Álgebra Conmutativa

Pedro Sancho de Salas

Diciembre-2001

Índice General

Bibliografía:

1. M. Atiyah, I.G. Macdonald: *Introducción al Álgebra Conmutativa*, Ed. Reverté, Barcelona (1973).

2. W. Fulton: *Curvas Algebraicas*, Ed. Reverté, Barcelona (1971).

3. S. Lang: *Algebra*, Addison Wesley, (1971).

4. H. Matsumura: *Commutative Algebra*, W.A. Benjamin Co, New York (1970).

5. J.A. Navarro: *Álgebra Conmutativa Básica*, Manuales UNEX, n§ 19, (1996).

6. R. Hartshorne: *Algebraic Geometry*, GTM n§ 52, Springer Verlag (1977).

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.

Paradójicamente, nuestro punto de partida va a ser el anillo, y a partir del anillo definiremos el espacio. El mirar "moderno" del espacio es coordenándolo. 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.

De hecho, 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 éste 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 $p(x_1, x_2, x_3) \in I = (p_1(x_1, x_2, x_3), \ldots, p_r(x_1, x_2, x_3))$, 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

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

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 algebraica 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).

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 toda 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. Ésto 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. Estos dos procesos pueden ser entendidos geométricamente como los dos procesos de restricción a abiertos y restricción a cerrados.

1.2 Anillos. Ideales

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

Definición 1.2.1. Un anillo A es un conjunto con dos operaciones $A \times A \xrightarrow{+} A,\ (a, a') \mapsto a + a'$, $A \times A \xrightarrow{\cdot} A,\ (a, a') \mapsto a \cdot a'$[1], que denominamos suma y producto, tales que

1. A es un grupo abeliano con respecto a la suma (luego, 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 $a \in A$.

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 $\mathbb{C}[x_1, \ldots, x_n]$, los anillos de series formales $\mathbb{C}[[x_1, \ldots, x_n]]$, etc.

Definición 1.2.2. 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 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.

Definición 1.2.3. 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 toda $a, a' \in A$.
2. $f(aa') = f(a)f(a')$, para todo $a, a' \in A$.
3. $f(1) = 1$.

Ejemplo 1.2.4. 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 con las operaciones de B es anillo. La composición de morfismos de anillos es un morfismo de anillos.

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

Definición 1.2.5. Un subconjunto $I \subseteq A$ diremos que es un ideal de A si es un subgrupo para la suma y cumple que $a \cdot i \in I$, para todo $a \in A$ y todo $i \in I$.

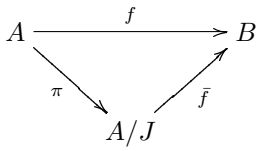
La intersección de ideales es un ideal. Dado un subconjunto $F \subseteq A$, denotaremos por (F) al ideal mínimo de A que contiene a F (que es la intersección de todos los ideales que contienen a F). Explicitamente $(F) = \{a \in A\colon a = \sum_{i=0}^{n} a_i f_i \text{ con } f_i \in F, a_i \in A \text{ y } n \in \mathbb{N} \text{ variables}\}$. Dado $a \in A$, también notaremos $(a) = aA$.

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 $\bar{a} \cdot \bar{a'} \underset{\text{def}}{=} \overline{a \cdot a'}$ 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, $\operatorname{Ker} f \underset{\text{def}}{=} \{a \in A\colon f(a) = 0\}$, 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



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

La antiimagen por un morfismo de anillos de un ideal es un ideal. Es inmediata la proposición siguiente.

Proposición 1.2.6. *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*

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

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

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

Definición 1.2.7. 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.

Proposición 1.2.8. *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. □

Definición 1.2.9. 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.

Proposición 1.2.10. *En todo anillo $A \neq 0$ existen ideales maximales.*

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

Ejercicio 1.2.11. En todo anillo $A \neq 0$ existen ideales primos minimales.

Corolario 1.2.12. *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

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

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

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

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.

Proposición 1.2.13. *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* 1.2.8.

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. □

Definición 1.2.14. 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 $\lambda \in k$.

Definición 1.2.15. 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.

Proposición 1.2.16. *Un ideal $\mathfrak{m}$ de $k[x_1, \ldots, x_n]$ es racional si y sólo si $\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$, $\alpha_i \in k$ para todo i.*

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

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

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

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

□

Así pues, existe una correspondencia biunívoca entre los ideales racionales de $k[x_1, \ldots, x_n]$ y los puntos $(\alpha_1, \ldots, \alpha_n)$ del espacio afín $\mathbb{A}_n(k)$. Es decir, si "pensamos" $k[x_1, \ldots, x_n]$ como las funciones algebraicas del espacio afín $\mathbb{A}_n(k)$, el modo de recuperar $\mathbb{A}_n(k)$ a partir de $k[x_1, \ldots, x_n]$ 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).

Ejercicio 1.2.17. Probar que los ideales racionales de $k[x_1, \ldots, x_n]/(p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n))$, se corresponden biyectivamente con los $(\alpha_1, \ldots, \alpha_n) \in \mathbb{A}_n(k)$ tales que $p_i(\alpha_1, \ldots, \alpha_n) = 0$, para todo i.

1.3 Espectro primo de un anillo

Definición 1.3.1. Se llama espectro primo de un anillo A al conjunto $\mathrm{Spec}\, A$ de sus ideales primos.

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

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

1. La función 0 se anula en todos los puntos de $\mathrm{Spec}\, A$.

2. Si dos funciones se anulan en un punto x, su suma también.

3. Si una función se anula en un punto x, sus múltiplos también.

4. Si un producto de funciones se anula en un punto x, algún factor se anula en x.

Definición 1.3.2. Sea A un anillo. Si $f \in A$, llamaremos *ceros* de la función f al subconjunto $(f)_0 \subset \operatorname{Spec} A$ formado por todos los puntos donde se anule f. Llamaremos ceros de un ideal $I \subseteq A$ al subconjunto de $\operatorname{Spec} A$ formado por los puntos donde se anulen todas las funciones de I y lo denotaremos $(I)_0$, es decir,

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

Ejercicio 1.3.3. 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 $p(\alpha, \beta) = 0$.

Proposición 1.3.4. *Se verifican las siguientes igualdades:*

1. $(0)_0 = \operatorname{Spec} A$ *y* $(A)_0 = \emptyset$.

2. $(\sum_{j \in J} I_j)_0 = \bigcap_{j \in J} (I_j)_0$.

3. $(\bigcap_{j=1}^{n} I_j)_0 = \bigcup_{j=1}^{n} (I_j)_0$.

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

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

□

Ejercicio 1.3.5. Demostrar que $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0$, donde denotamos por $I_1 \cdot I_2 = \{\sum_i a_i b_i \mid a_i \in I_1, b_i \in I_2\}$.

Definición 1.3.6. 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.

Ejercicio 1.3.7. Determinar los puntos y la topología de $\operatorname{Spec} \mathbb{Z}$.

Observemos que los cerrados de esta topología son intersecciones arbitrarias de ceros de funciones.

Por definición una base de abiertos de la topología de Zariski de $\operatorname{Spec} A$ está formada por los complementarios de los ceros de funciones, es decir, por los abiertos

$$U_f = \operatorname{Spec} A - (f)_0 = \{x \in \operatorname{Spec} A \colon f \text{ no se anula en } x\}$$

llamados abiertos básicos. Obsérvese que

$$U_{fg} = U_f \cap U_g$$

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 $\operatorname{Spec} A$.

Obviamente 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 $J \underset{\neq}{\subseteq} I$ tales que $C = (I)_0 = (J)_0$.

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

Proposición 1.3.8. *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 $(\mathfrak{p}_x)_0 = (I)_0 = \bar{x}$.

□

Definición 1.3.9. 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.

Proposición 1.3.10. *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 $g \in I$.

□

Ejercicio 1.3.11. Calcular las componentes irreducibles de $\operatorname{Spec} k[x,y]/(xy)$.

Ejemplo 1.3.12. 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 raices 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).

Ejemplo 1.3.13. 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 $U_{p_1}, \ldots, U_{p_n}$ recubren X. Por tanto, $f = f_{p_1}^2 + \cdots + f_{p_n}^2$ no se anula en ningún punto de X, luego es invertible y $f \in \mathfrak{m}$, contradicción.

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

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

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

Teorema 1.3.14. *El espectro de cualquier anillo es un espacio topológico compacto.*

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

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

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

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

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

□

1.4 Aplicación inducida en los espectros por un morfismo de anillos

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

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

Teorema 1.4.1. *La aplicación inducida en los espectros por cualquier morfismo de anillos es continua.*

Demostración. Consideremos los morfismos

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

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

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

y concluimos que j^* es continua.

□

Ejercicio 1.4.2. 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 1.3.13 y que todo morfismo $C(X) \to C(X)$ induce un morfismo entre los espectros).

Teorema 1.4.3. *Sea I un ideal de A. Consideremos los morfismos naturales*

$$\begin{array}{ccccc} A & \xrightarrow{\pi} & A/I & & a \mapsto \bar{a} \\ \operatorname{Spec} A & \xleftarrow{\pi^*} & \operatorname{Spec} A/I & & \end{array}$$

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

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

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

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

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

que es justamente el morfismo

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

Lo que demuestra la biyección buscada. Sabemos que π^* es continua, para ver que la biyección es un homeomoerfismo, 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.

□

Ejercicio 1.4.4. 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. 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).

Corolario 1.4.5. $\operatorname{Spec}(A \times B) = (\operatorname{Spec} A) \coprod (\operatorname{Spec} B)$.

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,

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

Explicitamente, 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.

□

Ejercicio 1.4.6. 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 $\operatorname{Spec} A \coprod \operatorname{Spec} B$".

1.5 Localización. Fórmula de la fibra

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

$$A_S = \{\frac{a}{s},\ a \in A \text{ y } s \in S\colon\ \frac{a}{s} = \frac{a'}{s'} \text{ si existe un } s'' \in S \text{ tal que } s''(as' - a's) = 0\}^2$$

.

Con la suma y producto ordinarios de fracciones A_S es un anillo.

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

Teorema 1.5.1. *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:*

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

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

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

Las asignaciones

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

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

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

están bien definidas y son inversas entre si, 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 $S = A - \mathfrak{p}_x$.

Corolario 1.5.2. *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. □

Ejercicio 1.5.3. Sea $C(\mathbb{R}^n)$ el anillo de funciones reales continuas sobre $\mathbb{R}^n$. Sea U un abierto de $\mathbb{R}^n$, $C(U)$ es 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: 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 $h = \frac{f}{s}$).

Corolario 1.5.4. *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 $\mathfrak{p}_x$. □

Definición 1.5.5. Los anillos con un único ideal maximal se les denomina anillos locales.

Observemos que el anillo de funciones que consideramos en U_f es A_f. Como es de desear, cuando nos pasamos a U_f, hacemos invertibles las funciones que no se anulan 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.

Definición 1.5.6. Dado un anillo A llamaremos radical de A al ideal formado por el conjunto de los elementos nilpotentes de A, es decir, si por denotamos $\operatorname{rad} A$ al radical de A entonces

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

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

Corolario 1.5.7. *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 anterior $\operatorname{Spec} A_f = \emptyset$. 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. □

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

Teorema 1.5.8 (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.

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

Las dos afirmaciones siguientes del teorema 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.

□

Ejemplo 1.5.9. 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).

Ejemplo 1.5.10. Calculemos $\operatorname{Spec}\mathbb{C}[x,y]/(q(x,y))$. Consideremos la descomposición en producto de polinomios irreducibles $q(x,y) = q_1(x,y)^{n_1}\cdots q_r(x,y)^{n_r}$, que no difieran en factores constantes. Tenemos que $\operatorname{Spec}\mathbb{C}[x,y]/(q(x,y)) = (q(x,y))_0 = \bigcup_{i=1}^{r}(q_i(x,y))_0$ que son:

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

1.6 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 $A \to A_S \xrightarrow{f_S} B$.

