}^{n,m}\dim_k k[x_1,x_2]/(a_ix_1+a_i'x_2,b_jx_1+b_j'x_2)=\sum_{i,j}^{n,m}1=n\cdot m\end{aligned}$$

□

En la teoría, un concepto pugna por emerger. Dado un espacio topológico, podemos hablar para cada abierto del espacio de las funciones continuas en el abierto. Dada una variedad algebraica afín $X=\operatorname{Spec}A$, hemos visto que $U_a=\operatorname{Spec}A_a$ y hemos dicho que A_a es el anillo de funciones algebraicas sobre U_a. Parece que podríamos decir que en las variedades algebraicas, como en los espacios topológicos, podemos hablar de las funciones algebraicas en cada abierto de la variedad. Es decir, cuando escribimos $X=\operatorname{Spec}A$, en realidad tenemos en mente la pareja $(\operatorname{Spec}A,A)$, y para cada abierto U_a, la pareja (U_a,A_a). Dada un variedad proyectiva, $X=\operatorname{Proj}k[\xi_1,\dots,\xi_n]$, hemos visto que $U_{\xi_i}^h=\operatorname{Spec}k[\frac{\xi_1}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$ y podríamos decir que $k[\frac{\xi_1}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$ es el anillo de funciones algebraicas sobre $U_{\xi_i}^h$. De nuevo, parece que podríamos decir, para cada abierto de X, cuáles son las funciones algebraicas en el abierto. Este va a ser el hecho nuclear en la definición de variedad algebraica (afín o no) que debemos explicitar con detalle y rigor. Para ello, se necesitan los conceptos de haces y espacios anillados, que se estudiarán en cursos posteriores.

3.6 Problemas

1. Probar que el morfismo $k[x]\hookrightarrow k[x,y]/(p(x,y))$ es finito si y sólo si la curva $p(x,y)=0$ no tiene asíntotas verticales.

2. Calcular las asíntotas imaginarias de la circunferencia $x^2+y^2=1$.

3. Probar que el conjunto de rectas que pasan por un punto ("haz de rectas") del plano afín se corresponde con el conjunto de puntos racionales de una recta proyectiva.

4. Probar que el conjunto de cónicas que pasan por cuatro puntos no alineados del plano afín se corresponden con los puntos racionales de una recta proyectiva.

5. Probar que el conjunto de cónicas que pasan tres puntos no alineados del plano afín y es tangente en uno de ellos a una recta fijada que pasa por el punto se corresponden con los puntos racionales de una recta proyectiva.

6. Probar que el conjunto de curvas de grado n de $\mathbb{P}^2$ se corresponden con los puntos racionales de un espacio proyectivo.

7. Probar que el conjunto de curvas afines de grado menor o igual que n de $\mathbb{A}^2$ se corresponden con los puntos racionales de un abierto de un espacio proyectivo.

8. Se dice que en general los puntos de una variedad algebraica irreducible cumplen una propiedad si existe un abierto de la variedad cuyos puntos cumplen la propiedad. Probar que en general las curvas planas afines de grado n son irreducibles.

9. Demostrar que en general las matrices cuadradas son invertibles. Sean A y B dos matrices cuadradas de orden n, probar que $c_{A\cdot B}(x) = c_{B\cdot A}(x)$.

10. Demostrar que $R_0[\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}] \simeq R_0[\xi_0, \ldots, \xi_n]/(\xi_i - 1)$ y que por tanto, $U^h_{\xi_i} \simeq (\xi_i - 1)_0$. Probar que $U^h_{\xi_i} \times (\mathbb{A}^1 - \{0\}) = U_{\xi_i}$. Dar una interpretación geométrica de estos resultados.

11. Demostrar que el conjunto de puntos cerrados de $\mathbb{P}^n(\mathbb{C}) = \operatorname{Proj} \mathbb{C}[x_0, \ldots, x_{n+1}]$ es biyectivo con el conjunto $\mathbb{C}^{n+1} - \{0\}/\sim$, donde $(\alpha_0, \ldots, \alpha_n) \sim (\alpha'_0, \ldots, \alpha'_{n+1})$ si $(\alpha'_0, \ldots, \alpha'_n) = \lambda(\alpha_0, \ldots, \alpha_{n+1})$.

12. (a) Escribir las ecuaciones de la curva proyectiva plana $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2)$ en cada uno de los abiertos "afines", complementario del cerrado $(x_i)^h_0$ ("deshomogeneizar").
    (b) Demostrar que el epimorfismo $\mathbb{C}[x_0, x_1, x_2] \to \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2)$ define una inmersión cerrada $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2) \hookrightarrow \mathbb{P}^2$
    (c) Definir una curva proyectiva plana que en uno de los abiertos afines sea la curva plana "afín" $y + x^2 = 0$. ¿Corta la recta $x = 0$, a la curva $y + x^2 = 0$, en algún punto del "infinito"?

13. Demostrar 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 $(\alpha_0, \alpha_1, \alpha_2)$ no singular es

$$\frac{\partial p(x_0, x_1, x_2)}{\partial x_1}(\alpha_0, \alpha_1, \alpha_2)X_0 + \frac{\partial p(x_0, x_1, x_2)}{\partial x_0}(\alpha_0, \alpha_1, \alpha_1)X_1 + \frac{\partial p(x_0, x_1, x_2)}{\partial x_2}(\alpha_0, \alpha_1, \alpha_2)X_2 = 0$$

14. Probar que $\dim \operatorname{Proj} k[\xi_0, \ldots, \xi_n] = (\dim \operatorname{Spec} k[\xi_0, \ldots, \xi_n]) - 1$.

15. Si X e Y son dos subvariedades proyectivas de $\mathbb{P}^n$, y $\operatorname{codim} X + \operatorname{codim} Y \leq n$, probar que $X \cap Y \neq \emptyset$ y que se cumple que

$$\operatorname{codim} X + \operatorname{codim} Y \geq \operatorname{codim} X \cap Y$$

16. Sea $f \in k[\xi_0, \ldots, \xi_n]$ una función homogénea de grado mayor que cero y $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$. Demostrar que

$$\dim (f)^h_0 \geq \dim X - 1$$

17. Parametrizar la curva $x^6 - x^2y^3 - y^5 = 0$. Calcular sus soluciones racionales.

18. (a) Sea C la cúbica plana $y^2 = x^2 + x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}_1 \to C$, $x = t^2 - 1$, $y = t^3 - t$. Calcular el área del "ojo del lazo" definido por la curva $y^2 = x^2 + x^3$.

    (b) Sea C la cúbica plana $y^2 = x^3$. El haz de rectas $y = tx$ define un morfismo birracional $\mathbb{A}_1 \to C$, $x = t^2$, $y = t^3$.

19. Probar que si una cónica tiene un único punto singular entonces no es irreducible.

20. Probar que si una cúbica plana tiene exactamente dos puntos singulares no es irreducible.

21. Probar que si una cuártica plana tiene exactamente cuatro puntos singulares entonces no es irreducible.

22. Probar que $(0,0), (2,0), (0,2)$ son puntos singulares de la cuártica plana $xy(x+y-2) - (x^2 + y^2 - 2x - 2y)^2 = 0$ ¿Existen más puntos singulares? Parametrizar esta cuártica (mediante un haz de cónicas).

23. Justificar por qué las circunferencias $x^2 + y^2 - 1 = 0$, $x^2 + y^2 - 2 = 0$ han de ser tangentes en algún punto del infinito, sin hacer el cálculo explícito de sus tangentes en los puntos del infinito.

Capítulo 4

Variedades algebraicas lisas

4.1 Módulo de las diferenciales de Kähler

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 y 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 $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$, al que pertenecen las diferenciales de funciones en α, se le denomina espacio cotangente en α de $\operatorname{Spec} A$.

El siguiente paso es abstraernos del punto concreto $\alpha \in \mathbb{R}$. El incremento de una función diferenciable $f(x)$, en un punto $\bar{x}$, cualquiera, lo podemos definir como $\Delta f(x) := f(x) - f(\bar{x})$ (con precisión, $\Delta f(x)$ es la función definida en $\mathbb{R} \times \mathbb{R}$, cuyo valor en cada punto $(x, \bar{x})$ es $f(x) - f(\bar{x})$). Obviamente, $\Delta f(x)$ se anula sobre la diagonal de $\mathbb{R} \times \mathbb{R}$ y su restricción a $\mathbb{R} \times \alpha$ es $\Delta_\alpha f$. Además, si Δ es el ideal de las funciones diferenciales de $\mathbb{R} \times \mathbb{R}$ que se anulan en la diagonal, entonces la restricción de Δ a $\mathbb{R} \times \alpha$ es $\mathfrak{m}_\alpha$. Puede demostrarse que la definición de diferencial de una función, en Geometría Diferencial o Análisis, es $df := \overline{\Delta f} = \overline{f(x) - f(\bar{x})} \in \Delta/\Delta^2$. Se dice que Δ/Δ^2 es el $\mathcal{C}^\infty(\mathbb{R})$-módulo de las diferenciales de las funciones diferenciales de $\mathbb{R}$.

Consideremos el anillo $k[x]$ de las funciones algebraicas de la recta afín y $k[x] \otimes_k k[x]$ el anillo de funciones algebraicas de $\mathbb{A}_1 \times_k \mathbb{A}_1 = \mathbb{A}_2$. Los morfismos $k[x] \to k[x, \bar{x}] = k[x] \otimes_k k[x]$, $p(x) \mapsto p(x)$, $p(x) \mapsto p(\bar{x})$ son obviamente los morfismos $p(x) \mapsto p(x) \otimes 1$ y $p(x) \mapsto 1 \otimes p(x)$, que inducen por tomas de espectros las dos proyecciones naturales de $\mathbb{A}_1 \times_k \mathbb{A}_1$ en $\mathbb{A}_1$. La inmersión diagonal $\mathbb{A}_1 \to \mathbb{A}_1 \times_k \mathbb{A}_1$, $\alpha \mapsto (\alpha, \alpha)$ es el morfismo inducido por el morfismo de anillos $k[x] \otimes_k k[x] \xrightarrow{\phi} k[x]$, $p(x) \otimes q(x) \mapsto p(x) \cdot q(x)$. El ideal de las funciones algebraicas que se anulan en la diagonal es $\operatorname{Ker} \phi$.

Más en general, sea k un anillo y A una k-álgebra. Si definimos $\operatorname{Spec} A \times_k \operatorname{Spec} A := \operatorname{Spec}(A \otimes_k A)$, los morfismos $A \to A \otimes_k A$, $a \mapsto a \otimes 1$ y $a \mapsto 1 \otimes a$, pueden interpretarse como los morfismos que asignan a cada función $f(x)$ de $\operatorname{Spec} A$, las funciones de $\operatorname{Spec} A \times_k \operatorname{Spec} A$ $f(x)$ y $f(\bar{x})$. Diremos que el morfismo $\operatorname{Spec} A \hookrightarrow \operatorname{Spec} A \times \operatorname{Spec} A$, inducido por el epimorfismo de anillos

$$A \otimes_k A \to A, \quad a \otimes b \mapsto a \cdot b$$

es la inmersión "diagonal" de $\operatorname{Spec} A$ en $\operatorname{Spec} A \times \operatorname{Spec} A$.

1. Definición : 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-módulo por la izquierda y por la derecha.

2. Proposición: *Δ está generado, como A-módulo por la izquierda, 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

$$\begin{aligned} d\colon A &\to \Omega_{A/k} \\ a &\mapsto \overline{a \otimes 1 - 1 \otimes a} \end{aligned}$$

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-módulo por la derecha e izquierda coinciden. Por la proposición anterior, $\Omega_{A/k}$ es un A-módulo generado por las diferenciales exactas.

La sucesión exacta de A-módulos

$$0 \to \Delta \to A \otimes_k A \to A \to 0$$

escinde, por la izquierda (resp. por la derecha), pues $A \to A \otimes_k A$, $a \mapsto a \otimes 1$ (resp. $a \mapsto 1 \otimes a$) es una sección del epimorfismo $A \otimes_k A \to A$.

4. Proposición : *Sea $\mathfrak{m}_\alpha$ un ideal de A tal que $A/\mathfrak{m}_\alpha = k$. Se verifica que $\Delta \otimes_A A/\mathfrak{m}_\alpha = \mathfrak{m}_\alpha$. Es decir, "la restricción a $\operatorname{Spec} A \times \alpha$ del ideal de las funciones que se anulan en la diagonal es el ideal de las funciones que se anulan en α"*

Demostración. Dado que la sucesión exacta

$$0 \to \Delta \to A \otimes_k A \to A \to 0$$

escinde, si tensorializamos 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 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 $d_\alpha(A) = \overline{f - f(\alpha)}$, donde $f(\alpha)$ es la clase de f en $A/\mathfrak{m}_\alpha = k$.

7. Proposición : *Si $k \to k'$ es un morfismo de anillos, entonces que*

$$\Omega_{A/k} \underset{k}{\otimes} k' = \Omega_{A \underset{k}{\otimes} k'/k'}$$

Demostración. Denotemos Δ_A el ideal de la diagonal definido a partir de A. Denotemos $A_{k'} = A \otimes_k k'$.

Si tensorializamos 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, $\Omega_{A/k} \otimes_k k' = (\Delta_A/\Delta_A^2) \otimes_k k' = (\Delta_A \otimes_k k')/(\Delta^2 \otimes_k k') = \Delta_{A_{k'}}/\Delta^2_{A_{k'}} = \Omega_{A_{k'}/k'}$.

□

4.2 Módulo de derivaciones

1. 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 $a, b \in B$.

Observemos que $D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = 2D(1)$, luego $D(1) = 0$. Además, dado $\lambda \in k$, $D(\lambda) = \lambda D(1) = 0$.

El conjunto de todas las k-derivaciones de A en M se denota por $Der_k(A, M)$. Si definimos

$$(D + D')(a) := D(a) + D'(a) \qquad (aD)(b) := aDb$$

tenemos que el conjunto de todas las k-derivaciones de A en M tiene estructura de A-módulo.

2. 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 inmediato comprobar que $\delta(ab) = a \cdot \delta b + (\delta a) \cdot b$. Haciendo módulo Δ^2, y teniendo en cuenta que la multiplicación por la derecha y por la izquierda coinciden en $\Omega_{A/k}$, se concluye. □

3. Corolario : *Si $\mathfrak{m}$ es un ideal tal que $A/\mathfrak{m} = k$, entonces $d_\mathfrak{m} \colon A \to \mathfrak{m}/\mathfrak{m}^2$ es una k-derivación.*

.

Demostración. Inmediato. □

4. Proposición : *Sea $\mathfrak{m}$ un ideal de A tal que $A/\mathfrak{m} = k$. Sea M un k-módulo, luego A-módulo a través del cociente $A \to A/\mathfrak{m} = k$. Se verifica que*

$$Der_k(A, M) = \operatorname{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, M)$$

En particular,

$$Der_k(A, k) = \operatorname{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k) \underset{Not}{=} (\mathfrak{m}/\mathfrak{m}^2)^*$$

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 $d_\mathfrak{m}$, una k-derivación $A \to M$. Dejamos al lector que compruebe que estas asignaciones son inversas entre sí.

□

5. Teorema : *Existe un isomorfismo canónico*

$$\operatorname{Hom}_A(\Omega_{A/k}, M) = Der_k(A, M),\ w \mapsto w \circ d$$

Demostración. Por la proposición anterior, para todo A-módulo M se verifica $Der_A(A \otimes_k A, M) = \operatorname{Hom}_A(\Delta/\Delta^2, M)$. Por tanto, basta probar que para todo morfismo de anillos $k \to k'$ y todo $A \otimes_k k'$-módulo M, se tiene un isomorfismo

$$Der_k(A, M) \simeq Der_{k'}(A \otimes_k k', M)$$

Dada una k-derivación $D \colon A \to M$, define una 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. □

Calculemos el módulo de diferenciales de Kahler de $k[x_1, \dots, x_n]$. Primero calculemos el módulo $Der_k(k[x_1, \dots, x_n], M)$. Toda derivación D de $k[x_1, \dots, x_n]$ en M está determinada por los valores Dx_i, $i \in \{1, \dots, n\}$. Si denotamos por $D' = \sum_i m_i \frac{\partial}{\partial x_i}$ la derivación definida por

$$D'(p(x_1, \dots, x_n)) = \sum_i \frac{\partial p(x_1, \dots, x_n)}{\partial x_i} \cdot m_i$$

entonces $D = \sum_i Dx_i \frac{\partial}{\partial x_i}$, para toda derivación.

Por tanto, $\operatorname{Der}_k(k[x_1, \dots, x_n], M) = M \frac{\partial}{\partial x_1} \oplus \cdots \oplus M \frac{\partial}{\partial x_n}$. El $k[x_1, \dots, x_n]$-módulo libre de rango n, que por razones obvias denotamos $L = k[x_1, \dots, x_n]dx_1 \oplus \cdots \oplus k[x_1, \dots, x_n]dx_n$, cumple que $\operatorname{Hom}_{k[x_1,\dots,x_n]}(L, M) = \operatorname{Der}_k(k[x_1, \dots, x_n], M)$, por tanto

$$\Omega_{k[x_1,\dots,x_n]/k} = k[x_1, \dots, x_n]dx_1 \oplus \cdots \oplus k[x_1, \dots, x_n]dx_n$$

y $d(p(x_1, \dots, x_n)) = \sum_i \frac{\partial p(x_1, \dots, x_n)}{\partial x_i} dx_i$.

6. Proposición : *Sea S un sistema multiplicativamente cerrado de A. Se verifica*

$$(\Omega_{A/k})_S = \Omega_{A_S/k}$$

Demostración. Empecemos demostrando que si M es un A_S-módulo entonces $Der_k(A,M) = Der_k(A_S,M)$. Basta ver para ello, que toda derivación $D \in Der_k(A,M)$ extiende de modo único a una derivación de A_S. La única derivación D' que puede coincidir con D en A es:

$$D'(a/s) = (sDa - aDs)/s^2$$

Ahora ya, tenemos

$$\begin{aligned} \mathrm{Hom}_{A_S}(\Omega_{A_S/k}, M) &= Der_k(A_S,M) = Der_k(A,M) = \mathrm{Hom}_A(\Omega_{A/k}, M) \\ &= \mathrm{Hom}_{A_S}((\Omega_{A/k})_S, M) \end{aligned}$$

Luego $(\Omega_{A/k})_S = \Omega_{A_S/k}$.

□

Dejamos al lector que demuestre con el mismo método

7. Proposición : $\Omega_{(A\otimes_k B)/k} = (\Omega_{A/k}\otimes_k B)\oplus(A\otimes_k \Omega_{B/k})$.

8. Proposición : $\Omega_{(A\times B)/k} = \Omega_{A/k}\oplus\Omega_{B/k}$

Para terminar estudiemos las sucesiones exactas de diferenciales. Comencemos para ello con las sucesiones exactas de derivaciones.

9. Proposición : *Si B es una A-álgebra y N un B-módulo, la siguiente sucesión es exacta:*

$$\begin{array}{ccccccc} 0 & \to & Der_A(B,N) & \to & Der_k(B,N) & \to & Der_k(A,N) \\ & & D & \mapsto & D & & \\ & & & & D & \mapsto & D_{|A} \end{array}$$

Demostración. Es evidente. □

Si B es una A-álgebra, el morfismo $A \to \Omega_{B/k}$, $a \mapsto da$ induce por 4.2.5, un morfismo $\Omega_{A/k} \to \Omega_{B/k}$. De otro modo, con las notaciones obvias, tenemos que Δ_A está "incluido" en Δ_B, luego tenemos un morfismo $\Omega_{A/k} = \Delta_A/\Delta_A^2 \to \Delta_B/\Delta_B^2 = \Omega_{B/k}$.

10. 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

$$\begin{array}{ccccccc} 0 \to & \mathrm{Hom}_B(\Omega_{B/A}, N) & \to & \mathrm{Hom}_B(\Omega_{B/k}, N) & \to & \mathrm{Hom}_B(\Omega_{A/k}\otimes_A B, N) \\ & \| & & \| & & \| \\ & Der_A(B,N) & & Der_k(B,N) & & \mathrm{Hom}_A(\Omega_{A/k}, N) \\ & & & & & \| \\ & & & & & Der_k(A,N) \end{array}$$

es exacta. Lo es por la proposición anterior.

□

11. 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*

$$0 \to Der_k(A/I, N) \to Der_k(A,N) \to \mathrm{Hom}_A(I,N)$$

Demostración. Es evidente. □

12. Proposición : *Sea $I \subset A$ un ideal. 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

$$0 \to \underset{\substack{\| \\ Der_k(A/I,N)}}{\mathrm{Hom}_{A/I}(\Omega_{(A/I)/k}, N)} \to \underset{\substack{\| \\ \mathrm{Hom}_A(\Omega_{A/k},N) \\ \| \\ Der_k(A,N)}}{\mathrm{Hom}_{A/I}(\Omega_{A/k} \otimes_A (A/I), N)} \to \underset{\substack{\| \\ \mathrm{Hom}_A(I,N)}}{\mathrm{Hom}_{A/I}(I/I^2, N)}$$

es exacta, luego se termina por la proposición anterior. □

13. Corolario : $\Omega_{(k[x_1,\dots,x_n]/(p_1,\dots,p_r))/k}$ *es igual a*

$$(k[x_1,\dots,x_n]/(p_1,\dots,p_r)dx_1 \oplus \dots \oplus k[x_1,\dots,x_n]/(p_1,\dots,p_r)dx_n)/(dp_1,\dots,dp_r)$$

4.3 Cono tangente y espacio tangente en un punto

El espacio tangente a una variedad diferenciable en un punto es un concepto intrínseco, que no depende de la inmersión de la variedad diferenciable en un $\mathbb{R}^n$. El espacio tangente a una variedad en un punto se define en términos de su anillo de funciones diferenciables. Ya sabemos que la diferencial de una función en un punto y los módulos de diferenciales de Kähler son conceptos algebraicos. En esta sección, dado un anillo local, definiremos el espacio tangente en el punto cerrado.