4. Probar que $(A_S)_{S'} = A_{S\cdot S'}$.
5. Probar que $k[x,y]/(xy-1) \simeq k[x]_{1,x,x^2,\ldots}$.
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. Calcular $\operatorname{Spec} \mathbb{Z}/6\mathbb{Z}$, $\operatorname{Spec}(\mathbb{C}[x,y]/(y^2-x^3))_x$.
10. Calcular $\operatorname{Spec} \mathbb{Z}[x]$, $\operatorname{Spec} \mathbb{Z}[\sqrt{5}]$.
11. Calcular $\operatorname{Spec} \mathbb{R}[x,y]$.
12. Si $\operatorname{Spec} A$ es la unión disjunta de dos abiertos U_1, U_2 probar que $U_1 = \operatorname{Spec} A_{U_1}$.
13. Sean $I, I' \subseteq A$ dos ideales. Probar que $(I)_0 = (I')_0$ si y sólo si $r(I) = r(I')$.
14. Probar que los elementos de los ideales primos minimales de un anillo son divisores de cero (Pista: localícese en los ideales primos minimales).
15. 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.
16. Probar que la intersección de dos rectas paralelas $(ax+by+c)_0$, $(ax+by+c')_0$ $(c \neq c')$ es vacía.
17. 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^*.
18. 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

Módulos

2.1 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, en esta breve justificación de la introducción de los espacios vectoriales, 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.

Los módulos aparecen también con frecuencia en Matemáticas. Ya veremos que los grupos abelianos y los espacios vectoriales con un endomorfismo lineal son ejemplos de módulos, y que su clasificación es la clasificación de la estructura de módulos.

Hablando sin precisión ni rigor, el estudio de los módulos equivale al estudio de los fibrados vectoriales $\pi\colon E \to X$, es decir, de los epimorfismos continuos, de fibras espacios vectoriales. El estudio de π será equivalente al estudio del $C(X)$-módulo de las secciones de π. La extensión del concepto de espacio vectorial (sobre un punto) a un espacio topológico es el concepto de fibrado vectorial, o el concepto de módulo. En cursos posteriores, se profundizará en lo que aquí apenas hemos esbozado.

Definición 2.1.1. 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 $A\times M \dot{\to} M$, $(a,m)\mapsto a\cdot m$, 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 $\phi\colon A\to \mathrm{End}(M)$, $\phi(a)=a\cdot$, es morfismo de anillos (donde $\mathrm{End}(M)$ son los endomorfismos de grupos del grupo conmutativo M). Recíprocamente, si M es un grupo conmutativo, cada morfismo de anillos $\phi\colon A\to\mathrm{End}(M)$ define una estructura de A-módulo en M tal que $a\cdot m \underset{\text{def}}{=} \phi(a)(m)$.

Ejemplo 2.1.2.

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

2. Si A es un cuerpo entonces los A-módulos son los A-espacios vectoriales.

3. Si G es un grupo abeliano, entonces es un $\mathbb{Z}$-módulo de modo natural: $n\cdot g = g+\overset{n}{\dots}+g$ si $n\in\mathbb{N}^+$, $n\cdot g = (-g)+\overset{n}{\dots}+(-g)$ si $-n\in\mathbb{N}^+$, y $0\cdot g = 0$. 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: $(\sum\lambda_i x^i)\cdot e \underset{\text{def}}{=} \sum\lambda_i T^i(e)$. Recíprocamente, dado un $k[x]$-módulo E, la aplicación $T\colon E\to E$ definida por $T(e)=x\cdot e$, es un endomorfismo de k-espacios vectoriales.

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

Definición 2.1.3. 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.

Definición 2.1.4. 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 $m\in M$.

Los elementos de un módulo M que por un morfismo de A-módulos $f\colon M \to M'$, van al cero, se les 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 $\operatorname{Ker} f = 0$. 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 morfismo y producto por elementos de A naturales:

$$(f+g)(m) \underset{\text{def}}{=} f(m)+g(m)$$
$$(af)(m) \underset{\text{def}}{=} a(f(m))$$

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

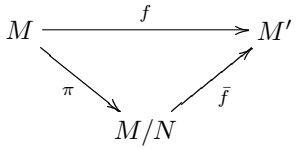
$$M/N = \{\bar{m},\ m \in M \text{ de modo que } \bar{m} = \bar{m'} \iff m - m' \in N\}$$

Ahora bien, el producto $a \cdot \bar{m} \underset{\text{def}}{=} \overline{a \cdot m}$ 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.

Ejercicio 2.1.5. 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 si).

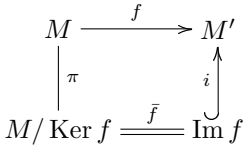
Dado un morfismo $i\colon N \to M$ inyectivo, si i tiene retracto (es decir, existe $r\colon M \to N$ de modo que $r \circ i = \mathrm{Id}$) entonces $M \simeq N \oplus M/N$. (Pista: Los morfismos $M \to N \oplus M/N$, $m \mapsto (r(m), \bar{m})$ y $N \oplus M/N \to M$, $(n, \bar{m}) \mapsto n + (m -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

Teorema 2.1.6. *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*



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

Teorema 2.1.7 (de isomorfía). *Sea $f\colon M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*



donde $\pi(m) = \bar{m}$, $\bar{f}(\bar{m}) = f(m)$ (que está bien definida) y $i(m') = m'$, es conmutativo, $\bar{f}$ es un isomorfismo, π es epiyectiva y 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 de tipo finito. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M si es un sistema generador y si $\sum_i a_i m_i = 0$ entonces $a_i = 0$ para todo i.

Denotaremos $M^{(I)} = \bigoplus_{i\in I} M_i$, siendo $M_i = M$. Se dice que un módulo es libre si es isomorfo a $A^{(I)}$. Si denotamos $1_j = (a_i) \in A^{(I)}$, 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.

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 $M/I \cdot M$ 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 $\bar{m}_1, \ldots, \bar{m}_r \in M/IM$ 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 $\bar{m}_1, \ldots, \bar{m}_r \in M/\mathfrak{m}M$ es un sistema A-generador de $M/\mathfrak{m}M$ si y sólo si es un sistema generador del $A/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}M$.

Lema 2.1.8 (de Nakayama). *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y M un módulo finito generado. Denotemos $\mathfrak{m}M = \{m \in M : m = \sum a_i m_i$, con $a_i \in \mathfrak{m}$ y $m_i \in M\}$. Se cumple que*

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

Como consecuencia se obtiene que $m_1, \ldots, m_n \in M$ es un sistema generador de M si sus clases $\bar{m}_1, \ldots, \bar{m}_n$ en $M/\mathfrak{m}M$ son un sistema generador.

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

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

2.2 Localización de módulos

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

$$M_S = \{\frac{m}{s},\ m \in M, s \in S \text{ de modo que}$$
$$\frac{m}{s} = \frac{m'}{s'} \text{ si existe un } s'' \in S \text{ tal que } s''(s'm - sm') = 0\}^1$$

Con las operaciones (bien definidas)

$$\frac{m}{s} + \frac{m'}{s'} \underset{\text{def}}{=} \frac{s'm + sm'}{ss'}$$
$$\frac{a}{s} \cdot \frac{m}{s'} \underset{\text{def}}{=} \frac{am}{ss'}$$

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

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

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

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

[1] El lector avisado se dará cuenta que hay que comprobar 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 $\frac{m}{s} = \frac{m''}{s''}$.

Proposición 2.2.1. *Dado un morfismo $f\colon M \to N$ de A-módulos y S un sistema multiplicativo de A entonces 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 $(\operatorname{Im} f)_S = \operatorname{Im} f_S$. □

Definición 2.2.2. 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 $\operatorname{Ker} \pi = \operatorname{Im} i$.

Dado un módulo M tenemos 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. Un ejemplo de este estudio se dará en el siguiente capítulo, con la introducción de los factores invariantes.

Proposición 2.2.3. *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. □

Ejercicio 2.2.4. 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. 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.

Definición 2.2.5. Sea M un A-módulo, llamaremos anulador de M al ideal

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

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 $\bar{a} \cdot m \underset{\text{def}}{=} am$).

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 $S = A - \mathfrak{p}_x$.

Definición 2.2.6. 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.,

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

Teorema 2.2.7. *El soporte de un A-módulo finito generado coincide con los ceros de su ideal anulador, i.e.,*

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

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

Demostración. Empecemos probando que si $M = \langle m_1, \ldots, m_r \rangle$ es un A-módulo finito generado entonces $M_S = 0$ si y sólo si existe un $f \in S$ de modo que $fM = 0$: Si $M_S = 0$ entonces $\frac{m_i}{1} = 0$ para todo i, luego existen $f_i \in S$ de modo que $f_i m_i = 0$. Por tanto, $f = f_1 \cdots f_r \in S$ cumple que $fM = 0$. Recíprocamente, si existe $f \in S$ de modo que $fM = 0$, 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 $M = 0$.

□

Proposición 2.2.8. *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.

□

Teorema 2.2.9. *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 2.2.3. La implicación $2 \Rightarrow 3$ es evidente.

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

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

Si U es un abierto de $\operatorname{Spec} A$ denotaremos A_U por la localización de A por el sistema multiplicativo de las funciones que no se anulan en ningún punto de U.

Proposición 2.2.10. *Si $\operatorname{Spec} A$ es la unión disjunta de dos abiertos U_1, U_2 entonces $A = A_{U_1} \times A_{U_2}$.*

Demostración. Observemos que $\operatorname{Spec} A_{U_1} = U_1$ (igualmente $\operatorname{Spec} A_{U_2} = U_2$). En efecto, $U_1 \subseteq \operatorname{Spec} A_{U_1}$, porque las funciones del sistema multiplicativo por las que localizamos no se anulan en ningún punto de U_1. Por otra parte, como U_1, U_2 son cerrados, si denotamos I_i al ideal de funciones que se anulan en U_i tenemos que $(I_1)_0 \cap (I_2)_0 = \emptyset$, por tanto $(I_1 + I_2)_0 = \emptyset$ y $I_1 + I_2 = A$. Así pues, existen $f_i \in I_i$, tales que $f_1 + f_2 = 1$. En conclusión, $f_2 = 1 - f_1$ es una función que se anula en todo los puntos de U_2 y no se anula en ningún punto de U_1, por tanto $\operatorname{Spec} A_{U_1} \subseteq U_1$ y $\operatorname{Spec} A_{U_1} = U_1$.

Consideremos el morfismo natural

$$A \to A_{U_1} \times A_{U_2}, \quad a \mapsto (\frac{a}{1}, \frac{a}{1})$$

Vamos a probar que este morfismo es isomorfismo. Por el teorema anterior, basta verlo localmente. Dado $x \in U_1$, tenemos que $(A_{U_1})_x = (A_x)_{U_1} = A_x$ porque el sistema multiplicativo de las funciones que no se anulan en U_1, está incluido en el sistema multiplicativo de las funciones que no se anulan en x. Por otra parte, $\operatorname{Spec}(A_{U_2})_x = \emptyset$, porque $U_2 \cap \{y \in \operatorname{Spec} A \colon \mathfrak{p}_y \subseteq \mathfrak{p}_x, i.e., x \in \bar{y}\} = \emptyset$, luego $(A_{U_2})_x = 0$. En conclusión, $A_x = (A_{U_1} \times A_{U_2})_x$ si $x \in U_1$, e igualmente si $x \in U_2$. Hemos terminado. □

Corolario 2.2.11. *Si* $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$*, donde* $x_1, \ldots, x_n$ *son puntos cerrados, entonces*

$$A = A_{x_1} \times \cdots \times A_{x_n}$$

2.3 Longitud de un módulo

El concepto de longitud de un módulo se corresponde con el concepto de dimensión en espacios vectoriales. Usualmente, se define la dimensión de un espacio vectorial como el número de vectores de sus bases. En los A-módulos pueden no existir bases, por tanto, no podemos dar esta definición. Por otra parte, tampoco es ésta la definición más natural o intuitiva. El concepto de base es más elaborado, si bien es muy práctico en espacios vectoriales. Si intuimos que $\mathbb{R}^3$ es de dimensión 3 es porque observamos la cadena de inclusiones irrefinable punto, recta, plano, espacio. En teoría de módulos, seguiremos este otro punto de vista.