Comencemos con un ejemplo sencillo. Consideremos el nodo en el plano afín $y^2 - x^2 + x^3 = 0$. El espacio tangente en el origen del nodo es aquella variedad homogénea que mejor se aproxima al nodo. El nodo "infinitesimalmente" en el origen es equivalente a $y^2 - x^2 = 0$. Así pues, diremos que el cono tangente a $y^2 - x^2 + x^3 = 0$ en el origen es $y^2 - x^2 = 0$. En general, si una subvariedad $X \subset \mathbb{A}_n$, viene definida por los ceros de un ideal $I \subset k[x_1,\dots,x_n]$, entonces el cono tangente C_xX en el origen es la variedad definida por el ideal $I_h = (f_r)_{f\in I}$, donde f_r es la parte homogénea de grado más pequeño de f. Es decir, si pensamos que X es la intersección de las variedades $f = 0$, con $f \in I$, entonces el cono tangente es la intersección de las variedades homogéneas $f_r = 0$.[1]

Veamos cómo construir I_h. Consideremos el ideal maximal $\bar{\mathfrak{m}}_x = (x_1,\dots,x_n) \subset k[x_1,\dots,x_n]/I$ de las funciones de X que se anulan en el origen. Se verifica que

$$\bar{\mathfrak{m}}_x^r/\bar{\mathfrak{m}}_x^{r+1} = \{\text{Polinomios } p(x_1,\dots,x_n) \text{ homogéneos de grado } r\}/\{f_r\}_{f=f_r+\dots+f_n\in I}$$

Por tanto, $\underset{r}{\oplus}\bar{\mathfrak{m}}_x^r/\bar{\mathfrak{m}}_x^{r+1} = k[x_1,\dots,x_n]/I_h$. Entonces $\mathrm{Spec}\underset{r}{\oplus}\bar{\mathfrak{m}}_x^r/\bar{\mathfrak{m}}_x^{r+1}$ es el cono tangente de X en x y $\mathrm{Proj}\overset{\infty}{\underset{r=0}{\oplus}}\bar{\mathfrak{m}}_x^r/\bar{\mathfrak{m}}_x^{r+1}$ es el espacio tangente de X en x.

Demos ahora las definiciones con toda precisión y mayor generalidad.

1. Definición : Una filtración de un A-módulo M es una cadena de submódulos

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots \supseteq M_n \supseteq \dots$$

[1] Advertamos que debemos tomar todas las $f \in I$ y que no basta con tomar cualquier sistema generador

2. Definición : Llamaremos graduado de M por la filtración $\{M_n\}$ al módulo $GM = \overset{\infty}{\underset{i=0}{\oplus}} M_i/M_{i+1}$. Si I es un ideal de A, denotaremos $G_I M$ al graduado de M por la filtración $M_n = I^n M$.

3. Definición : Sea $X = \operatorname{Spec} A$ y $x \in X$ un punto cerrado de ideal $\mathfrak{m}$. Llamaremos cono tangente de X en x a

$$C_x X = \operatorname{Spec} G_{\mathfrak{m}} A := \operatorname{Spec} \overset{\infty}{\underset{i=0}{\oplus}} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

Llamaremos vértice del cono al punto de $C_x X$ definido por el ideal (maximal) irrelevante $\underset{r>0}{\oplus} \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Llamaremos espacio tangente de X en x a

$$T_x X := \operatorname{Proj}\, G_{\mathfrak{m}} A$$

4. Ejemplo : El cono tangente de un espacio afín en el origen es isomorfo al espacio afín. Es decir, si $A = k[x_1, \ldots, x_n]$ y $\mathfrak{m} = (x_1, \ldots, x_n)$, entonces $G_{\mathfrak{m}} A \simeq A$.

5. Proposición: *Sea $I \subset A$ un ideal y $f \in I^r - I^{r+1}$. Denotemos f_r la clase de f en $I^r/I^{r+1} \subset G_I A$. Si f_r es no divisor de cero en $G_I A$, entonces*

1. *$(f) \cap I^n = f \cdot I^{n-r}$, para $r \geq n$.*
2. *$G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$, donde $\bar{I}$ es el ideal I en $A/(f)$.*

Demostración. 1. Es claro que $f \cdot I^{n-r} \subseteq (f) \cap I^n$. Probemos la inclusión inversa. Si $h \in (f) \cap I^n$, entonces $h = f \cdot g$, con $g \in A$. Sea $s \geq 0$ el máximo tal que $g \in I^s$. Tenemos que ver que $s \geq n - r$. Escribamos $0 \neq g_s = \bar{g} \in I^s/I^{s+1}$. Por hipótesis, $0 \neq f_r \cdot g_s \in I^{r+s}/I^{r+s+1}$, luego $h = f \cdot g \notin I^{r+s+1}$. Por tanto, $n < r + s + 1$, es decir, $s \geq n - r$.

2. Por 1., la sucesión

$$0 \to I^{n-r}/I^{n-r+1} \xrightarrow{\cdot f = \cdot f_r} I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1} \to 0$$

es exacta, luego $G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$.

□

6. Ejercicio : Escribamos el polinomio $p(x, y) = p_n(x, y) + p_{n+1}(x, y) + \ldots + p_m(x, y)$ como suma de polinomios homogéneos. Sea $\mathcal{O} = (k[x, y]/p(x, y))_{x_0}$, con $\mathfrak{m}_{x_0} = (x, y)$. Demostrar que $G_{\mathfrak{m}_{x_0}} \mathcal{O} = k[x, y]/(p_n(x, y))$.

7. Ejercicio : Probar que el espacio tangente de la intersección de dos hipersuperficies transversales es la intersección de los espacios tangentes. Es decir, considérese el espacio afín $\mathbb{A}_3 = \operatorname{Spec} k[x_1, x_2, x_3]$ y las superficies $f_1(x_1, x_2, x_3) = 0$, $f_2(x_1, x_2, x_3) = 0$. Sea $\mathfrak{m} = (x_1, x_2, x_3)$, y $f_{1,n}$, $f_{2,m}$ las componentes homogéneas de grado mínimo de f_1, f_2. Si $f_{2,m}$ es no divisor de cero en $G_{\mathfrak{m}}(k[x_1, x_2, x_3]/(f_1)) = k[x_1, x_2, x_3]/(f_{1,n})$, entonces

$$G_{\mathfrak{m}}(k[x_1, x_2, x_3]/(f_1, f_2) \simeq k[x_1, x_2, x_3]/(f_{1,n}, f_{2,m}))$$

8. Teorema : *Sea $X = \operatorname{Spec} A$ una k-variedad algebraica, $x \in X$ un punto cerrado. Se verifica que la dimensión del cono tangente a X en x es igual a la dimensión de la variedad algebraica en x, es decir,*

$$\dim A_x = \dim G_{\mathfrak{m}_x} A$$

Demostración. Los ideales primos minimales de una k-álgebra graduada $k[\xi_1,\dots,\xi_n]$, $\operatorname{gr}\xi_i = 1$, son homogéneos, porque dado un ideal primo el ideal generado por sus elementos homogéneos es un ideal primo homogéneo contenido en él. Es decir, todas las componentes irreducibles de una variedad homogénea pasan por el origen. Por tanto, la dimensión del cono tangente de una variedad es la dimensión del anillo graduado localizado en el vértice.

Veamos que $\dim A_x \geq \dim G_{\mathfrak{m}_x} A = n$: Sean $f_1,\dots,f_n$ n-elementos de $G_{\mathfrak{m}_x}A$ k-algebraicamente independientes. Si todas las componentes homogéneas de f_1 dependen algebraicamente de $f_2,\dots,f_n$ entonces f_1 también dependería algebraicamente de $f_2,\dots,f_n$. Podemos suponer que $f_1,\dots,f_n$ son homogéneos, es más, tomando potencias de ellos podemos suponer que son homogéneos del mismo grado, digamos m. Sean $g_i \in \mathfrak{m}_x^m \subseteq A_x$ tales que $\bar g_i = f_i \in \mathfrak{m}_x^m/\mathfrak{m}_x^{m+1}$. Es fácil probar que los g_i son algebraicamente independientes. Tenemos, pues, una inclusión $k[x_1,\dots,x_n] \hookrightarrow A_x$, $x_i \mapsto g_i$. Sea $\mathfrak{p}$ un ideal primo de A_x que corta a $k[x_1,\dots,x_n]$ en cero, entonces el grado de trascendencia del cuerpo de fracciones de $A_x/\mathfrak{p}$ es mayor o igual que n, luego la dimensión de $A_x/\mathfrak{p}$ es mayor o igual que n y $\dim A_x \geq n$.

Veamos que $\dim A_x \leq \dim G_{\mathfrak{m}_x} A = n$: Procedamos por inducción sobre n. Si $n = 0$, entonces no hay más ideal primo que el irrelevante, que habrá de ser nilpotente. Luego para $n >> 0$, $\mathfrak{m}_x^n/\mathfrak{m}_x^{n+1} = 0$, y por el lema de Nakayama en A_x, $\mathfrak{m}_x^n = 0$, y $\dim A_x = 0$. Supongamos que $n > 0$. Sea f un elemento homogéneo tal que $\dim(G_{\mathfrak{m}_x}A)/(f) = n-1$, Digamos que el grado de f es m, y sea $g \in \mathfrak{m}_x^m$ tal que $\bar g = f \in \mathfrak{m}_x^m/\mathfrak{m}_x^{m+1}$. Como el graduado de $A/(g)$ es un cociente de $(G_{\mathfrak{m}_x}A)/(f)$ entonces $\dim G_{\mathfrak{m}_x}A/(f) \leq n-1$. Por inducción $\dim A_x/(g) \leq G_{\mathfrak{m}_x}A/(f)$. Como $\dim A_x \leq A_x/(g) + 1$, concluimos que $\dim A_x \leq \dim G_{\mathfrak{m}_x} A$.

□

4.4 Anillos locales regulares

El objetivo de esta sección es caracterizar localmente los anillos de funciones de las variedades algebraicas sin singularidades, es decir, regulares. Diremos que una variedad algebraica de dimensión n es regular en un punto si y sólo si existen n hipersuperficies que se cortan transversalmente en el punto, con multiplicidad de corte 1. Está definición equivaldrá a que el cono tangente a la variedad en el punto sea un espacio afín. Más adelante daremos criterios diferenciales que caractericen la regularidad.

Los anillos de funciones algebraicas de la cúspide $y^2 - x^3 = 0$, el nodo $y^2 - x^2 + x^3 = 0$, el cono $x^2 + y^2 - z^2 = 0$ son no regulares en el origen y regulares en cualquier otro punto, como veremos.

1. Notación : Supondremos siempre que $\mathcal{O}$ es el anillo local en un punto cerrado de una variedad algebraica y $\mathfrak{m}$ el ideal maximal.

2. Definición : Diremos que $\mathcal{O}$ es regular, si $\dim \mathcal{O} = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. El espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ se denomina espacio cotangente de Zariski.

Si $\mathcal{O}$ es el anillo local de una variedad algebraica entonces $\dim \mathcal{O} \leq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, porque si $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = n$ y $f_1,\dots,f_n$ es un sistema de parámetros obtenido por Nakayama, sabemos por el teorema del ideal principal de Krull que $\dim \mathcal{O} \leq n$. Por tanto,

$$\mathcal{O} \text{ es regular } \Leftrightarrow \dim \mathcal{O} \geq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$$

3. Proposición : *Sea $\dim \mathcal{O} = n$. $\mathcal{O}$ es regular si y sólo si existe un sistema de n parámetros $f_1,\dots,f_n$ que generan el ideal maximal.*

Demostración. Si $\mathcal{O}$ es un anillo regular entonces $n = \dim \mathcal{O} = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. Si $f_1, \ldots, f_n$ es un sistema generador de $\mathfrak{m}$ obtenido por Nakayama, éste será el sistema de parámetros buscado. Recíprocamente, si $f_1, \ldots, f_n$ es un sistema de parámetros que generan $\mathfrak{m}$ entonces $\dim \mathcal{O} = n \geq \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathcal{O}$ es regular. □

Aunque no hayamos definido la multiplicidad de intersección, digamos que esta proposición se interpreta geométricamente del siguiente modo: "Una variedad algebraica irreducible $X = \operatorname{Spec} A$ de dimensión n, es regular en un punto cerrado $x \in X$ si y sólo si existen n hipersuperficies, $(f_i)_0$, que se cortan con multiplicidad 1 en x".

4. Proposición : *El anillo local de $k[x_1, \ldots, x_n]$ en el origen es un anillo regular de dimensión n.*

Demostración. Denotemos $\mathfrak{m} = (x_1, \ldots, x_n)$. Sabemos que $k[x_1, \ldots, x_n]_\mathfrak{m}$ es un anillo local de dimensión n. Como $\dim_k \mathfrak{m}/\mathfrak{m}^2 = n$ se concluye. □

5. Teorema : *$\mathcal{O}$ es regular si y sólo si $G_\mathfrak{m}\mathcal{O} = k[x_1, \ldots, x_n]$, con $k = \mathcal{O}/\mathfrak{m}$. Es decir, $\mathcal{O}$ es regular si y sólo si el cono tangente en el punto cerrado es un espacio afín.*

Demostración. Si $\mathcal{O}$ es un anillo regular de dimensión n, existe un sistema de parámetros $f_1, \ldots, f_n$ que genera el ideal maximal $\mathfrak{m}$ de $\mathcal{O}$. Se tiene entonces un epimorfismo graduado

$$\begin{aligned} k[x_1, \ldots, x_n] &\longrightarrow G_\mathfrak{m}\mathcal{O} \\ x_i &\longmapsto \bar{f}_i \end{aligned}$$

que además es inyectivo por 4.3.8.

Recíprocamente, si $G_\mathfrak{m}\mathcal{O} = k[x_1, \ldots, x_n]$, entonces por 4.3.8, $\dim \mathcal{O} = n$. Además

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k (x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 = n$$

luego $\mathcal{O}$ es regular.

□

6. Lema de Krull: *Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Entonces*

$$\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$$

Demostración. Procedamos por inducción sobre $\dim \mathcal{O}$. Si $\dim \mathcal{O} = 0$, entonces $\mathfrak{m}^n = 0$ para $n >> 0$ y se concluye. Sea $\dim \mathcal{O} = n > 0$. Sea $f \in \mathcal{O}$ de modo que $\dim (f)_0 = n - 1$. Por hipótesis de inducción $\bigcap_{n \in \mathbb{N}} \bar{\mathfrak{m}}^n = 0$ en $\mathcal{O}/(f)$, luego $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n \subseteq (f)$. Igualmente, $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n \subseteq (f^r)$, para todo $r \in \mathbb{N}$. Así pues, dada $g \in \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$, tenemos que $g = f \cdot g_1 = f^2 \cdot g_2 = \ldots$. Tenemos la cadena de inclusiones $(g_1) \subseteq (g_1, g_2) \subseteq \cdots$. Por noetherianidad, para algún i, $(g_1, \ldots, g_i) = (g_1, \ldots, g_{i+1})$. Entonces, $(g_{i+1}) \subseteq (g_1, \ldots, g_i)$ y

$$(g) = f^{i+1}(g_{i+1}) \subseteq f \cdot f^i \cdot (g_1, \ldots, g_i) \subseteq f \cdot (g)$$

y por el lema de Nakayama $g = 0$ y $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$. □

7. Proposición : *Si $\mathcal{O}$ es regular, entonces es íntegro.*

Demostración. Sean $f, g \in \mathcal{O}$, no nulas. Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Por el Lema de Krull, $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$. Por tanto, existen $r, s \in \mathbb{N}$ de modo que $f \in \mathfrak{m}^r - \mathfrak{m}^{r+1}$, $g \in \mathfrak{m}^s - \mathfrak{m}^{s+1}$. Es decir, $\bar f \in \mathfrak{m}^r/\mathfrak{m}^{r+1}$ y $\bar g \in \mathfrak{m}^s/\mathfrak{m}^{s+1}$ son no nulas.

Si $\mathcal{O}$ es regular, entonces $G_{\mathfrak{m}}\mathcal{O} = k[x_1, \dots, x_n]$ es un anillo íntegro. Por tanto, $\bar f \cdot \bar g \neq 0$, luego $\bar f \cdot \bar g = \overline{f \cdot g} \in \mathfrak{m}^{r+s}/\mathfrak{m}^{r+s+1}$ no es nulo y $f \cdot g \neq 0$. □

Sea x el punto cerrado de $\operatorname{Spec}\mathcal{O}$. Si $f \in \mathfrak{m}_x$, denotaremos $d_x f$ la clase de f en $\mathfrak{m}_x/\mathfrak{m}_x^2$ y la denominaremos diferencial de f en x. En el caso de que $\mathcal{O}$ sea una k-álgebra y $\mathcal{O}/\mathfrak{m}_x = k$, denotaremos $f(x) = \bar f \in \mathcal{O}/\mathfrak{m}_x = k$ y definiremos $d_x f = \overline{f - f(x)} \in \mathfrak{m}_x/\mathfrak{m}_x^2$.

8. Teorema: *Sea $\mathcal{O}$ un anillo local regular de ideal maximal $\mathfrak{m}_x$ y sea $I \subset \mathcal{O}$ un ideal. Entonces $\mathcal{O}/I$ es regular $\Leftrightarrow$ I está generado por un sistema de parámetros cuyas diferenciales en x son linealmente independientes.*

Demostración. Denotemos $\bar{\mathfrak{m}}_x$ la imagen de $\mathfrak{m}_x$ en $\mathcal{O}/I$.

$\Leftarrow$) Si $I = (f_1, \dots, f_r)$ y $\{d_x f_1, \dots, d_x f_r\}$ son linealmente independientes en $\mathfrak{m}_x/\mathfrak{m}_x^2$, entonces la sucesión

$$0 \to I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

es exacta, porque $\bar f_1, \dots, \bar f_r$ es un sistema generador de $I/\mathfrak{m}_x I$ linealmente independiente en $\mathfrak{m}_x/\mathfrak{m}_x^2$. Por tanto,

$$\dim_{\mathcal{O}/\mathfrak{m}_x} \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 = \dim_{\mathcal{O}/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 - r = \dim \mathcal{O} - r \leq \dim \mathcal{O}/I$$

luego $\mathcal{O}/I$ es regular (y de dimensión $\dim \mathcal{O} - r$).

$\Rightarrow$) Supongamos que $\mathcal{O}/I$ es regular. Escribamos $\dim \mathcal{O} = n$ y $\dim \mathcal{O}/I = n - r$. Consideremos la sucesión exacta

$$I/\mathfrak{m}_x I \to \mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2 \to 0$$

Sean $f_1, \dots, f_r \in I$ tales que $\bar f_1, \dots, \bar f_r$ sea una base del núcleo del epimorfismo $\mathfrak{m}_x/\mathfrak{m}_x^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2$. Se tiene un epimorfismo $\mathcal{O}/(f_1, \dots, f_r) \to \mathcal{O}/I$, que es isomorfismo: en efecto, por la implicación anterior, $\mathcal{O}/(f_1, \dots, f_r)$ es regular y de dimensión $n - r$; si hubiese núcleo, la dimensión de $\mathcal{O}/I$ sería menor que $n - r$, por 2.8.9, ya que $\mathcal{O}/(f_1, \dots, f_r)$ es íntegro por ser regular.

En conclusión, $I = (f_1, \dots, f_r)$ y $d_x f_1, \dots, d_x f_r$ son linealmente independientes. □

Los anillos locales de una variedad diferenciable, si bien no son noetherianos, pueden considerarse regulares, pues el cono tangente en todo punto es un espacio afín. Sea X una variedad diferenciable e Y el cerrado definido por r funciones diferenciables $f_1, \dots, f_r \in \mathcal{C}^\infty(X)$. Es bien conocido en Geometría Diferencial que si $d_y f_1, \dots, d_y f_r$ son linealmente independientes para todo $y \in Y$, entonces Y es una subvariedad diferenciable de X.

4.4.1 Grado de trascendencia y dimensión del módulo de diferenciales

Queremos relacionar la regularidad con la “lisitud”. Con otras palabras, queremos relacionar la regularidad de una variedad en un punto, con el rango de las diferenciales de Kähler en el punto. Empecemos relacionando la dimensión de una variedad con el rango de las diferenciales de Kähler.

9. Proposición: *Sea $k \to K = k(\xi_1, \dots, \xi_m)$ una extensión de tipo finito. Se verifica*

$$\dim_K \Omega_{K/k} \geq \operatorname{gr}\operatorname{tr}_k K$$

Además, la desigualdad es una igualdad si y sólo si existe una base de trascendencia $\{x_1, \dots, x_n\}$ tal que $k(x_1, \dots, x_n) \hookrightarrow K$ sea una extensión separable.

Demostración. Sea $\Sigma \to \Sigma(\xi)$ una extensión. Se verifica que

$$\dim_{\Sigma(\xi)} \Omega_{\Sigma(\xi)/k} = \begin{cases} \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es trascendente} \\ \dim_\Sigma \Omega_{\Sigma/k} \text{ ó } \dim_\Sigma \Omega_{\Sigma/k} + 1, & \text{si } \xi \text{ es algebraico} \end{cases}$$

En efecto: Consideremos $\Sigma[x]$. Tenemos que

$$\Omega_{\Sigma[x]/k} = \Omega_{\Sigma \otimes_k k[x]/k} = (\Omega_{\Sigma/k} \otimes_k k[x]) \oplus (\Sigma \otimes_k \Omega_{k[x]/k}) = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma[x]) \oplus \Sigma[x]dx$$

Localizando en el punto genérico de $\Sigma[x]$

$$\Omega_{\Sigma(x)/k} = (\Omega_{\Sigma/k} \otimes_\Sigma \Sigma(x)) \oplus \Sigma(x)dx$$

y se concluye la primera parte. Supongamos ahora que ξ es algebraico. Así pues, $\Sigma(\xi) = \Sigma[x]/(p(x))$. De la sucesión exacta $0 \to (p(x)) \to \Sigma[x] \to \Sigma(\xi) \to 0$, se obtiene la sucesión exacta de diferenciales

$$\begin{array}{ccc} (p(x))/(p(x)^2) & \to & \Omega_{\Sigma[x]/k} \underset{\Sigma[x]}{\otimes} \Sigma(\xi) \to \Omega_{\Sigma(\xi)/k} \to 0 \\ p(x) & \mapsto & dp(x) \end{array}$$

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

$$(**) \qquad \Omega_{K'/k} \otimes_{K'} K \xrightarrow{i^*} \Omega_{K/k} \to \underset{\substack{\| \\ 0}}{\Omega_{K/K'}} \to 0$$

deducimos que i^* es un epimorfismo, luego $\dim_K \Omega_{K/k} \leq \dim_{K'} \Omega_{K'/k} = n = \operatorname{gr}\operatorname{tr}_k K$ y por tanto $\dim_K \Omega_{K/k} = \operatorname{gr}\operatorname{tr}_k K$.