Definición 2.3.1. Diremos que un A-módulo $M \neq 0$ es simple cuando sus únicos submódulos son los triviales: 0 y M.

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

Definición 2.3.2. Diremos que una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ es una serie de composición si los cocientes sucesivos M_i/M_{i-1} son A-módulos simples. Diremos que la longitud de esta serie de composición es n.

Como los submódulos de M_i/M_{i-1} se corresponden biyectivamente con los submódulos de M_i que contienen a M_{i-1}, el que M_i/M_{i-1} sea simple equivale a que no existe una cadena $M_{i-1} \underset{\neq}{\subset} N \underset{\neq}{\subset} M_i$. Por tanto, que una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ sea serie de composición equivale a decir que no podemos añadirle más "eslabones".

Definición 2.3.3. Llamaremos longitud de M a la mínima longitud de todas sus series de composición. Si no existe ninguna serie de composición diremos que la longitud de M es infinita. Denotaremos a la longitud de un módulo M por $l(M)$.

Sobre espacios vectoriales el concepto de longitud coincide con el de dimensión.

Proposición 2.3.4. *Todas las series de composición de un módulo tienen la misma longitud.*

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

Dado un submódulo propio $N \subset M$ se cumple que $l(N) < l(M)$: Sea $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ una serie de composición de longitud mínima de M. Si en $0 = M_0 \cap N \subseteq M_1 \cap N \subseteq \cdots \subset M_n \cap N = N$ quitamos los términos repetidos obtenemos una serie de composición en N, porque $M_i \cap N/M_{i-1} \cap N \hookrightarrow M_i/M_{i-1}$, luego $M_i \cap N/M_{i-1} \cap N = M_i/M_{i-1}$ pues M_i/M_{i-1} es simple. Por tanto, $l(N) \leq l(M)$. Si $l(N) = l(M)$ entonces $M_i \cap N/M_{i-1} \cap N \neq 0$ para todo i. Entonces, $M_1 \cap N$ contiene estrictamente a $M_0 \cap N = 0$ y está incluido en M_1, luego $M_1 \cap N = M_1$. Sigamos, $M_2 \cap N$ contiene estrictamente a $M_1 \cap N = M_1$ y está incluido en M_2 luego $M_2 \cap N = M_2$ Recurrentemente, $N = M_n \cap N = M_n = M$, lo que es contradictorio.

Así pues, dada una serie de composición $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_m = M$, tenemos que $l(M) > l(M'_{m-1}) > \cdots > l(M'_1)$, luego $l(M) \geq m$. Como $m \geq n = l(M)$, tenemos que $m = n$.

□

Observemos que hemos demostrado que si un módulo es de longitud finita entonces todo submódulo suyo es de longitud finita. Es fácil probar que si un módulo es de longitud finita entonces es finito generado, y por tanto, también todo submódulo, que es de longitud finita, será finito generado.

Si un módulo es de longitud finita todo cociente suyo también lo es, pues toda serie de composición define por paso al cociente una serie de composición (eliminando las igualdades que aparezcan en la serie).

Proposición 2.3.5. *La longitud es una función aditiva, es decir, dada una sucesión exacta* $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ *se cumple que* $l(M) = l(M') + l(M'')$.

Demostración. Si $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_{n'} = M'$ y $0 = M''_0 \subset M''_1 \subset \cdots \subset M''_{n''} = M''$ son series de composición de M' y M'' entonces

$$0 = i(M'_0) \subset i(M'_1) \subset \cdots \subset i(M'_{n'}) = i(M') = \pi^{-1}(M''_0) \subset \pi^{-1}(M''_1) \subset \cdots \subset \pi^{-1}(M''_{n''}) = M$$

es una serie de composición de M, luego $l(M) = n' + n'' = l(M') + l(M'')$. □

En particular, si consideramos la sucesión exacta

$$\begin{array}{ccccccccc} 0 & \to & M' & \to & M' \oplus M'' & \to & M'' & \to & 0 \\ & & m' & \mapsto & (m', 0) & & & & \\ & & & & (m', m'') & \mapsto & m'' & & \end{array}$$

tenemos que $l(M' \oplus M'') = l(M') + l(M'')$.

La sucesión de morfismos de módulos

$$0 \to M_0 \to \cdots \to M_{s-1} \xrightarrow{f_s} M_s \xrightarrow{f_{s+1}} M_{s+1} \to \cdots \to M_n \to 0 \qquad (*)$$

es exacta si y sólo si son exactas las sucesiones $0 \to \operatorname{Im} f_s \to M_s \xrightarrow{f_{s+1}} \operatorname{Im} f_{s+1} \to 0$. Así, si la sucesión $*$ es exacta, tendremos que $l(\operatorname{Im} f_s) - l(M_s) + l(\operatorname{Im} f_{s+1}) = 0$ y haciendo el sumatorio para todo s tenemos

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

Proposición 2.3.6. *Si M es de longitud finita, entonces* $\mathrm{Sop}(M)$ *es un número finito de puntos cerrados.*

Demostración. Recordemos que los módulos simples son isomorfos a $A/\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal. Si $\mathfrak{m}_x$ es un ideal maximal y $\mathfrak{p}_{x'}$ es un ideal primo distinto de $\mathfrak{m}_x$ entonces $(A/\mathfrak{m}_x)_{x'} = 0$, pues $\mathrm{Sop}(A/\mathfrak{m}_x) = (\mathfrak{m}_x)_0 = x$ por 2.2.7. Ahora ya, dada una serie de composición

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

tenemos que $M_i/M_{i-1} \simeq A/\mathfrak{m}_{x_i}$, siendo $\mathfrak{m}_{x_i}$ ideales maximales. Por tanto, $(M_i/M_{i-1})_x \simeq (A/\mathfrak{m}_{x_i})_x = 0$, para todo punto $x \in \mathrm{Spec}\, A$ distinto de los x_i. Luego $M_x = (M_n)_x = \cdots = (M_0)_x = 0$, para todo punto $x \in \mathrm{Spec}\, A$ distinto de los x_i. En conclusión, el soporte de M es subconjunto de $\{x_i\}$ y hemos terminado.

□

2.4 Problemas

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

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

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

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

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

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

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

4. Sea $f \colon M \to M'$ un morfismo de A-módulos. Sean N_1, N_2 dos submódulos de M probar que $f(N_1 + N_2) = f(N_1) + f(N_2)$ (denotamos por $f(N) = \{f(n) \in M'$, con $n \in N\}$). Sea I un ideal, probar que $f(I \cdot N_1) = I \cdot f(I_1)$.

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

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

7. Calcular los siguientes $\mathbb{Z}$-módulos: $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z})$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Q})$ y $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z})$.

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

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

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

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

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

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

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

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

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

17. Sea M un A-módulo y N un submódulos de M. Probar que si N y M/N son A-módulos finito generados entonces M es finito generado.

18. Sea $C(\mathbb{R})$ el anillo de todas las funciones reales continuas de variable real. Demostrar que el conjunto de las funciones reales continuas de variable real que se anulan en algún entorno del cero forman un ideal de $C(\mathbb{R})$, que no es finito generado.

19. Probar que todo $\mathbb{Z}$-submódulo finito generado de $\mathbb{Q}$ no nulo, es libre generado por un elemento. Probar que $\mathbb{Q} \not\simeq \mathbb{Z}$.

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

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

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

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

23. Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta de A módulos. Se dice que la sucesión exacta rompe si existe un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \| \mathrm{Id} & & \| \phi & & \| \mathrm{Id} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M' \oplus M'' & \xrightarrow{\pi} & M'' & \longrightarrow & 0 \end{array}$$

    donde ϕ es un isomorfismo, $i(m') = (m', 0)$ y $\pi(m', m'') = m''$.

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

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

25. Sea $f\colon A \to B$ un morfismo de anillos. Sea $S \subset A$ un sistema multiplicativo. Sabemos que B es de modo natural un A-módulo, por tanto, podemos definir B_S. Por otra parte, $f(S) \subset B$ es un sistema multiplicativo. Demostrar que $B_S = B_{f(S)}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Capítulo 3

Módulos sobre dominios de ideales principales

3.1 Dominios de ideales principales

Definición 3.1.1. Diremos que un ideal $\mathfrak{p}$ es principal si está generado, como A-módulo, por un sólo elemento, i.e., $\mathfrak{p} = aA$.

Diremos que un anillo es un dominio de ideales principales si es un anillo íntegro cuyos ideales son principales.

Ejemplo 3.1.2. Los anillos euclídeos, en particular $\mathbb{Z}$, $k[x]$, son dominios de ideales principales. La localización de un dominio de ideales principales es un dominio de ideales principales.

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

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

Si A es un dominio de ideales principales, los elementos de A, salvo productos por invertibles, se corresponden con los ideales de A. En éstos anillos es válida gran parte de la teoría elemental de la divisibilidad de números enteros. En efecto, si $a, b \in A$, entonces $aA + bA = dA$, siendo el máximo común divisor: Si c divide á a y b entonces divide á d y obviamente d divide á a y b. Igualmente, el mínimo común múltiplo de a y b es el generador del ideal $aA \cap bA$. Por tanto, el máximo común divisor y el mínimo común múltiplo de dos elementos de un dominio de ideales principales A siempre existen y estan bien definidos salvo factores invertibles. Además,

Proposición 3.1.3 (Identidad de Bézout). *Sea d el máximo común divisor de a y b. Existen elementos $\alpha, \beta \in A$ tales que*

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

Definición 3.1.4. Un elemento propio (no nulo ni invertible) se dice que es irreducible si no descompone en producto de dos elementos propios. Se dice que dos elementos propios son primos entre sí si carecen de divisores propios comunes.

Lema 3.1.5 (de Euclides). *Si un elemento irreducible divide a un producto divide algún factor.*

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

Corolario 3.1.6. *Sea p un elemento no nulo de un dominio de ideales principales A. Las siguientes condiciones son equivalentes:*

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

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

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

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

□

Lema 3.1.7. *Toda cadena creciente de ideales de A estabiliza.*

Demostración. Dada una cadena de ideales $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots$, consideremos el generador c del ideal $\bigcup_i \mathfrak{p}_i$. Se cumple que $c \in \mathfrak{p}_n$, para algún n. Las inclusiones

$$\mathfrak{p}_n \subseteq \mathfrak{p}_{n+j} \subseteq \bigcup_i \mathfrak{p}_i = cA \subseteq \mathfrak{p}_n$$

prueban que $\mathfrak{p}_n = \mathfrak{p}_{n+j}$, para todo $j \geq 0$. □

Teorema 3.1.8 (de descomposición en factores irreducibles). *Todo elemento propio $a \in A$ descompone en producto de factores irreducibles $a = p_1 \cdots p_n$. Además la descomposición es única salvo orden y factores invertibles.*

Demostración. Empecemos probando que a todo elemento $a \in A$ lo divide algún elemento irreducible: Si a no es irreducible entonces $a = a_1 \cdot b_1$, a_1, b_1 elementos propios. Si a_1 no es irreducible, entonces $a_1 = a_2 \cdot b_2$, con a_2, b_2 elementos propios. Así sucesivamente, vamos obteniendo una cadena $(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \ldots$ que ha de ser finita por el lema anterior y terminará cuando a_n sea irreducible.