Recíprocamente, si $\dim_K \Omega_{K/k} = \operatorname{gr}\operatorname{tr}_k K = n$, sean $x_1, \dots, x_n \in K$ tales que $dx_1, \dots, dx_n$ sean una base de $\Omega_{K/k}$. De la sucesión $**$ obtenemos que i^* es epiyectiva, luego $\Omega_{K/K'} = 0$. Por tanto, $K' \hookrightarrow K$ es finita y separable y $\{x_1, \dots, x_n\}$ es una base de trascendencia. $\square$

10. Proposición : *Si k es un cuerpo perfecto y K es una extensión de tipo finito entonces existe una base de trascendencia $\{x_1, \dots, x_n\}$ de modo que el morfismo $k(x_1, \dots, x_n) \hookrightarrow K$ es separable y $\Omega_{K/k} = Kdx_1 \oplus \dots \oplus Kdx_n$.*

Demostración. Sean $x_1, \dots, x_n \in K$ tales que $dx_1, \dots, dx_n$ sean una base de $\Omega_{K/k}$. El morfismo $k(x_1, \dots, x_n) \hookrightarrow K$ es separable, por la sucesión exacta $**$ de la proposición anterior. Sólo tenemos que ver que $x_1, \dots, x_n$ son algebraicamente independientes. Si no fuesen algebraicamente independientes, sea $p(x_1, \dots, x_n) = 0$ una relación algebraica de grado mínimo. Entonces, $dp(x_1, \dots, x_n) =$

$\sum_i \frac{\partial p}{\partial x_i} dx_i = 0$, luego $\frac{\partial p}{\partial x_i} = 0$ para todo i, de donde se deduce que $p(x_1, \dots, x_n) = q(x_1^p, \dots, x_n^p)$. 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 $x_1, \dots, x_n$. Contradicción.

Por dimensiones y por la sucesión exacta $**$ de la proposición anterior, concluimos que $\Omega_{K/k} = K dx_1 \oplus \dots \oplus K dx_n$. □

4.4.2 Criterios diferenciales de regularidad

11. Definición : Sea $X = \operatorname{Spec} A$. Diremos que X es regular en un punto cerrado x, si A_x es un anillo regular. Diremos que X es regular si lo es en todo punto cerrado.

12. Ejercicio : Sea $X = \operatorname{Spec} k[x_1, \dots, x_n]/(p(x_1, \dots, x_n))$. Demostrar que X es regular en un punto $\alpha = (\alpha_1, \dots, \alpha_n)$ si y sólo si $\sum\limits_i \frac{\partial p}{\partial x_i}(\alpha_1, \dots, \alpha_n) d_\alpha x_i \neq 0$

13. Teorema : *Sea k un cuerpo algebraicamente cerrado. Sea $\mathcal{O}$ el anillo local en un punto cerrado de una variedad algebraica sobre k. Entonces*

$$\mathcal{O} \textit{ es regular} \Leftrightarrow \Omega_{\mathcal{O}/k} \textit{ es un } \mathcal{O}\textit{-módulo libre de rango } \dim \mathcal{O}.$$

Demostración. $\Rightarrow$) Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$ y Σ el cuerpo de fracciones de $\mathcal{O}$. Como $\mathcal{O}$ es regular $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim \mathcal{O} = \operatorname{gr}\operatorname{tr} \Sigma = n$. Sea $\omega_1, \dots, \omega_n$ un sistema generador de $\Omega_{\mathcal{O}/k}$ obtenido por Nakayama (recordemos que $\Omega_{\mathcal{O}/k} \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = \mathfrak{m}/\mathfrak{m}^2$). Consideremos la sucesión exacta

$$\begin{gathered} 0 \to \operatorname{Ker} \phi \to \mathcal{O} \oplus \overset{n}{\cdots} \oplus \mathcal{O} \xrightarrow{\phi} \Omega_{\mathcal{O}/k} \to 0 \\ (0,\dots, \underset{i}{1},\dots, 0) \longmapsto \omega_i \end{gathered}$$

Localizando en el punto genérico (los anillos regulares son íntegros) tenemos

$$0 \to (\operatorname{Ker} \phi)_0 \longrightarrow \Sigma \oplus \overset{n}{\cdots} \oplus \Sigma \longrightarrow \Omega_{\Sigma/k} \to 0$$

Ahora bien, por la proposición 4.4.10, $\dim_\Sigma \Omega_{\Sigma/k} = \operatorname{gr}\operatorname{tr} \Sigma = n$. Por tanto, $(\operatorname{Ker} \phi)_0 = 0$. Pero $\operatorname{Ker} \phi$ está incluido en un $\mathcal{O}$-módulo libre, que no tiene torsión, luego $\operatorname{Ker} \phi = 0$ y $\Omega_{\mathcal{O}/k} = \mathcal{O} \oplus \overset{n}{\cdots} \oplus \mathcal{O}$.

$\Leftarrow$) Si $\Omega_{\mathcal{O}/k}$ es un $\mathcal{O}$-módulo libre de rango $\dim \mathcal{O}$, entonces $\dim \mathcal{O} = \dim_{\mathcal{O}/\mathfrak{m}}(\Omega_{\mathcal{O}/k} \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}) = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, luego $\mathcal{O}$ es regular.

□

14. Ejercicio : Sea $k = \mathbb{Z}/3\mathbb{Z}(t)$ y $A = \operatorname{Spec} k[x, y]/(y^2 + x^3 - t)$. Demostrar que la curva plana $\operatorname{Spec} A$ es regular en todo punto cerrado pero $\Omega_{A_x/k}$ no es un A_x-módulo libre de rango 1 para $\mathfrak{m}_x = (x^3 - t, y)$.

15. Definición : Se dice que una variedad algebraica conexa es lisa si su módulo de diferenciales es localmente libre de rango igual a la dimensión. En general, una variedad algebraica se dice lisa si lo es cada componente conexa.

Una variedad algebraica es lisa si y sólo si lo es por cambio de base, pues el módulo de diferenciales, el rango y la dimensión cambian de base . El teorema anterior dice que sobre cuerpos algebraicamente cerrados las variedades lisas coinciden con las regulares. El ejercicio anterior muestra que el concepto de regularidad no es estable por cambio de base, pues la curva del ejercicio no es lisa pero sí regular y por cambio de base al cierre algebraico no es lisa, luego tampoco regular.

16. Proposición: *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra sobre un cuerpo k algebraicamente cerrado. El conjunto de puntos cerrados regulares 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 $\dim_\Sigma \Omega_{\Sigma/k} = \operatorname{gr}\operatorname{tr}\Sigma = \dim X$. 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 regular. Como el conjunto de puntos donde $\Omega_{A/k}$ es libre es un abierto (no vacío porque contiene al punto genérico), se concluye por ser k algebraicamente cerrado. □

17. Lema : *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$, M un $\mathcal{O}$-módulo finito y $f\colon M \to L$ un morfismo en un libre finito. Si $\bar{f}\colon M/\mathfrak{m}M \to L/\mathfrak{m}L$ es inyectivo, entonces f es inyectivo.*

Demostración. Sea $m_1, \dots, m_r$ un sistema generador de M obtenido por Nakayama y $l_1, \dots, l_r$ sus imágenes en L. Dado que $\bar{f}$ es inyectivo, existen $l_{r+1}, \dots, l_n \in L$ tales que $\bar{l}_1, \dots, \bar{l}_n$ son base de $L/\mathfrak{m}L$. Denotemos $L' =< l_{r+1}, \dots, l_n >$. El morfismo $f \oplus \mathrm{id}\colon M \oplus L' \to L$ es epiyectivo pues es isomorfismo al hacer módulo $\mathfrak{m}$. Denotemos $N = \operatorname{Ker}(f \oplus \mathrm{id})$. La sucesión exacta

$$0 \to N \to M \oplus L' \to L \to 0$$

rompe porque L es libre, luego N es finito y la sucesión vuelve a ser exacta al tensorializar por $\mathcal{O}/\mathfrak{m}$, de donde se deduce que $N \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = 0$ y por tanto $N = 0$. Es decir, $f \oplus \mathrm{id}$ es isomorfismo y f es inyectiva. □

18. Criterio Jacobiano de lisitud: *Sea $X = \operatorname{Spec} A$ una variedad algebraica regular sobre un cuerpo algebraicamente cerrado. Sea $Y = \operatorname{Spec} A/I \subset X$ una subvariedad. Entonces Y es regular si y sólo si*

1. *$\Omega_{(A/I)/k}$ es localmente libre.*

2. *La sucesión $0 \to I/I^2 \to \Omega_{A/k} \otimes_A A/I \to \Omega_{(A/I)/k} \to 0$ es exacta.*

Demostración. 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 tensorializar 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 4.4.8 A/I es regular.

$\Rightarrow$) Si Y es regular, ya sabemos que satisface la condición 1. Sólo queda probar que la sucesión de 2. es exacta por la izquierda. Por el lema anterior, basta ver que

$$I/\mathfrak{m}_x I \xrightarrow{\bar{i}} \mathfrak{m}_x/\mathfrak{m}_x^2$$

es inyectivo. Esto último es consecuencia directa de 4.4.8. □

4.5 Problemas

1. Sea $A = k[x_1, \dots, x_n]$. Probar que $\Omega_{A/k} = Adx_1 \oplus \cdots \oplus Adx_n$.

2. Sea $A = k[x](p(x))$. Probar que $\Omega_{A/k} = k[x]/(p, p')dx$. Probar que $\Omega_{A/k} = 0 \Leftrightarrow p(x)$ tiene raíces dobles.

3. Sea B una A-álgebra y $M = (\underset{b\in B}{\oplus} B\cdot db)/N$, donde N es el submódulo del módulo libre $(\underset{b\in B}{\oplus} B\cdot db)$, generado por los elementos $d(b_1b_2) - b_1 \cdot db_2 - b_2 \cdot db_1$, $d(b_1 + b_2) - db_1 - db_2$, da ($a \in A$, $b_1, b_2 \in B$). Demostrar que

   (a) $M \simeq \Omega_{B/A}$.