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

Veamos ahora la unicidad. Sean $a = p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones en factores irreducibles. Por el Lema de Euclides, q_1 divide algún factor p_i, luego coincide con él (salvo un factor invertible). Pongamos $p_1 = q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$ (salvo invertibles). Razonando con q_2 como hemos hecho antes con q_1 llegamos a que q_2 coincide con algún p_i. Reiterando el argumento, obtendremos que las dos descomposiciones son iguales (salvo orden y factores invertibles). □

3.2 Teoremas de descomposición

El objetivo de esta sección, es clasificar y determinar la estructura de los A-módulos finito generados sobre un dominio de ideales principales. En particular, obtendremos la clasificación de los grupos abelianos y la clasificación de los endomorfismos de un espacio vectorial de dimensión finita, como veremos en las siguientes secciones.

Definición 3.2.1. Sea A un anillo íntegro y M un A-módulo. Denotemos $\Sigma = A_{A-\{0\}}$ y $M_\Sigma = M_{A-\{0\}}$. Llamaremos rango de M al número $\dim_\Sigma M_\Sigma$.

Observemos que si $M = A \oplus \overset{n}{\ldots} \oplus A$ entonces el rango de M es n.

Definición 3.2.2. Sea A un anillo íntegro y M un A-módulo. Llamaremos torsión de M, que denotaremos $T(M)$, a

$$T(M) = \{m \in M : \text{existe } a \in A \text{ no nulo tal que } am = 0\}$$

Es fácil comprobar que $T(M)$ coincide con el núcleo del morfismo de localización $M \to M_{A-\{0\}} = M_\Sigma$, $m \mapsto \frac{m}{1}$.

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

Ejemplo 3.2.3. Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})$.

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

Proposición 3.2.4. *Sea A un anillo íntegro. Si M es un A-módulo finito generado libre de torsión entonces es un submódulo de un A-módulo libre del mismo rango.*

Demostración. Tenemos que $M = \langle m_1, \ldots, m_n \rangle$ y el morfismo de localización $M \hookrightarrow M_\Sigma$ es inyectivo. Evidentemente $\frac{m_1}{1}, \ldots, \frac{m_n}{1}$ es un sistema generador del Σ-espacio vectorial M_Σ. Reordenado, podemos suponer que $\frac{m_1}{1}, \ldots, \frac{m_r}{1}$ es una base del Σ-espacio vectorial M_Σ, $(r \geq n)$. Por tanto, para cada m_j tendremos $\frac{m_j}{1} = \sum_{s=1}^{r} \frac{a_{js}}{b_{js}} \frac{m_s}{1}$. Denotemos $b = \prod_{i,j} b_{ij}$. Con las notaciones obvias, tendremos el siguiente diagrama conmutativo de morfismos inyectivos

$$\begin{array}{ccc} M & \hookrightarrow & M_\Sigma \\ & \searrow & \uparrow \\ & & A\frac{m_1}{b} \oplus \cdots \oplus A\frac{m_r}{b} \end{array}$$

□

Proposición 3.2.5. *Sea A un dominio de ideales principales. Si M es un A-módulo finito generado libre de torsión entonces es un A-módulo libre.*

Demostración. Basta probar que los submódulos de un A-módulo libre son libres, por 3.2.4. Procederemos por inducción sobre el rango del módulo libre, que denotaremos L.

Si el rango de L es cero es obvio. Si el rango de L es uno entonces $L \simeq A$. Por tanto, todo submódulo M de L es isomorfo a un ideal de A, luego $M \simeq aA$. Si $a \neq 0$ entonces $A \simeq aA$, $b \mapsto ab$, luego M es libre de rango 1. Si $a = 0$ entonces $M = 0$.

Supongamos que el rango de L es $n > 1$. Como $L \simeq A^n$ es fácil definir una sucesión

$$0 \to L' \to L \to L'' \to 0$$

con L' libre de rango 1 y L'' libre de rango $n-1$. Dado $M \subseteq L$ consideremos el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L' & \longrightarrow & L & \xrightarrow{\pi} & L'' & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & L' \cap M & \longrightarrow & M & \longrightarrow & \pi(M) & \longrightarrow & 0 \end{array}$$

de filas exactas. Por inducción $L' \cap M$ y $\pi(M)$ son libres de rango finito. Por tanto, como $\pi(M)$ es libre, el epimorfismo $M \to \pi(M)$ tiene sección y por el ejercicio 2.1.5 $M = L' \cap M \oplus \pi(M)$. En conclusión, M es libre. □

Teorema 3.2.6 (Primer teorema de descomposición). *Sea A un dominio de ideales principales y M un A-módulo finito generado. Se cumple*

$$M \simeq T(M) \oplus (M/T(M))$$

donde $T(M)$ es un módulo finito de torsión y $M/T(M)$ es un módulo finito libre. Se cumple además que si $M \simeq M' \oplus L$, siendo M' un A-módulo de torsión y L libre, entonces $M' \simeq T(M)$ y $L \simeq (M/T(M))$.

Demostración. $M/T(M)$ es un módulo finito libre de torsión: si $\bar{m} \in T(M/T(M))$ entonces existe $a \in A$ no nulo tal que $a\bar{m} = 0$, luego $am \in T(M)$ y existe $b \in A$ no nulo tal que $bam = 0$, por tanto $m \in T(M)$ y $\bar{m} = 0$. Por la proposición anterior $M/T(M)$ es un módulo libre. El epimorfismo de paso al cociente $M \to M/T(M)$ tiene sección, porque $M/T(M)$ es libre, luego $M \simeq T(M) \oplus (M/T(M))$.

Si $M \simeq M' \oplus L$, entonces $T(M) \simeq T(M' \oplus L) = T(M') \oplus T(L) = M'$. Luego $(M/T(M)) \simeq (M' \oplus L)/M' = L$. Hemos concluido.

□

Observemos que $M_{A-\{0\}} = (M/T(M))_{A-\{0\}}$. Por tanto, el rango de $M/T(M)$ es el de M. Así pues, en el teorema anterior $M/T(M)$ es un módulo libre de rango el de M.

Hemos reducido el problema de la clasificación de los módulos finitos sobre dominios de ideales principales, a la clasificación de los módulos finitos de torsión. Si M es un módulo finito generado de torsión, entonces $\mathrm{Anul}(M) \neq 0$. En efecto, si $M = \langle m_1, \ldots, m_n \rangle$, y $a_i \in A - \{0\}$ cumplen que $a_i m_i = 0$, entonces $0 \neq a_1 \cdots a_n \in \mathrm{Anul}(M)$.

Lema 3.2.7. *Sea M un A-módulo anulado por pq, siendo p y q primos entre sí. Entonces M descompone en suma directa de un módulo anulado por p y otro submódulo anulado por q, en concreto*

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

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

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

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

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

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

□

Teorema 3.2.8 (Segundo teorema de descomposición). *Sea M un A-módulo de ideal anulador aA y $a = p_1^{n_1} \cdots p_s^{n_s}$ la descomposición de a en factores irreducibles. Entonces M descompone de modo único en suma directa de submódulos M_i de anuladores respectivos $p_i^{n_i}A$, en concreto*

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

Demostración. Por el lema anterior,

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

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

□

Si M es un A-módulo anulado por $\mathfrak{m}_x^n$ entonces M es un $A/\mathfrak{m}_x^n$-módulo. Si $a \notin \mathfrak{m}_x$ entonces $\bar{a}$ es invertible en $A/\mathfrak{m}_x^n$, y por tanto, el morfismo $M \xrightarrow{a\cdot=\bar{a}\cdot} M$ es un isomorfismo. En consecuencia, $M = M_x$ y es un A_x-módulo. En particular, $(A/\mathfrak{m}_x^n) = (A/\mathfrak{m}_x^n)_x = A_x/(\mathfrak{m}_x^n A_x)$. Por otra parte, si $x \neq y \in \operatorname{Spec} A$, entonces $M_y = 0$. Por tanto, si M es un A-módulo finito generado de torsión, entonces

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

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

Proposición 3.2.9. *Sea A un dominio de ideales principales local, de ideal maximal $\mathfrak{m} = (p)$. Sea $\phi\colon A^m \to A^n$ un morfismo de A-módulos. Se cumple que existen bases $\{e_1, \ldots, e_m\}$, $\{e_1', \ldots, e_n'\}$ en A^m y A^n, de modo que $\phi(e_i) = \lambda_i e_i'$.*

Demostración. Sea (a_{ij}) la matriz asociada a ϕ, en las bases estándar $\{u_1, \ldots, u_m\}$, $\{u_1', \ldots, u_n'\}$ de A^m y A^n. Si en vez de $\{u_1, \ldots, u_m\}$, consideramos la base que se obtiene permutando dos vectores de $\{u_1, \ldots, u_m\}$, la matriz de ϕ en las nuevas bases, se obtiene permutando las correspondientes columnas de la matriz (a_{ij}). Igualmente, si permutamos dos vectores de $\{u_1', \ldots, u_n'\}$, la matriz de ϕ se obtiene permutando las correspondientes filas de (a_{ij}). Si en vez de $\{u_1, \ldots, u_m\}$, consideramos la base $\{u_1, \ldots, u_i \overset{i}{-} a_j u_j, \ldots, u_m\}$, la matriz de ϕ en las nuevas bases, se obtiene cambiando la columna i, C_i de la matriz (a_{ij}) por la columna $C_i - a_j C_j$. Si en vez de $\{u_1', \ldots, u_m'\}$, consideramos la base $\{u_1', \ldots, u_i' \overset{i}{-} a_j u_j', \ldots, u_n'\}$, la matriz de ϕ en las nuevas bases, se obtiene cambiando la fila j, F_j de la matriz (a_{ij}) por la fila $F_j + a_j F_i$.

Este tipo de transformaciones de la matriz (a_{ij}) (o equivalentemente de las bases $\{u_i\}, \{u_i'\}$) las denominaremos transformaciones elementales. Vamos a probar que mediante transformaciones elementales la matriz de ϕ es "diagonal", es decir, $\phi(e_i) = \lambda_i e_i'$, para todo i.

Dado $a \in A$, tendremos que $a = p^i \cdot b$, con b no divisible por p, es decir, $b \notin \mathfrak{m} = (p)$, luego b invertible. Por tanto, $(a) = (p^i)$. Sea p^i el máximo común divisor de todos los a_{ij}. Existe un a_{rs}, tal que $(a_{rs}) = (p^i)$. Por tanto, a_{rs} divide a todos los coeficientes a_{ij}. Permutando filas y columnas podemos suponer que $r = 1$ y $s = 1$. Transformando las columnas C_i por $C_i - \frac{a_{1i}}{a_{11}} C_1$ para $i > 1$, y posteriormente las filas F_i por $F_i - \frac{a_{i1}}{a_{11}} F_1$, obtendremos la matriz

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}$$

Procediendo del mismo modo reiteradamente, con la matriz (b_{ij}), "diagonalizaremos" ϕ.

□

Teorema 3.2.10 (Tercer teorema de descomposición). *Sea A un dominio de ideales principales y M un A-módulo finito generado, de ideal anulador $p^n A$, siendo $p \in A$ irreducible. Se cumple que*

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

con $n_i \leq n$, determinados unívocamente por M.

Demostración. Podemos suponer que A es local, de ideal maximal $\mathfrak{m} = (p)$. Consideremos un epimorfismo $\pi\colon A^n \to M$. Por ser $\operatorname{Ker}\pi$ submódulo de un módulo libre, es libre, digamos $A^m = \operatorname{Ker}\pi$. Existe, pues, una sucesión exacta

$$A^m \xrightarrow{\phi} A^n \to M \to 0$$

y $M = \operatorname{Coker}\phi$. Por la proposición anterior, existen bases $\{e_1, \dots, e_m\}$, $\{e'_1, \dots, e'_n\}$ de A^m y A^n, de modo que $\phi(e_i) = \lambda_i e'_i$, para todo i. Luego,

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

y fácilmente concluimos.

Veamos la unicidad de los n_i. Reordenando tenemos

$$M = (A/p^n A)^{m_n} \oplus (A/p^{n-1}A)^{m_{n-1}} \oplus \cdots \oplus (A/pA)^{m_1}$$

con $m_i \geq 0$. Tenemos que ver que M determina los m_i.