   (b) El morfismo $d\colon \Omega_{B/A} \to \Omega_{B/A} \wedge \Omega_{B/A}$, $d(b \cdot db') := db \wedge db'$, está bien definido.

   (c) El morfismo $d_n\colon \Lambda^n\Omega_{B/A} \to \Lambda^{n+1}\Omega_{B/A}$, $d_n(b \cdot db_1 \wedge \ldots \wedge db_n) := db \wedge db_1 \wedge \ldots \wedge db_n$, está bien definido.

4. Sea $k = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^{\frac{1}{p}})$, $A = k[x]/(x^p - t)^n$. Calcular $\Omega_{A/k}$, $\Omega_{A/K}$ y $\Omega_{K/k}$.

5. Probar que una k-álgebra finita A es separable si y sólo si $\Omega_{A/k} = 0$.

6. Sea $\mathfrak{m}_x = (x_1, \dots, x_n)$ y $\mathcal{O} = (k[x_1, \dots, x_n]/(p_1, \dots, p_r))_x$. Supongamos que $\dim \mathcal{O} = n - r$. Probar que $\mathcal{O}$ es regular si y sólo si $\operatorname{rg}(\frac{\partial p_i}{\partial x_j}(0)) = r$.

7. Sean X e Y dos k-variedades algebraicas y $x \in X$ e $y \in Y$ dos puntos racionales regulares. Probar que $X \times_k Y$ es regular en (x, y).

Capítulo 5

Curvas planas

5.1 Explosión de curvas planas

Consideremos el nodo $y^2 - x^2 + x^3 = 0$. Voy a "levantar" esta curva a una curva en $\mathbb{A}_3$, de modo que el nudo se deshaga. Consideremos la hipersuperficie de $\mathbb{A}_3$, $y = zx$, que es el conjunto de las rectas $y = \alpha x$ (sobre los planos $z = \alpha$). Si consideramos la intersección del cilindro de $\mathbb{A}_3$ $y^2 - x^2 + x^3 = 0$ con la hipersuperficie $y = zx$, quitamos el eje z y tomamos el cierre de la curva obtenida construimos el levantamiento buscado. En coordenadas, la curva levantada es $\frac{y^2-x^2+x^3}{x^2} = (\frac{y}{x})^2 - 1 + x = 0$, es decir, la curva $z^2 - 1 + x = 0$ sobre la superficie $y = zx$. Así pues, la curva levantada es $\operatorname{Spec} k[x,y,z]/(z^2-1+x, y-zx) = \operatorname{Spec} k[x,z]/(z^2-1+x)$. El cálculo de la multiplicidad de intersección del nodo $y^2 - x^2 + x^3$ con otra curva plana $q(x,y) = q_s(x,y) + \cdots + q_n(x,y)$ en el origen se reduce al cálculo de la multiplicidad de intersección de $\frac{y^2-x^2+x^3}{x^2} = 0$ con $\frac{q(x,y)}{x^s} = 0$, como veremos.

1. Teorema : *Sea $C \equiv p(x,y) = 0$ una curva plana y supongamos que la recta $x = 0$ no es tangente a la curva en $p = (0,0)$. Escribamos $p(x,y) = p_r(x,y) + p_{r+1}(x,y) + \cdots + p_n(x,y)$ y $\frac{p(x,y)}{x^r} = p_r(1, \frac{y}{x}) + p_{r+1}(1, \frac{y}{x})x + \cdots + p_n(1, \frac{y}{x})x^{n-r} = \tilde{p}(x,z)$ (donde $z = \frac{y}{x}$) y $\tilde{C} \equiv \tilde{p}(x,z) = 0$. Consideremos el morfismo natural $i\colon k[x,y]/(p(x,y)) \to k[x,z]/(\tilde{p}(x,z))x \mapsto x, y \mapsto xz$. Se cumple que*

1. $(k[x,y]/(p(x,y)))_x = (k[x,z]/(\tilde{p}(x,z)))_x$
2. *El número de puntos (distintos o no) de la fibra de p por i^* es igual al número de tangentes (distintas o no) de C en p.*
3. $(i^*)^{-1}(p) = (x)_0 \cap \tilde{C}$ *en* $\operatorname{Spec} k[x,z]$. *Por tanto por 2., $\mu_p(C)$ coincide con la multiplicidad de intersección de $(x)_0$ con $\tilde{C}$.*
4. $\tilde{C} = (i^*)^{-1}(p) \coprod (C - (x)_0)$.
5. $i_p\colon A = (k[x,y]/(p(x,y)))_p \to B = (k[x,z]/(\tilde{p}(x,z)))_p, x \mapsto x, y \mapsto xz$ *es un morfismo finito. Además, i_p es un isomorfismo si y sólo si p es un punto no singular de C.*

Demostración. El punto 1. es obvio, sin más que observar que el morfismo inverso es $x \mapsto x$, $z \mapsto \frac{y}{x}$.

Tenemos que

$$(i^*)^{-1}(p) = \operatorname{Spec} k[x,z]/(\tilde{p}(x,z), x, xz) = \operatorname{Spec} k[z]/(p_r(1,z))$$

y fácilmente se concluye el punto 2 y que $(i^*)^{-1}(p) = (x)_0 \cap \tilde{C}$.

Del punto 1. se deduce que $\tilde{C} = (i^*)^{-1}(p) \coprod (\tilde{C} - (x)_0) = (i^*)^{-1}(p) \coprod (C - (x)_0)$.

Veamos el punto 5.: Obviamente x es finito sobre A y z también: $p(x,y) = y^r \cdot q_1(x,y) + q_2(x,y)$, donde $q_2(x,y)$ es un polinomio en y de grado menor que r, con coeficientes en $k[x]$ y $q_1(0,0) \neq 0$ (porque $p_r(0,y) = ay^r$, con $a \neq 0$, pues $x = 0$ no es una tangente a la curva en el origen), luego $q(x,y)$ es un invertible de A y B. Por tanto,

$$\begin{aligned} 0 = \tilde{p}(x,z) = \frac{p(x,y)}{x^r} &= (\frac{y}{x})^r(inv) + \text{ polinomio en } \frac{y}{x} \text{ con coeficientes en } k[x], \text{ de grado} < r \\ &= z^r(inv) + \text{ polinomio en } z \text{ con coeficientes en } k[x], \text{ de grado} < r \end{aligned}$$

Luego i es un morfismo finito.

Si $r = 1$ entonces $x, z \in A$ e i_p es un isomorfismo. Recíprocamente si i_p es un isomorfismo entonces $r = \#(i_p^*)^{-1}(p) = 1$ y p es un punto no singular.

□

2. Observación: De la ecuación entera que cumple z se obtiene que $B = A + Az + \ldots + Az^{r-1}$. Por tanto, $(x,y)^r \cdot B = (x,zx)^r \cdot B = x^r \cdot B = Ax^r + Ax^{r-1}y + \ldots + Ay^r = (x,y)^r$

Diremos que $\tilde{C} = \operatorname{Spec} k[x,z]/(\tilde{p}(x,z))$ es la explosión de C en p, que el morfismo $i^* \colon \tilde{C} \to C$ es el morfismo de explosión o una transformación cuadrática, que $(i^*)^{-1}(p)$ es la fibra excepcional y que $(x)_0 \subset \operatorname{Spec} k[x,z]$ es el ciclo excepcional.

3. Teorema: *Sean $C \equiv p(x,y) = 0$ y $C' = q(x,y) = 0$ dos curvas planas sin componentes comunes, y $p \in C \cap C'$. Se cumple que*

$$\mu_p(C \cap C') = \mu_p(C) \cdot \mu_p(C') + \sum_{p_i \in Fibra\ excep.} \mu_{p_i}(\tilde{C} \cap \tilde{C}')$$

Demostración. Podemos suponer que $p = (0,0)$ y que $x = 0$ no es tangente a C ni a C'. Escribamos $p(x,y) = p_r(x,y) + p_{r+1}(x,y) + \cdots + p_n(x,y)$, $q(x,y) = q_s(x,y) + \cdots + q_m(x,y)$. Podemos suponer que $p(x,y)$ es irreducible, porque $\mu_p(C_1 \cup C_2) = \mu_p(C_1) + \mu_p(C_2)$ y $\mu_p(C_1 \cup C_2, C') = \mu_p(C_1, C') + \mu_p(C_2, C')$ (como esencialmente hemos visto en 3.4.4) y la explosión de la unión es la unión de los explotados.

Consideremos el morfismo

$$A = (k[x,y]/(p(x,y)))_p \overset{i}{\hookrightarrow} (k[x,z]/(\tilde{p}(x,z))_p = B$$

Se verifica que i es un morfismo finito y birracional por el teorema anterior. Por tanto, el ideal anulador $I \subset A$ de B/A es no nulo. Como B/A es un A/I-módulo finito, y A/I un k-espacio vectorial de dimensión finita tenemos que B/A es un k-espacio vectorial de dimensión finita. Por el lema que sigue

$$\begin{aligned} \dim_k A/(q(x,y)) &= \dim_k B/(q(x,y)) = \dim_k B/(x^s \cdot \tilde{q}(x,z)) \\ &= \dim_k B/(x^s) + \dim_k B/(\tilde{q}(x,z)) = s \cdot \dim_k B/(x) + \dim_k B/(\tilde{q}(x,z)) \end{aligned}$$

Ahora bien, por el punto 3. del teorema $B/(x) = r$. En conclusión,

$$\mu_p(C \cap C') = \dim_k A/(q(x,y)) = s \cdot r + \dim_k B/(\tilde{q}(x,z)) = \mu_p(C) \cdot \mu_p(C') + \sum_{p_i \in \text{Fibra excep.}} \mu_{p_i}(\tilde{C} \cap \tilde{C}')$$

$\square$

4. Lema : *Sean A y B k-álgebras íntegras y $A \hookrightarrow B$ un morfismo de k-álgebras. Supongamos que $A/aA, B/aB$ y B/A son k-espacios vectoriales de dimensión finita. Se cumple que*

$$\dim_k A/aA = \dim_k B/aB$$

Demostración. Consideremos el diagrama

$$\begin{tikzcd} aA \arrow[r, hook] & aB \\ A \arrow[u, hook] \arrow[r, hook] & B \arrow[u, hook] \end{tikzcd}$$

Entonces

$$\dim_k B/aB + \dim_k aB/aA = \dim_k B/aA = \dim_k B/A + \dim_k A/aA$$

Observemos que $B/A \simeq aB/aA, \bar{b} \mapsto \overline{ab}$. Por tanto, $\dim_k A/aA = \dim_k B/aB$ $\square$

5. Ejercicio : Siguiendo las notaciones de la proposición anterior, probar que C y C' no tienen tangentes comunes en p si y sólo si $p_r(1, \frac{y}{x})$, $q_s(1, \frac{y}{x})$ son primos entre si, o equivalentemente si $\frac{q(x,y)}{x^s} = \tilde{q}(x,z)$ es invertible en B. Concluir que C y C' no tienen tangentes comunes en p si y sólo si su multiplicidad de intersección en p es igual al producto de la multiplicidad de C en p por la de C' en p.

6. Corolario : *La multiplicidad de una curva plana $p(x,y) = 0$ en un punto es r si existe una curva no singular en p que corte a la curva con multiplicidad r en el punto, y toda otra curva no singular en p corta a la curva con multiplicidad mayor o igual que r. Una recta será tangente a la curva en el punto si y sólo si la corta con multiplicidad mayor que r.*

7. Corolario : *La multiplicidad de una curva plana en un punto p es mayor o igual que la suma de las multiplicidades de los puntos de la fibra excepcional de la explosión de la curva plana en el punto p y es estrictamente mayor si y sólo si el ciclo excepcional es tangente a la curva explotada.*

Demostración. Recordemos que $\mu_p(C)$ es igual a la multiplicidad de intersección del ciclo excepcional con la curva explotada. Como el ciclo excepcional es una recta (luego no singular), la multiplicidad de intersección del ciclo excepcional con la curva explotada es igual a la suma de las multipicidades de los puntos de la fibra excepcional, cuando el ciclo excepcional no sea tangente a la curva explotada. En caso contrario es mayor. $\square$

8. Ejercicio : Sea $C \equiv p(x,y) = 0$ una curva plana, x', y' polinomios que se anulan en el origen tales que $k[x,y] = k[x',y']$. Escribamos $p(x,y) = p'(x',y')$. Supongamos que x' no es tangente a C en el origen. Demostrar que

$$(k[x,z]/(\tilde{p}(x,z)))_{\frac{x'}{x}} = (k[x',z']/(\tilde{p}'(x',z')))_{\frac{x}{x'}}$$

Justificar que la explosión de una curva plana en un punto p no depende, localmente en p, del sistema de coordenadas.

5.2 Desingularización de curvas planas vía el contacto maximal

En esta sección vamos a demostrar, dada una curva plana, la existencia de curvas de "contacto maximal". Es decir, dada una curva y un punto de ella, existe una curva regular, que pasa por el punto, con multiplicidad de corte con la curva dada, en el punto dado, máxima. Esta curva, verificará que pasa por el punto y los puntos de las sucesivas fibras excepcionales siempre que no bajen de multiplicidad. Como la multiplicidad de corte de dos curvas es finita (siempre que no tengan componentes comunes) obtendremos que la multiplicidad de una curva en un punto habrá de bajar después de un número finito de explosiones. Así podremos demostrar la desingularización de las curvas planas por un número finito de explosiones.

Otra razón fundamental de la introducción de este apartado es que las técnicas e ideas aquí desarrolladas para la desingularización de curvas planas son básicamente las usadas para la desingularización de superficies.

En este apartado supondremos que k es un cuerpo algebraicamente cerrado de característica cero.

1. Lema : *Sea $p(x,y)=0$ una curva de multiplicidad m en un punto p y sea $D\colon k[x,y]\to k[x,y]$ una derivación. Entonces la curva $Dp(x,y)=0$ tiene multiplicidad mayor o igual que $m-1$.*

Demostración. Denotemos $C\equiv p(x,y)=0$, $m_p(C)=m$ si y sólo si $p(x,y)\in\mathfrak{m}_p^m-\mathfrak{m}_p^{m+1}$. Por tanto, $p(x,y)=\sum f_{i_1}\cdots f_{i_m}$, con $f_{i_j}\in\mathfrak{m}_p$. Así pues, $Dp(x,y)=\sum f_{i_1}\cdots Df_{i_j}\cdots f_{i_m}\in\mathfrak{m}_p^{m-1}$. Con lo que concluimos. □

2. Observación : El lema sigue siendo cierto para operadores diferenciales de orden 1, es decir, para $D=h+D_0$, $D(p):=h\cdot p+D_0p$ (con $h\in k[x,y]$ y D_0 derivación).

3. Lema : *Con las notaciones anteriores, existe una derivación D, tal que $Dp(x,y)=0$ tiene multiplicidad $m-1$ en p.*

Demostración. Podemos suponer que p es el origen de coordenadas, es decir, $\mathfrak{m}_p=(x,y)$. Escribamos $p(x,y)$ como suma de polinomios homogéneos

$$p(x,y)=p_m(x,y)+p_{m+1}(x,y)+\cdots+p_n(x,y)\qquad p_m(x,y)=\sum_{r=0}^{m}\lambda_r x^r y^{m-r}$$

Como $m\geq 1$, en la expresión de $p_m(x,y)$, parece x o y. Supongamos que aparece y, es decir, $\lambda_r\neq 0$ para algún $r\neq m$. Entonces

$$\frac{\partial}{\partial y}p(x,y)=\sum_{r=0}^{m}(m-r)\lambda_r x^r y^{m-r-1}+\text{monomios de grado mayor o igual que } m$$

Como $\sum\limits_{r=0}^{m}(m-r)\lambda_r x^r y^{m-r-1}\neq 0$, concluimos que $Dp(x,y)=0$ tiene multiplicidad $m-1$. □

Denotemos $A=k[x,y]$ y $\bar{A}=A[\frac{x}{t},\frac{y}{t}]$, con $t=\lambda\cdot x+\mu\cdot y$ (por ejemplo, si $\mu\neq 0$ entonces $k[x,y]=k[x,t]$ y $\bar{A}=k[x,\frac{x}{t}]$).

4. Lema fundamental : *Sea $D\colon A \to A$ un operador diferencial de orden 1. Existe un operador diferencial de orden 1 $\bar{D}\colon \bar{A} \to \bar{A}$ tal que para todo $P \in A$ (de multiplicidad m en el origen) se verifica*

$$\frac{DP}{t^{m-1}} = \bar{D}(\frac{P}{t^m})$$

"La transformada propia de la derivada es la derivada de la transformada propia".

Demostración. Todo operador diferencial de orden 1 es la suma de una homotecia y una derivación. Basta demostrar el lema para cuando D sea una homotecia y para cuando sea una derivación.

1. Sea $D = h$ una homotecia, i.e., $DP = h \cdot P$. Tomando $\bar{D} = t \cdot h$ se cumple la igualdad requerida.

2. Sea D una derivación. Tenemos que

$$\frac{DP}{t^{m-1}} = (tD)(\frac{P}{t^m}) + (mDt)(\frac{P}{t^m}) = \bar{D}(\frac{P}{t^m})$$

donde $\bar{D} = m \cdot Dt + tD$. Observemos que $\bar{D}$ es un operador diferencial de orden 1 porque $m \cdot Dt$ es una homotecia y tD es una derivación de A_t que deja estable a $\bar{A}$, pues $\bar{D}(\frac{x}{t}) = Dx - \frac{x}{t}Dt$ y $\bar{D}(\frac{y}{t}) = Dy - \frac{y}{t}Dt$.

□

5. Definición : Sea $p \in C$ y $C_r \to \overset{\pi}{\dots} \to C$ una sucesión de transformaciones cuadráticas. Los puntos de $\pi^{-1}(p)$ se les llamará "puntos de la curva C infinitamente próximos" a p.

6. Teorema de existencia de curvas de contacto maximal : *Sea p un punto de multiplicidad m de una curva plana C. Existe una curva plana C' regular en p que pasa (sus transformadas propias) por todos los puntos de C infinitesimalmente próximos a p de multiplicidad m.*

Demostración. Vamos a proceder por inducción sobre la multiplicidad m de $C \equiv P = 0$ en p.

Si $m = 1$ la propia C es una curva de contacto maximal.

Supongamos que $m > 1$. Consideremos un operador diferencial D de orden 1 tal que $DP = 0$ tenga multiplicidad $m - 1$ en p. Todo punto de C infinitamente próximo a p de multiplicidad m es un punto de $C' \equiv DP = 0$ infinitamente próximo a p de multiplicidad $m - 1$: Sigamos las notaciones del lema fundamental. La explosión de $C \equiv P = 0$ en p tiene de ecuaciones $P/t^m = 0$, la explosión de $\tilde{C} \equiv DP = 0$ en p tiene de ecuaciones $DP/t^{m-1} = \bar{D}(P/t^m) = 0$. Por tanto, si un punto de la explosión de $C \equiv P = 0$ en p tiene multiplicidad m, éste será un punto de la explosión de $\tilde{C} \equiv DP = 0$ en p de multiplicidad mayor o igual $m - 1$. Como la multiplicidad no aumenta después de una explosión, tendremos que si un punto de la explosión de $C \equiv P = 0$ en p tiene multiplicidad m, éste será un punto de la explosión de $\tilde{C} \equiv DP = 0$ en p de multiplicidad $m - 1$. Argumentando del mismo modo con las curvas explotadas $P/t^m = 0$ y $DP/t^{m-1} = \bar{D}(P/t^m) = 0$ concluimos.

Por hipótesis de inducción, existe una curva C' regular en p que pasa (sus transformadas propias) por todos los puntos infinitamente próximos a $p \in \tilde{C} \equiv DP = 0$ de multiplicidad $m - 1$. Por tanto, C' pasa (sus transformadas propias) por todos los puntos de C infinitesimalmente próximos a p de multiplicidad m.

□

7. Corolario : *Toda curva plana reducida desingulariza mediante un número finito de transformaciones cuadráticas.*

Demostración. Escribamos la ecuación de la curva $P = p_1 \cdots p_r = 0$ (con p_i irreducibles y $p_i \neq p_j$ cuando $i \neq j$, pues la curva es reducida). Los puntos singulares de la curva son los que verifican las ecuaciones $P = \frac{\partial P}{\partial x} = \frac{\partial P}{\partial y} = 0$, que son un número de puntos. Sabemos que al explotar en un punto la multiplicidad de los puntos de la fibra excepcional es menor o igual que la del punto (si hay dos o más puntos en la fibra excepcional es menor). El corolario es obvio, si probamos que no puede suceder que un punto tenga multiplicidad m, y que al explotar sucesivamente la multiplicidad se mantenga.

Explotando hasta separar las componentes, podemos suponer que la curva viene definida por los ceros de un polinomio $P = 0$ irreducible.

Consideremos una curva $P' = 0$, regular en p, que pase por todos los puntos infinitesimalmente próximos a $P = 0$, de multiplicidad m. Como la multiplicidad de intersección de éstas dos curvas es finita, tenemos que después de un número finito de explosiones la multiplicidad de C ha de bajar estrictamente.

□

5.3 Teorema de Max Noether

Ahora vamos a demostrar el teorema de Max Noether, con el que se podrán resolver múltiples problemas geométricos, como los teoremas de Pascal y Pappus.

Dado un ideal homogéneo $(p_n(x_0, x_1, x_2)) \subseteq k[x_0, x_1, x_2]$ y un punto $x \in \mathbb{P}_2 - (x_i)_0^h$ denotaremos $[p_n(x_0, x_1, x_2)]_x \underset{\text{Not.}}{=} (p_n(x_0/x_i, x_1/x_i, x_2/x_i))_x \subseteq k[x_0/x_i, x_1/x_i, x_2/x_i]_x$. Puede comprobarse que si $x \in \mathbb{P}_2 - (x_j)_0^h$, entonces $k[x_0/x_i, x_1/x_i, x_2/x_i]_x = k[x_0/x_j, x_1/x_j, x_2/x_j]_x$ y $(p_n(x_0/x_i, x_1/x_i, x_2/x_i))_x = (p_n(x_0/x_j, x_1/x_j, x_2/x_j))_x$.