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

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

Teorema 3.2.11 (de clasificación). *Dado un A-módulo M finito generado, existe un isomorfismo de A-módulos*

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

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

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

Definición 3.2.12. A las potencias $p_i^{n_{i,j}}$ del teorema de clasificación se les denomina divisores elementales de M.

Corolario 3.2.13. *Dos módulos finito generados son isomorfos si y sólo si tienen el mismo rango y los mismos divisores elementales.*

Ejercicio 3.2.14. Dos módulos finito generados sobre un dominio de ideales principales son isomorfos si y sólo si son localemente isomorfos.

Ejercicio 3.2.15. Probar que en el caso de que $r = 0$ entonces $\mathrm{Anul}(M) = m.c.m.\{p_i^{n_{i,j}}\}_{i,j} A$.

Demos, por razones prácticas, la siguiente proposición.

Proposición 3.2.16. *Sea M un A-módulo finito generado de torsión. Sean $m_{ijk} \in M$ tales que las clases de $\{m_{ijk}\}_k$ sean una base del A/p_iA-espacio vectorial $\operatorname{Ker} p_i^j / \operatorname{Ker} p_i^{j-1} + p_i \cdot \operatorname{Ker} p_i^{j+1}$. Se cumple que*

$$M = \bigoplus_{i,j,k} A/p_i^j A \cdot m_{ijk}$$

Demostración. El morfismo natural $\phi\colon \bigoplus_{i,j,k} (A/p_i^j A) \cdot m_{ijk} \to M$, $\phi(m_{ijk}) = m_{ijk}$, es un epimorfismo: Basta verlo localmente, por lo que podemos suponer que $M = \operatorname{Ker} p_i^n$. Por Nakayama, basta ver que $\bar{\phi}\colon \bigoplus_{i,j,k} (A/p_i^j A) \cdot m_{ijk} \to M/p_i \cdot M$ es epiyectivo. Tenemos que $\overline{\langle m_{i1k}\rangle_k} = \overline{\operatorname{Ker} p_i}$, luego $\overline{\langle m_{i1k}\rangle_k} + \overline{\langle m_{i2k}\rangle_k} = \overline{\operatorname{Ker} p_i^2}$, etc.

Por último, M y $\bigoplus_{i,j,k} A/p_i^j A \cdot m_{ijk}$ tienen los mismos divisores elementales (repásese la demostración de la unicidad de los divisores elementales), luego son isomorfos y tienen la misma longitud. Por tanto, el epimorfismo ϕ es un isomorfismo.

□

3.3 Clasificación de los grupos abelianos finito generados

Dado un grupo abeliano G tiene de modo natural estructura de $\mathbb{Z}$-módulo: La suma considerada es la suma del grupo abeliano y el producto por escalares se define

$$n \cdot g = \begin{cases} \overbrace{g + \stackrel{n}{\ldots} + g}^{} & \text{si } n \in \mathbb{N}^+ \\ \overbrace{(-g) + \stackrel{-n}{\ldots} + (-g)}^{} & \text{si } n \notin \mathbb{N} \\ 0 & \text{si } n = 0 \end{cases}$$

Recíprocamente, todo $\mathbb{Z}$-módulo es en particular un grupo abeliano. Así pues, hablar de grupos abelianos o de $\mathbb{Z}$-módulos es sólo una diferencia en la terminología usada.

Así por ejemplo, un grupo abeliano es finito generado si y sólo si es finito generado como $\mathbb{Z}$-módulo.

Teorema 3.3.1 (de clasificación). *Sea G un grupo abeliano finito generado. Existe un isomorfismo de grupos*

$$G \simeq (\mathbb{Z} \oplus \stackrel{r}{\ldots} \oplus \mathbb{Z}) \oplus (\bigoplus_{i,j} \mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z})$$

con $p_i \in \mathbb{Z}$ primos, y r, $n_{i,j}$ y p_i determinados.

En particular, todo grupo abeliano finito generado es suma directa de grupos cíclicos.

En el caso particular de que G sea un grupo abeliano finito tendremos que

$$G \simeq \underset{i,j}{\oplus} \mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}$$

Corolario 3.3.2. *Dos grupos abelianos finito generados son isomorfos si y sólo si tienen el mismo rango y los mismos divisores elementales.*

Ejercicio 3.3.3. Probar que $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

3.4 Clasificación de los endomorfismos de un espacio vectorial

Un endomorfismo $T\colon E \to E$ de un k-espacio vectorial E, induce una estructura de $k[x]$-módulos en E del siguiente modo

$$p(x) \cdot e = p(T)(e)$$

en particular $x \cdot e = T(e)$. Recíprocamente, si E es un $k[x]$-módulo, tenemos el endomorfismo $E \xrightarrow{x\cdot} E$, $e \mapsto x \cdot e$. Cuando pensemos E con la estructura de $k[x]$-módulo inducida por el endomorfismo T, lo escribiremos E_T.

Definición 3.4.1. Dos endomorfismos T, T' de E se dicen que son equivalentes si existe un automorfismo lineal τ de E tal que $T' = \tau \circ T \circ \tau^{-1}$. Esta igualdad significa la conmutatividad del cuadrado

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

Proposición 3.4.2. *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y sólo si existen una base para T y otra base para T' en las que que T y T' tienen la misma matriz.*

Demostración. El endomorfismo τ es precisamente el que manda una base a la otra. □

Proposición 3.4.3. *Dos endomorfismos T, T' de un espacio vectorial son equivalentes si y sólo si inducen estructuras de $k[x]$-módulos isomorfas.*

Demostración. Si T, T' son equivalentes existe un automorfismo lineal τ tal que $\tau \circ T = T' \circ \tau$. Veamos que $\tau\colon E_T \to E_{T'}$ es un isomorfismo de $k[x]$-módulos:

$$\tau(x \cdot e) = \tau(T(e)) = T'(\tau(e)) = x \cdot \tau(e)$$

Reiterativamente, probamos que $\tau(x^i \cdot e) = \tau(T^i(e)) = T'^i(\tau(e)) = x^i \cdot \tau(e)$ y por linealidad que $\tau(p(x) \cdot e) = p(x) \cdot \tau(e)$.

Para el recíproco se razona de modo similar. □

Si T es un endomorfismo de un espacio vectorial de dimensión finita, entonces es un $k[x]$-módulo finito, y el rango de E_T ha de ser cero, porque la dimensión de $k[x]$ sobre k es infinita.

Teorema 3.4.4. *Dos endomorfismos de un espacio vectorial de dimensión finita son equivalentes si y sólo si poseen los mismos divisores elementales.*

3.4.1 Matrices de Jordan

1. Caso de un cuerpo k algebraicamente cerrado

Lema 3.4.5. *Sea $p(x) \in k[x]$ un polinomio de grado n, entonces $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ es una base de $k[x]/(p(x))$.*

Demostración. Escribamos $p(x) = a_n x^n + \cdots + a_0$. Veamos que $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ son linealmente independientes: si $\sum_{i=0}^{n-1} \lambda_i \bar{x}^i = 0$, con $\lambda_i \in k$, entonces $\sum_{i=0}^{n-1} \lambda_i x^i = p(x)$. Ahora bien, el grado del término de la izquierda de la igualdad es menor que n, mientras que el de la derecha es mayor o igual que n, salvo que sea cero, así ha de ser y por tanto $\lambda_i = 0$ para todo i.

Veamos que $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ son generadores: Escribamos $p(x) = a_n x^n + \cdots + a_0$. Tenemos $0 = \overline{p(x)} = a_n \bar{x}^n + \cdots + a_0$, por tanto

$$\begin{aligned} \bar{x}^n &= \tfrac{-1}{a_n}(a_{n-1}\bar{x}^{n-1} + \cdots + a_0) \in \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle \\ \bar{x}^{n+1} &= \tfrac{-\bar{x}}{a_n}(a_{n-1}\bar{x}^{n-1} + \cdots + a_0) \in \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}, \bar{x}^n \rangle = \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle \end{aligned}$$

etc. □

Lema 3.4.6. *$\{\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)}^{n-1}\}$ es una base de $k[x]/((x-\lambda)^n)$.*

Demostración. Sabemos que las clases $\bar{1}, \bar{y}, \ldots, \bar{y}^{n-1}$ forman una base de $k[y]/(y^n)$. Haciendo el cambio $y = x - \lambda$ concluimos. □

Sea T un endomorfismo de un espacio vectorial E. Supongamos que $E_T \simeq k[x]/((x-\lambda)^n)$. Tomemos la base $\{e_j = \overline{(x-\lambda)}^{j-1} \mid 0 \leq j \leq n-1\}$. Se tiene

$$T(e_j) = x \cdot \overline{(x-\lambda)}^{j-1} = (x-\lambda) \cdot \overline{(x-\lambda)}^{j-1} + \lambda \overline{(x-\lambda)}^{j-1} = e_{j+1} + \lambda e_j$$

Por lo tanto, la matriz de T vale

$$\begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

En general, la descomposición de E_T será

$$E_T = \bigoplus_{i,j} k[x]/((x-\lambda_i)^{n_{ij}})$$

(no hay sumandos de la forma $k[x]$ porque E es de dimensión finita). Tomando una base en cada sumando $k[x]/((x-\lambda_i)^{n_{ij}})$, como acabamos de hacer, obtendremos una base de E en la que la matriz de T es de la forma llamada de Jordan:

$$\begin{pmatrix} (B_{11}) & & & \\ & \ddots & & \\ & & (B_{ij}) & \\ & & & \ddots \end{pmatrix}$$

siendo (B_{ij}) la siguiente matriz $n_{ij} \times n_{ij}$

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

2. Caso del cuerpo $\mathbb{R}$

Lema 3.4.7. *Sea E un espacio vectorial sobre $\mathbb{C}$, de base $\{e_1, \ldots, e_n\}$. Entonces $\{e_1, ie_1, \ldots, e_n, ie_n\}$ es una base de E como $\mathbb{R}$ espacio vectorial.*

Demostración. $\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i$, por tanto

$$E = \mathbb{C}e_1 \oplus \cdots \oplus \mathbb{C}e_n = (\mathbb{R}e_1 \oplus \mathbb{R}ie_1) \oplus \cdots \oplus (\mathbb{R}e_n \oplus \mathbb{R}ie_n)$$

□

Lema 3.4.8. *Sea E un espacio vectorial sobre $\mathbb{C}$, de base $\{e_1, \ldots, e_n\}$. Sea $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal, cuya matriz asociada es (a_{ij}). Escribamos $a_{ij} = b_{ij} + b'_{ij}i$. Entonces T es un endomorfismo $\mathbb{R}$-lineal cuya matriz en la base $\{e_1, ie_1, \ldots, e_n, ie_n\}$ es*

$$\begin{pmatrix} (a_{11}) & \ldots & (a_{1n}) \\ & (a_{ij}) & \\ (a_{1n}) & \ldots & (a_{nn}) \end{pmatrix}$$

siendo $(a_{ij}) = \begin{pmatrix} b_{ij} & -b'_{ij} \\ b'_{ij} & b_{ij} \end{pmatrix}$, es decir, (a_{ij}) es la matriz de multiplicar por a_{ij} en $\mathbb{C}$.

Demostración. Sólo es observar que

$$T(e_i) = \sum_j a_{ij}e_i = \sum_j (b_{ij}e_i + b'_{ij}ie_i)$$
$$T(ie_i) = \sum_j a_{ij}ie_i = \sum_j (-b'_{ij}e_i + b_{ij}ie_i)$$

□

Lema 3.4.9. *Sea $\alpha \in \mathbb{C} - \mathbb{R}$. Existe un isomorfismo de $R[x]$-módulos*

$$\mathbb{R}[x]/((x-\alpha)^n(x-\bar{\alpha})^n) = \mathbb{C}[x]/((x-\alpha)^n)$$

Por tanto, multiplicar por x en el término de la izquierda de la igualdad es multiplicar por x en el término de la derecha y aquí es un endomorfismo $\mathbb{C}$-lineal.

Demostración. Ambos módulos son $\mathbb{R}$-espacios vectoriales de dimensión $2n$. Sea $\langle\bar{1}\rangle$ el $\mathbb{R}[x]$-submódulo de $\mathbb{C}[x]/((x-\alpha)^n)$ generado por la clase $\bar{1}$. Determinemos el anulador de $\bar{1}$: Por una parte, es claro que $(x-\alpha)^n(x-\bar{\alpha})^n$ es un polinomio con coeficientes reales que anula a $\bar{1}$; por otra parte, el anulador deberá ser un múltiplo de $(x-\alpha)^n$. Dado que todo polinomio con coeficientes reales que tiene una raíz compleja tiene también la conjugada (con igual multiplicidad) se concluye que el polinomio anulador de $\bar{1}$ es $(x-\alpha)^n(x-\bar{\alpha})^n$.

Se tiene entonces una inclusión

$$\mathbb{R}[x]/((x-\alpha)^n(x-\bar{\alpha})^n) = \langle \bar{1} \rangle \subseteq \mathbb{C}[x]/((x-\alpha)^n)$$

y como ambos $\mathbb{R}$-espacios vectoriales son de la misma dimensión, se concluye que la inclusión anterior es una igualdad. □

Los polinomios irreducibles de $\mathbb{R}[x]$ son $x-\lambda$, $(\lambda \in \mathbb{R})$ y $(x-\alpha)(x-\bar{\alpha})$, con $\alpha \in \mathbb{C}-\mathbb{R}$.

Sea T un endomorfismo de un espacio vectorial real E.

Supongamos que $E_T \simeq \mathbb{R}[x]/((x-\alpha)^n(x-\bar{\alpha})^n) = \mathbb{C}[x]/((x-\alpha)^n)$. Multiplicar por x en $\mathbb{C}[x]/((x-\alpha)^n)$ es un endomorfismo $\mathbb{C}$-lineal, cuya matriz asociada en la base, sobre $\mathbb{C}$, $\bar{1}, \overline{(x-\alpha)}, \ldots, \overline{(x-\alpha)}^{n-1}$ es

$$\begin{pmatrix} \alpha & & & \\ 1 & \alpha & & \\ & \ddots & \ddots & \\ & & 1 & \alpha \end{pmatrix}$$

por tanto, en la base $\{e_j = (x-\alpha)^{j-1}, e'_j = i(x-\alpha)^{j-1}\}$ la matriz asociada a T es

$$\begin{pmatrix} (\alpha) & & & \\ (1) & (\alpha) & & \\ & \ddots & \ddots & \\ & & (1) & (\alpha) \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} b & -b' \\ b' & b \end{pmatrix} & & & \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} b & -b' \\ b' & b \end{pmatrix} & & \\ & \ddots & \ddots & \\ & & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} b & -b' \\ b' & b \end{pmatrix} \end{pmatrix}$$

siendo $\alpha = b + b'i$.

Nota: Si en $\mathbb{R}[x]/((x-\alpha)^n(x-\bar{\alpha})^n)$ consideramos la base $\{e_j = (x-\alpha)^{j-1}, e'_j = i(x-\alpha)^{j-1}\}$, donde $i = \overline{q(x)}$ cumple que $\overline{q(x)}^2 = -1$ (y escribimos $\alpha = b + b'\overline{q(x)}$), entonces la matriz asociada a T es la anterior. Explícitamente, como es tedioso comprobar, puede tomarse $q(x) = y \cdot \sum_{i=0}^{n-1} a_i(y^2+1)^i$, con $y = \frac{x-b}{b'}$, $a_0 = 1$, $a_r = \frac{1}{2} - \frac{1}{2} \sum_{\substack{i+j=r \\ i,j<r}} a_i a_j$.

En el caso general, la descomposición del $\mathbb{R}$-espacio vectorial E de dimensión finita será

$$E_T = \underset{i,j}{\oplus} \mathbb{R}[x]/(p_i(x)^{n_{ij}})$$

donde los $p_i(x)$ son irreducibles y por lo tanto son de la forma $p_i(x) = x - \lambda_i$ ó bien $p_i(x) = (x-\alpha_i)(x-\bar{\alpha}_i)$, con $\alpha_i = b_i + b'_i i$ $(b'_i \neq 0)$.

Tomando como antes una base en cada sumando $\mathbb{R}[x]/(p_i(x)^{n_{ij}})$, obtendremos una base de E en la que la matriz de T es

$$\begin{pmatrix} (B_{11}) & & & \\ & \ddots & & \\ & & (B_{ij}) & \\ & & & \ddots \end{pmatrix}$$

donde (B_{ij}) es la matriz:

Si $p_i(x) = x - \lambda_i$ entonces

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

Si $p_i(x) = (x - \alpha_i)(x - \bar{\alpha}_i)$ entonces

$$(B_{ij}) = \begin{pmatrix} \begin{pmatrix} b_i & -b_i' \\ b_i' & b_i \end{pmatrix} & & & \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} b_i & -b_i' \\ b_i' & b_i \end{pmatrix} & & \\ & \ddots & \ddots & \\ & & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} b_i & -b_i' \\ b_i' & b_i \end{pmatrix} \end{pmatrix}$$

3.5 Factores invariantes

Consideremos una presentación de un A-módulo M finito generado, es decir, una sucesión exacta

$$A^m \xrightarrow{\psi} A^n \longrightarrow M \longrightarrow 0$$

Consideremos sendas bases $\{e_1', \ldots, e_m'\}$ y $\{e_1, \ldots, e_n\}$ de A^m y A^n. Escribamos $\psi(e_i') = \sum_j a_{ij} e_j$, así que (a_{ij}) es la matriz de ψ. Definimos entonces los siguientes ideales:

Definición 3.5.1. Se llama i-ésimo ideal de Fitting de M al ideal $F_i(M)$ generado por los menores de orden $n - i$ de la matriz de ψ. Si $i > n$ seguiremos la convención $F_i(M) = (1)$ y si $m < i \leq n$ seguiremos la convención $F_i(M) = (0)$.

Veamos que los ideales de Fitting de un módulo no dependen de las bases elegidas en la presentación: Consideremos otra base $\{\bar{e}_1, \ldots, \bar{e}_m\}$ de A^m y escribamos $\psi(\bar{e}_j) = \sum_i \bar{a}_{ij} e_i$, así que la nueva matriz de ψ es $(\bar{a}_{ij})$. Denotemos $F_i(M)$ y $\bar{F}_i(M)$ a los respectivos ideales i-ésimos de Fitting de las matrices (a_{ij}) y $(\bar{a}_{ij})$. Cada $\bar{e}_j$ es combinación lineal de la antigua base $\{e_1', \ldots, e_m'\}$ y, por lo tanto, cada columna de $(\bar{a}_{ij})$ es combinación lineal de las columnas de (a_{ij}). En consecuencia, los menores de orden $n - i$ de $(\bar{a}_{ij})$ son combinación lineal de los menores de (a_{ij}), es decir, $\bar{F}_i(M) \subseteq F_i(M)$. Por simetría también se cumple $F_i(M) \subseteq \bar{F}_i(M)$; luego en conclusión $F_i(M) = \bar{F}_i(M)$. Si la que cambiamos es la base de A^n se razona de modo similar (por filas en vez de por columnas).

Dada la sucesión exacta $A^m \xrightarrow{\psi} A^n \to M \to 0$ y $x \in \operatorname{Spec} A$, entonces $A_x^m \xrightarrow{\psi_x} A_x^n \to M_x \to 0$ es exacta. La matriz asociada a ψ, es la misma que la asociada a ψ_x, por tanto $(F_i(M))_x = F_i(M_x)$.

Notación: Denotemos c_i al generador del ideal $F_i(M)$, es decir, c_i es el máximo común divisor de los menores de orden $n - i$ de la matriz de ψ. Los menores de orden $n - i$ son combinación lineal de menores de orden $n - i - 1$, por tanto, c_i es múltiplo de c_{i+1}.

Definición 3.5.2. A los elementos $\phi_i = c_{i-1}/c_i$ se les llama factores invariantes del módulo M. Si $c_i = c_{i-1} = 0$ diremos que $\phi_i = 0$.

Teorema 3.5.3 (de clasificación. Segunda versión). *Los ideales de Fitting de un módulo no dependen de la presentación finita escogida. Por tanto, los factores invariantes no dependen de la presentación finita escogida.*

Además,

$$M \simeq A/(\phi_1) \oplus \cdots \oplus A/(\phi_n)$$

Luego, dos A-módulos finito generados son isomorfos si y sólo si poseen los mismos factores invariantes.

Demostración. Sea $A^m \xrightarrow{\psi} A^n \to M \to 0$ una sucesión exacta. Dos elementos de A son iguales (salvo invertibles) si al localizar en cada punto cerrado del espectro son iguales y dos módulos son isomorfos si lo son localmente. Por lo tanto, podemos suponer que A es un anillo local de ideal maximal $\mathfrak{m} = (p)$.

Por 3.2.9 existen bases de A^m y A^n de modo que correspondiente matriz de ψ es

$$\begin{pmatrix}
p^{n_1} & & & & & & & & \\
& \overset{s}{\ddots} & & & & & & & \\
& & p^{n_s} & & & & & & \\
& & & 1 & & & & & \\
& & & & \overset{s'}{\ddots} & & & & \\
& & & & & 1 & & & \\
0 & & & & & & 0 & & \\
\vdots & & & & & & & \ddots & \\
r & & & & & & & & 0 \\
\vdots & & & & & & & & \vdots \\
0 & & & & & & & & 0
\end{pmatrix}$$

Reordenado la base de A^m, podemos suponer que $p^{n_1} \geq \cdots \geq p^{n_s}$.

Ahora ya tenemos que $M = A^r \oplus A/(p_1^n) \oplus \cdots \oplus A/(p^{n_s})$. Por tanto, r es el rango de M y p^{n_i} son los divisores elementales de M. Es una sencilla comprobación el ver que $c_i = 0$ para $i < r$, $c_i = p^{n_s} \cdots p^{n_{i-r+1}}$, para $r \leq i < r + s$, $c_i = 1$, para $i \geq r + s$. Tenemos calculados los ideales de Fitting, en términos del rango y los divisores elementales de M, por tanto, no dependen de ψ. Por último, $\phi_i = 0$ para $i \leq r$, $\phi_i = p^{n_{i-r}}$ para $r < i \leq r + s$, y $\phi_i = 1$ para $i > r + s$. Así pues,

$$M \simeq A/(\phi_1) \oplus \cdots \oplus A/(\phi_n)$$

□

Observación 3.5.4. Observemos, por el cálculo efectuado en la demostración del teorema anterior, que ϕ_i es múltiplo de ϕ_{i+1}. Por tanto, (ϕ_1) es el ideal anulador de M.

Teorema 3.5.5 (de clasificación de endomorfismos). *Dos endomorfismos de un k-espacio vectorial de dimensión finita E son equivalentes si y sólo si poseen los mismos factores invariantes.*

Sea E un k-espacio vectorial de dimensión n. Consideremos un endomorfismo T y la correspondiente estructura de $k[x]$-módulo sobre E. Sea (λ_{ij}) la matriz de T en una base $\{e_1, \ldots, e_n\}$ de E. Vamos a determinar los factores invariantes de T a partir de su matriz.

Sea $E[x]$ el conjunto de polinomios con coeficientes en E. $E[x]$ es $k[x]$-módulo, $(\sum_i a_i x^i)*(\sum_j e'_j x^j) = \sum_{i,j} a_i e'_j x^{i+j}$, y resulta ser libre de base $\{e_1, \ldots, e_n\}$. Consideremos el epimorfismo de $k[x]$-módulos $\pi\colon E[x] \to E$, $\pi(\sum_i e'_i x^i) = \sum_i x^i e'_i$. Obviamente el $k[x]$-módulo $\langle ex - xe \mid e \in E\rangle_{k[x]}$ está incluido en el núcleo de π. Veamos que coinciden:

En $E[x]/\langle ex - xe \mid e \in E\rangle$ se verifica que $x * \bar{e} = \overline{ex} = \overline{xe}$, luego $\overline{ex^n} = x^n * \bar{e} = \overline{x^n e}$. Por tanto, el morfismo de k-espacios vectoriales $E \xrightarrow{i} E[x]/\langle ex - xe \mid e \in E\rangle$, $e \mapsto \bar{e}$ es epiyectivo. Como la composición

$$E \xrightarrow{i} E[x]/\langle ex - xe \mid e \in E\rangle \xrightarrow{\pi} E$$

es el morfismo identidad, se deduce que $E[x]/\langle ex - xe \mid e \in E\rangle = E$.