1. Teorema Max Noether: *Sean $p_i \in k[x_0, x_1, x_2]$ polinomios homogéneos ($i = 1, 2, 3$). Consideremos las curvas proyectivas planas $C_i \equiv p_i = 0$. Supongamos que C_1, C_2 no tienen componentes comunes. Existe una ecuación*

$$p_3 = a \cdot p_1 + b \cdot p_2$$

con a, b polinomios homogéneos de grados $\operatorname{gr} a = \operatorname{gr} p_3 - \operatorname{gr} p_1, \operatorname{gr} b = \operatorname{gr} p_3 - \operatorname{gr} p_2$, si y sólo si para todo $x \in C_1 \cap C_2$ se verifica que $[p_3]_x \subseteq [p_1]_x + [p_2]_x$.

Demostración. Es obvio que si $p_3 = a \cdot p_1 + b \cdot p_2$ entonces $[p_3]_x \subseteq [p_1]_x + [p_2]_x$. Veamos con el recíproco.

Por cambio homogéneo de coordenadas, podemos suponer que $x_0 = 0$ no pasa por 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

$$\frac{p_3}{x_0^{n_3}} = a \cdot \frac{p_1}{x_0^{n_1}} + b \cdot \frac{p_2}{x_0^{n_2}}$$

Tenemos homogeneizando que $x_0^r \cdot p_3 = a' p_1 + b' p_2$. Sea r mínimo en las igualdades de esta forma. Si $r > 0$, entonces $0 = a'(0, x_1, x_2) p_1(0, x_1, x_2) + b'(0, x_1, x_2) p_2(0, x_1, x_2)$. Por tanto, $a'(0, x_1, x_2) = h \cdot p_2(0, x_1, x_2)$ y $b'(0, x_1, x_2) = -h \cdot p_1(0, x_1, x_2)$. Luego $a'' = a' - h \cdot p_2$, $b'' = b' - h \cdot p_1$ son divisibles por x_0 y $x_0^r \cdot p_3 = a'' p_1 + b'' p_2$. Dividiendo en esta igualdad por x_0 llegamos a contradicción, porque $r - 1 < r$.

En conclusión,

$$p_3 = a \cdot p_1 + b \cdot p_2$$

En cuanto a los grados de a y b es fácil demostrar que se puede suponer que cumplen lo requerido.

□

2. Proposición : *Sean C_i curvas proyectivas planas definidas por polinomios homogéneos $p_i \in k[x_0, x_1, x_2]$ ($i = 1, 2, 3$). Supongamos que C_1, C_2 no tienen componentes comunes. Supongamos el cuerpo base k es algebraicamente cerrado. C_3 verifica las condiciones de Noether en un punto cerrado $x \in C_1 \cap C_2$, es decir, $[p_3]_x \subseteq [p_1]_x + [p_2]_x$ si*

1) C_1 y C_2 son simples en x, se cortan transversalmente en x y $x \in C_3$.

2) El punto x es un punto simple de C_1 y $\mu_x(C_1 \cap C_3) \geq \mu_x(C_1 \cap C_2)$ (es decir, la multiplicidad de intersección de C_3 con C_1 en x es mayor o igual que la multiplicidad de intersección de C_2 con C_1 en x).

3) C_1 y C_2 poseen tangentes distintas y $\mu_x(C_3) \geq \mu_x(C_1) + \mu_x(C_2) - 1$.

Demostración. Como la proposición es local, podemos suponer que las curvas C_i son curvas planas afines de ecuaciones $p_i(x, y) = 0$.

1) Por las hipótesis $(k[x, y]/(p_1, p_2))_x = k$. Por tanto, si denotamos $\mathfrak{m}_x$ el ideal maximal de las funciones que se anulan en x, tenemos que $\mathfrak{m}_x = (p_1, p_2)_x$, luego $(p_3)_x \subset (p_1, p_2)_x$.

2) Si x es un punto simple de C_1, entonces $\overline{\mathfrak{m}}_x = (t)$ en $(k[x, y]/(p_1(x, y)))_x$. Además, $\overline{(p_i(x, y))} = (t^{\mu_x(C_i \cap C_1)})$. Por tanto, $\overline{(p_3(x, y))} \subseteq \overline{(p_2(x, y))}$, luego $(p_3)_x \subset (p_1, p_2)_x$.

3) Dado $C \equiv p(x, y) = 0$, denotemos por $\mathcal{O}_C = k[x, y]/(p(x, y))$ y $\mathcal{O}_{C,x}$ la localización de $\mathcal{O}_C$ en x. Vamos a usar la observación 5.1.2, que dice si $\mathcal{O}_{C_1,x} \to \mathcal{O}_{\tilde{C}_1,x}$ es el morfismo de explosión en el punto x entonces $\mathfrak{m}_x^{\mu_x(C_1)-1} = \mathfrak{m}_x^{\mu_x(C_1)-1} \cdot \mathcal{O}_{\tilde{C}_1,x}$.

Por otra parte, si ξ es un parámetro transversal a C_1 en x, por el que explotamos, tenemos que $p_2(x, y) \cdot \mathcal{O}_{\tilde{C}_1,x} = p'(x/\xi, y/\xi) \cdot \xi^{\mu_x(C_2)} \cdot \mathcal{O}_{\tilde{C}_1,x} = \xi^{\mu_x(C_2)} \cdot \mathcal{O}_{\tilde{C}_1,x}$ porque C_1 y C_2 no tienen tangentes comunes en x. Por tanto, $p_2(x, y) \cdot \mathcal{O}_{\tilde{C}_1,x} = \mathfrak{m}_x^{\mu_x(C_2)} \cdot \mathcal{O}_{\tilde{C}_1,x}$.

Con todo,

$$\begin{aligned} p_3(x, y) \in \mathfrak{m}_x^{\mu_x(C_3)} &\subset \mathfrak{m}_x^{\mu_x(C_1)+\mu_x(C_2)-1} = \mathfrak{m}_x^{\mu_x(C_2)} \cdot \mathfrak{m}_x^{\mu_x(C_1)-1} \\ &= \mathfrak{m}_x^{\mu_x(C_2)} \cdot \mathfrak{m}_x^{\mu_x(C_1)-1} \cdot \mathcal{O}_{\tilde{C}_1,x} = p_2(x, y) \cdot \mathfrak{m}_x^{\mu_x(C_1)-1} \cdot \mathcal{O}_{\tilde{C}_1,x} \\ &= p_2(x, y) \cdot \mathfrak{m}_x^{\mu_x(C_1)-1} \subset p_2(x, y)\mathcal{O}_{C_1,x} \end{aligned}$$

por lo que $(p_3)_x \subset (p_1, p_2)_x \in k[x, y]$.

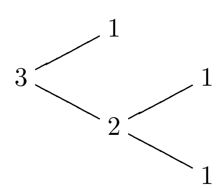
□

5.4 Problemas

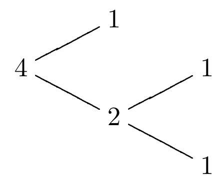
1. Desingularizar la curva $y^2 - x^7 = 0$. ¿Es esta curva birracional a la recta afín?

2. Calcular la multiplicidad de intersección de $y^2 - x^3 + y^4 = 0$ con $yx + x^3 + y^3 = 0$ en el origen.

3. Definir una curva plana que pase por el origen cuyo árbol de explosión en el origen sea



4. Definir una curva plana que pase por el origen cuyo árbol de explosión en el origen sea



5. Sea $m \text{ --- } \overset{r}{\cdots} \text{ --- } m \text{ --- } m'$, con $m' < m$, el árbol de explosión de una curva plana C en un punto p. Demostrar si C' es una curva plana no singular en p entonces $\mu_p(C \cap C') = sm$, con $s \leq r$, ó $\mu_p(C \cap C') = rm + m'$ y que existe una curva C', tal que $\mu_p(C \cap C') = rm + m'$.

6. Probar el Teorema de Pascal: Si un hexágono está inscrito en una cónica irreducible, entonces los lados opuestos se cortan en puntos alineados.

7. Probar el Teorema de Pappus: Sean R_1, R_2 dos rectas; $p_1, p_2, p_3 \in R_1$ y $q_1, q_2, q_3 \in R_2$ (ninguno de ellos se encuentran sobre $R_1 \cap R_2$). Sea R_{ij} la recta que une p_i y q_j. Probar que los puntos $p_{ij} = R_{ij} \cap R_{ji}$ $(i < j)$ están alineados.

8. Ley de grupo en las cúbicas. Sea C una cúbica plana no singular. Fijemos un punto $p_0 \in C$. Dados dos puntos $p, q \in C$, la recta que pasa estos dos puntos, corta a C en un tercer punto r. Definamos $\phi\colon C \times C \to C$, $(p, q) \mapsto r$. Probar que la aplicación $C \times C \to C$, $(p, q) \mapsto \phi(p_0, \phi(p, q))$ dota a C de estructura de grupo abeliano.

9. Sean C_3, C_3' dos cúbicas planas que se cortan en 9 puntos distintos, de manera que 6 de ellos están sobre una cónica. Probar que los tres restantes están alineados.

10. Demostrar que las tangentes a una cúbica irreducible plana en 3 puntos alineados cortan a la cúbica en otros 3 puntos alineados.

11. Demostrar que si un triángulo está inscrito en una cónica irreducible, entonces los puntos de corte de cada lado del triángulo con la tangente a la cónica en el vértice opuesto, están alineados.

12. Probar que una recta que pase por dos puntos de inflexión de una cúbica plana irreducible pasa por un tercer punto de inflexión.

13. Probar que si una cúbica pasa por ocho de los nueve puntos distintos de corte de otras dos cúbicas, entonces también pasa por el noveno.

14. Sea C_3 una cúbica plana y $x \in C_3$ un punto de inflexión. Probar que los puntos $y \in C_3$ para los que existe una cónica que que cumpla $\mu_x(C_3 \cap C_2) = \mu_y(C_3 \cap C_2) = 3$, son las terceras intersecciones de las rectas que unen los puntos de inflexión con x.

15. Teorema de Cayley-Bacharay: Sea C_{n+m-3} una curva plana de $n+m-3$ que pasa por $n \cdot m - 1$ de los puntos de intersección de dos curvas de grados n y m. Probar que C_{n+m-3} pasa por el punto restante.

16. Si una curva $C_{n+m-\gamma}$ de grado $n + m - \gamma$ $(\gamma > 3)$, pasa por $n \cdot m - \frac{(\gamma-1)(\gamma-2)}{2}$ de los $n \cdot m$ puntos distintos en los que se cortan dos curvas de grados n y m, entonces pasa también por los restantes puntos siempre que dichos puntos no estén en una curva de grado $\gamma - 3$.

17. Calcular la multiplicidad de intersección de las cúbicas proyectivas planas $y^2 - x^3 = 0$ con $y^2 - x^3 - 1 = 0$, en todos los puntos de intersección. Poner un ejemplo de dos cúbicas planas afines irreducibles, cuyos puntos de corte sean afines y estén alineados.

Índice de Materias