Así pues, tenemos la sucesión exacta de $k[x]$-módulos

$$\begin{array}{ccccc} E[x] & \overset{(x*-x\cdot)}{\to} & E[x] & \xrightarrow{\pi} & E \to 0 \\ e & \mapsto & ex - xe & & \end{array}$$

Por lo tanto, la sucesión anterior es una presentación de E_T como $k[x]$-módulo. La matriz del morfismo $(x * -x\cdot)$ es $xId - (\lambda_{ij})$. Luego

Teorema 3.5.6. *Sea (λ_{ij}) la matriz $n \times n$ de un endomorfismo T. Sea $c_i(x)$ el máximo común divisor de los menores de orden $n - i$ de la matriz $xId - (\lambda_{ij})$. Se verifica*

$$c_i(x) = \phi_{i+1}(x) \cdots \phi_n(x)$$
$$\phi_i(x) = c_{i-1}(x)/c_i(x)$$

siendo $\phi_1(x), \ldots, \phi_n(x)$ los factores invariantes de T.

Observaciones:

a) El polinomio $c_0(x) = det\left(xId - (\lambda_{ij})\right)$ se llama polinomio característico de T. Según el teorema anterior, el polinomio característico es igual al producto de los factores invariantes. Además como todos los factores invariantes dividen al primet factor invariante, ϕ_1 (que es el polinomio anulador), tenemos que el polinomio característico tiene las mismas raíces salvo multiplicidades que el polinomio anulador.

b) Un caso particular es el **Teorema de Hamilton-Cayley:**

$$\phi_1(x) = c_0(x)/c_1(x)$$

es decir, el polinomio anulador de T es igual al cociente del polinomio característico por el máximo común divisor de los menores de orden $n - 1$ de la matriz $xId - (\lambda_{ij})$.

3.6 Problemas

1. Sea A un dominio de ideales principales. Si $aA \cap bA = cA$, pruébese que c es el mínimo común múltiplo de a y b.
2. Sea A un dominio de ideales principales. Sean $a = p_1^{n_1} \cdots p_r^{n_r}$, $b = p_1^{m_1} \cdots p_r^{m_r}$ con $n_i, m_j \geq 0$, p_i irreducibles y p_i primo con p_j, para $i \neq j$. Calcúlese el mínimo común múltiplo y máximo común divisor de de a y b.

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

   (a) Probar la fórmula de conmutación

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

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

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

   (c) Resolver la ecuación diferenciales: $y'''' - 2y''' + 2y'' = 0$, $y'' + y = 0$.

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

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

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

   (a) Probar las fórmulas de conmutación

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

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

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

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

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

8. Sea A un dominio de ideales principales y M un A-módulo de ideal anulador no nulo $a \cdot A$. Probar que si a' es un elemento propio que divide a a, entonces $\operatorname{Ker} a'\cdot \neq 0$, donde $a'\cdot$ es el endomorfismo de M, definido por $(a'\cdot)(m) = am$.

9. Sean p y q números primos distintos. Calcular el número de grupos abelianos finitos desisomorfos de orden p^2q.

10. Pruébese que un grupo abeliano finito que no sea cíclico contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, para un cierto entero primo p.

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

12. Sea G un subgrupo discreto del grupo aditivo de $\mathbb{R}^n$. Pruébese que existe un número natural $r \leq n$, tal que G está generado como $\mathbb{Z}$-módulo por r vectores linealmente independientes sobre $\mathbb{R}$.

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

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

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

15. Clasifíquense los endomorfismos T de un espacio vectorial real E, que cumplan

    (a) Anulador de $T = (x-1)^2$, $\dim E = 5$.

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

16. Sea E el espacio vectorial real de todos los polinomios con coeficientes reales de grado menor que 6, y sea D el operador derivada sobre E. Clasifíquese el endomorfismo $T = D^2$.

17. Probar que un grupo abeliano finito generado es cíclico si y sólo si tiene un único factor invariante.

18. Clasificar sobre el cuerpo racional los endomorfismos

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

19. Sean $T, T' \colon E \to E$ dos endomorfismos lineales de un espacio vectorial de dimensión finita, de modo que en cierta base la matriz de T es la transpuesta de la de T'. Probar que T y T' son endomorfismos equivalentes.

20. Sea A un anillo euclídeo y (a_{ij}) una matriz con coeficientes $a_{ij} \in A$. Sustituyendo de modo conveniente y sucesivo la fila F_i por la fila $F_i + b_j F_j$, $i \neq j$, $b_j \in A$ (i, j, b_j arbitrarios), demostrar que la matriz (a_{ij}) es triangulable. Si admitimos, además, las mismas transformaciones "elementales" con las columnas, demostrar que (a_{ij}) es diagonalizable. Resolver el sistema de ecuaciones diofánticas

$$7x + 5y = 1$$
$$5x + 3y = 3$$

21. Clasificar los $\mathbb{Z}$-módulos $(\mathbb{Z} \times \mathbb{Z})/\langle (7,5), (5,3) \rangle$ y $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle (12,30,24), (4,8,6), (6,4,8) \rangle$.

22. Mediante transformaciones elementales calcular los factores invariantes del endomorfismo de $\mathbb{R}^3$ de matriz

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 1 & 3 \end{pmatrix}$$

Calcular $e_1, e_2 \in \mathbb{R}^3$ de modo que $\mathbb{R}^3 = (k[x]/(\phi_1))e_1 \oplus (k[x]/(\phi_2))e_2$.

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

24. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Probar que la condición necesaria y suficiente para que el endomorfismo $p(T)$ sea invertible es que $p(x)$ y $c_T(x)$ sean primos entre sí.

25. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Sea $E' \subseteq E$ un subespacio estable por T. Denotemos $\bar{T}\colon E/E' \to E/E'$, $\bar{T}(\bar{e}) = \overline{T(e)}$, el endomorfismo inducido por T en E/E'. Probar que

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

26. Sea E un $\mathbb{C}$-espacio vectorial de dimensión n y T un endomorfismo de E. Sea $c_T(x) = \prod_{i=1}^{n}(x-\alpha_i)$ la descomposición en factores lineales del polinomio característico de T. Pruébese que si $p(x)$ es un polinomio con coeficientes en $\mathbb{C}$, entonces

$$c_{p(T)}(x) = \prod_{i=1}^{n}(x - p(\alpha_i))$$

En particular, se tiene que $\operatorname{tr}(p(T)) = \sum_{i=1}^{n} p(\alpha_i)$, $\det(p(T)) = \prod_{i=1}^{n} p(\alpha_i)$.

27. Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita. Sea $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal de E. Demostrar que si $c_T(x)$ es el polinomio característico de T considerado como endomorfismo $\mathbb{C}$-lineal, entonces el polinomio característico de T considerado como endomorfismo $\mathbb{R}$-lineal es $c_T(x) \cdot \overline{c_T(x)}$ (donde $\overline{c_T(x)}$ es el conjugado de $c_T(x)$).

28. (a) Sea $X' = AX$ un sistema homogéneo de ecuaciones diferenciales, siendo A una matriz cuadrada de coeficientes constantes. Probar que $e^{At} \cdot C$ son las soluciones del sistema, siendo C una matriz columna de constantes.

    (b) Sea $X' = AX + B(t)$ un sistema lineal de ecuaciones diferenciales. Calcular la matriz columna $C(t)$ tal que $e^{At} \cdot C(t)$ sea una solución del sistema.

29. Resuélvanse los siguientes sistemas de ecuaciones diferenciales

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

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

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

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

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

(b) Pruébese este resultado como caso particular de 28 (b).

32. Sea A una matriz con coeficientes en $k[D]$. Probar que mediante las transformaciones elementales, el problema de resolver los sistemas $AX(t) = Y(t)$, se reduce al problema de resolver ecuaciones $P(D)f(t) = h(t)$.

33. Resolver el sistema de ecuaciones diferenciales

$$\begin{aligned} &x'' - x + y' = e^t \\ &x'' + 2x' + x + y'' = e^t \end{aligned}$$

Capítulo 4

Producto tensorial. Módulos proyectivos e inyectivos

4.1 Categorías. Funtor de homorfismos

Dar una categoría $\mathcal{C}$ es dar

1. Una familia arbitraria, cuyos elementos llamaremos objetos de $\mathcal{C}$.
2. Unos conjuntos $\mathrm{Hom}_{\mathcal{C}}(M,N)$, para cada par de objetos M,N de $\mathcal{C}$, cuyos elementos f llamaremos morfismos de M en N y denotaremos por el símbolo $f\colon M \to N$.
3. Una aplicación

$$\mathrm{Hom}_{\mathcal{C}}(N,P) \times \mathrm{Hom}_{\mathcal{C}}(M,N) \to \mathrm{Hom}_{\mathcal{C}}(M,P), \quad (f,g) \mapsto f \circ g$$

para cada terna M,N,P de objetos de $\mathcal{C}$. Satisfaciéndose

   (a) $(f \circ g) \circ h = f \circ (g \circ h)$.
   (b) Para cada objeto M de $\mathcal{C}$, existe un morfismo $\mathrm{Id}_M\colon M \to M$ de modo que $f \circ \mathrm{Id}_M = f$ y $\mathrm{Id}_M \circ g = g$ para todo morfismo $f\colon M \to N$ y $g\colon N \to M$.

Un morfismo $f\colon M \to N$ se dice que es un isomorfismo si existe $g\colon N \to M$ de modo que $f \circ g = \mathrm{Id}_N$ y $g \circ f = \mathrm{Id}_M$.

Ejemplo 4.1.1. La categoría $\mathcal{C}_{Conj}$ de conjuntos es la categoría cuyos objetos son los conjuntos y los morfismos entre los objetos son las aplicaciones de conjuntos. La categoría $\mathcal{C}_{Mod}$ de A-módulos es la categoría cuyos objetos son los A-módulos y los morfismos entre los objetos son los morfismos de módulos.

Definición 4.1.2. Sean $\mathcal{C}$ y $\mathcal{C}'$ dos categorías. Dar un funtor covariante $F\colon \mathcal{C} \rightsquigarrow \mathcal{C}'$ es asignar a cada objeto M de $\mathcal{C}$ un objeto $F(M)$ de $\mathcal{C}'$, y cada morfismo $f\colon M \to M$ de $\mathcal{C}$ un morfismo $F(f)\colon F(M) \to F(N)$ de $\mathcal{C}'$, de modo que se verifique que $F(f \circ g) = F(f) \circ F(g)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Análogamente se definen los funtores F contravariantes, que invierten el sentido de los morfismos; es decir, asignan a cada morfismo $f\colon M \to N$ de $\mathcal{C}$ un morfismo $F(f)\colon F(N) \to F(M)$ de $\mathcal{C}'$, de modo que verifica $F(f \circ g) = F(g) \circ F(f)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Un morfismo $f\colon M \to M'$ induce las aplicaciones

$$\mathrm{Hom}(N,M) \xrightarrow{f_*} \mathrm{Hom}(N,M'),\ g \mapsto f_*(g) \underset{\text{def}}{=} f\circ g$$
$$\mathrm{Hom}(M',N) \xrightarrow{f^*} \mathrm{Hom}(M,N),\ g \mapsto f^*(g) \underset{\text{def}}{=} g\circ f$$

Estamos diciendo que $\mathrm{Hom}(N,-)$ es un funtor covariante de $\mathcal{C}$ en la categoría de los conjuntos $\mathcal{C}_{Conj}$, es decir,

$$\begin{aligned}\mathrm{Hom}(N,-)\colon \mathcal{C} &\rightsquigarrow \mathcal{C}_{Conj}\\ M &\rightsquigarrow \mathrm{Hom}(N,M)\\ f &\rightsquigarrow f_*\\ (f\circ g) &\rightsquigarrow (f\circ g)_* = (f_*\circ g_*)\end{aligned}$$

$\mathrm{Hom}(-,N)$ es un funtor contravariante

$$\begin{aligned}\mathrm{Hom}(-,N)\colon \mathcal{C} &\rightsquigarrow \mathcal{C}_{Conj}\\ M &\rightsquigarrow \mathrm{Hom}(M,N)\\ f &\rightsquigarrow f^*\\ (f\circ g) &\rightsquigarrow (f\circ g)^* = (g^*\circ f^*)\end{aligned}$$

Definición 4.1.3. Dos funtores $F, F'\colon \mathcal{C}\rightsquigarrow\mathcal{C}'$ se dicen que son isomorfos, y escribimos $F \overset{\theta}{\simeq} F'$, si para cada objeto M de $\mathcal{C}$ tenemos isomorfismos $\theta_M\colon F(M) \simeq F'(M)$, de modo que para cada morfismo $f\colon M \to N$ el diagrama

$$\begin{array}{ccc} F(M) & \xrightarrow{F(f)} & F(N)\\ \Big\| \theta_M & & \Big\| \theta_N\\ F'(M) & \xrightarrow{F'(f)} & F'(N)\end{array}$$

es conmutativo.

Proposición 4.1.4. *El funtor* $\mathrm{Hom}(M,-)$ *es isomorfo al funtor* $\mathrm{Hom}(M',-)$*, si y sólo si* $M \simeq M'$*. "Los objetos de una categoría están determinados por sus relaciones"*

Demostración. Veamos sólo la suficiencia. Si $\mathrm{Hom}(M,-) \overset{\theta}{\simeq} \mathrm{Hom}(M',-)$, entonces este isomorfismo queda determinado por $\theta_M(\mathrm{Id}_M) = g$: Dado $f \in \mathrm{Hom}(M,N)$ consideremos el diagrama

$$\begin{array}{ccc} \mathrm{Hom}(M,M) & \overset{\theta_M}{=\!=} & \mathrm{Hom}(M',M)\\ \Big| f_* & & \Big| f_*\\ \mathrm{Hom}(M,N) & \overset{\theta_N}{=\!=} & \mathrm{Hom}(M',N)\end{array} \qquad \begin{array}{ccc} \mathrm{Id}_M & \xrightarrow{\theta_M} & g\\ \Big| f_* & & \Big| f_*\\ f & \overset{\theta_N}{\dashrightarrow} & f_*(g) = f\circ g\end{array}$$

Luego $\theta_N(f) = f_*(g) = f\circ g$.

Así pues, si tenemos un isomorfismo $\mathrm{Hom}(M,-) \overset{\theta}{\simeq} \mathrm{Hom}(M',-)$ y denotamos $\theta_M(\mathrm{Id}_M) = g$ y $\theta_{M'}^{-1}(\mathrm{Id}_{M'}) = f$ tendremos que

$$\mathrm{Id}_M \overset{\theta_M}{\rightsquigarrow} g \overset{\theta_{M'}^{-1}}{\rightsquigarrow} g_*(f) = g \circ f = \mathrm{Id}_M$$
$$\mathrm{Id}_{M'} \overset{\theta_{M'}^{-1}}{\rightsquigarrow} f \overset{\theta_M}{\rightsquigarrow} f_*(g) = f \circ g = \mathrm{Id}_{M'}$$

□

Definición 4.1.5. Se dice que un funtor covariante F es representable si existe un objeto M, de modo que $F = \mathrm{Hom}(M,-)$. Se dice que un funtor contravariante F es representable si existe un objeto M, de modo que $F = \mathrm{Hom}(-,M)$. En estos casos se dice que M es el representante de F.

Por la proposición anterior sabemos que el representante de un funtor representable es único salvo isomorfismos.

Teorema 4.1.6. *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

$$0 \to \mathrm{Hom}_A(N,M') \xrightarrow{i_*} \mathrm{Hom}_A(N,M) \xrightarrow{p_*} \mathrm{Hom}_A(N,M'')$$

"Se dice que $\mathrm{Hom}_A(N,-)$ es un funtor exacto por la izquierda".

Demostración. Es sencillo comprobar la necesidad de la condición. En cuanto a la suficiencia, basta tomar $N = A$, pues para todo A-módulo M tenemos un isomorfismo natural $\mathrm{Hom}_A(A,M) = M$, $f \mapsto f(1)$. □

También se tiene el teorema "dual" del anterior:

Teorema 4.1.7. *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

$$0 \to \mathrm{Hom}_A(M'',N) \xrightarrow{p^*} \mathrm{Hom}_A(M,N) \xrightarrow{i^*} \mathrm{Hom}_A(M',N)$$

"Se dice que $\mathrm{Hom}_A(-,N)$ es un funtor exacto por la derecha".

Demostración. Es sencillo comprobar la necesidad de la condición. Veamos la suficiencia. Sea $N = M''/\operatorname{Im} p$, y $\pi\colon M \to N$ la proyección canónica. Tenemos que $p^*(\pi) = \pi \circ p = 0$, luego $\pi = 0$ y p es epiyectiva. Si tomamos ahora $N = M''$, entonces $0 = (p^* \circ i^*)(\mathrm{Id}) = p \circ i$, luego $\operatorname{Im} i \subseteq \operatorname{Ker} p$. Por último, si $N = M/\operatorname{Im} i$ y $\pi\colon M \to M/\operatorname{Im} i$ es la proyección canónica, entonces $i^*(\pi) = \pi \circ i = 0$. Luego existe un morfismo $f\colon M'' \to N$ tal que $f \circ p = p^*(f) = \pi$ y concluimos que $\operatorname{Ker} p = p^{-1}(0) \subseteq (f \circ p)^{-1}(0) = \pi^{-1}(0) = \operatorname{Im} i$. □

4.2 Construcción del producto tensorial de módulos

El objetivo de esta sección es definir el producto tensorial de dos A-módulos. Si bien se puede dar una interpretación geométrica del producto tensorial, creemos conveniente que primero se domine esta

operación. Queremos definir "el producto" ($\otimes$) de elementos de M por N, cumpliendo las siguientes propiedades

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

Es decir, queremos definir un módulo $M\otimes_A N$ generado por elementos $m\otimes n$, $m\in M$ y $n\in N$, cumpliendo las propiedades anteriores y sin más relaciones que las generadas por las relaciones de M y N y estas propiedades. Empecemos con el formalismo necesario para la construcción de $M\otimes_A N$.

Sean M y N dos A-módulos. Consideremos el A-módulo libre $A^{(M\times N)}$. Dado $(m,n)\in M\times N$, denotemos $(m,n)=(a_i)_{i\in M\times N}$ al elemento de $A^{(M\times N)}$ definido por $a_{(m',n')}=0$ si $(m',n')\neq(m,n)$ y $a_{(m',n')}=1$ si $(m',n')=(m,n)$. Es decir, estamos identificando los elementos de $M\times N$ con la base estándar de $A^{(M\times N)}$.

Sea R el submódulo de $A^{(M\times N)}$ generado por los elementos de la forma

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

Definición 4.2.1. Llamaremos producto tensorial de M y N sobre el anillo A al A-módulo cociente $A^{(M\times N)}/R$ y lo denotaremos $M\otimes_A N$. Cada clase $\overline{(m,n)}\in A^{(M\times N)}/R = M\otimes_A N$ la denotaremos $m\otimes n$.

De acuerdo con la definición de R y $M\otimes_A N$ tenemos que

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

propiedades que se expresan diciendo "el producto tensorial es A-bilineal".

Dado que los elementos $\{(m,n)\}_{(m,n)\in M\times N}$ forman una base de $A^{(M\times N)}$ entonces los elementos $\{m\otimes n\}_{(m,n)\in M\times N}$ forman un sistema generador de $M\otimes_A N$. Por las propiedades de bilinealidad recién escritas, si $\{m_i\}$ y $\{n_j\}$ son sistemas generadores de M y N, entonces $\{m_i\otimes n_j\}$ es un sistema generador de $M\otimes_A N$.

Sea P un A-módulo.

Definición 4.2.2. Diremos que una aplicación $\beta\colon M\times N\to P$ es A-bilineal si

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

El conjunto de las aplicaciones A-bilineales de $M\times N$ en P se denota $Bil_A(M,N;P)$. La condición de que una aplicación $\beta\colon M\times N\to P$ sea A-bilineal expresa que la aplicación $\beta_m\colon N\to P$, $\beta_m(n)=\beta(m,n)$, es un morfismo de A-módulos para cada elemento $m\in M$. Obtenemos así un isomorfismo natural

$$Bil_A(M,N;P)=\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$$

El morfismo natural $\pi\colon M\times N\to M\otimes N$, $(m,n)\mapsto m\otimes n$, es bilineal.

Teorema 4.2.3 (Propiedad universal del producto tensorial). *La aplicación*

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

es un isomorfismo. Es decir, $M \otimes_A N$ es el representante del funtor $Bil_A(M, N; -)$.

Demostración. Sea $\beta\colon M \times N \to P$ una aplicación A-bilineal, entonces el morfismo de A-módulos

$$\varphi\colon A^{(M\times N)} \to P,\ \varphi(\sum_i a_i(m_i, n_i)) = \sum_i a_i\beta(m_i, n_i)$$

se anula sobre los generadores del submódulo R, anteriormente definido. Por la tanto, induce el morfismo de A-módulos $\phi\colon M \otimes_A N \to P$, $m \otimes n \mapsto \beta(m, n)$. Este morfismo cumple que $\beta = \phi \circ \pi$ y si un morfismo ϕ' cumple esta igualdad entonces $\phi'(m \otimes n) = \beta(m, n)$ y coincide con ϕ, pues los elementos $m \otimes n$ generan $M \otimes N$.

Por último, es una simple comprobación ver que dado un morfismo de A-módulos $\phi\colon M \otimes N \to P$ entonces $\beta = \phi \circ \pi$ es una aplicación bilineal de $M \times N$ en P.

□

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

Observación 4.2.4. Análoga construcción se puede hacerse para cualquier familia finita $M_1, \ldots, M_n$ de A-módulos, obteniéndose un A-módulo $M_1 \otimes_A \cdots \otimes_A M_n$ con una propiedad universal similar. Para definir un morfismo de A-módulos $f\colon M_1 \otimes_A \cdots \otimes_A M_n \to P$, bastará definir las imágenes $f(m_1 \otimes \cdots \otimes m_n)$ de modo que

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

4.3 Propiedades del producto tensorial

Teorema 4.3.1. *Existen isomorfismos naturales*

1. $(M \otimes_A N) \otimes_A P = M \otimes_A N \otimes_A P$, $(m \otimes n) \otimes p \mapsto m \otimes n \otimes p$.
2. $M \otimes_A N = N \otimes_A M$, $m \otimes n \mapsto n \otimes m$.
3. $A \otimes_A M = M$, $a \otimes m \mapsto am$.
4. $(\underset{i\in I}{\oplus} M_i) \otimes_A N = \underset{i\in I}{\oplus}(M_i \otimes N)$, $(m_i)_{i\in I} \otimes n \mapsto (m_i \otimes n)_{i\in I}$.
5. $M \otimes_A A_S = M_S$, $m \otimes \frac{a}{s} \mapsto \frac{am}{s}$.
6. $M \otimes_A (A/I) = M/IM$, $m \otimes \bar{a} \mapsto \overline{am}$.

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

Probemos, con otro método, $(\underset{i\in I}{\oplus} M_i)\otimes_A N = \underset{i\in I}{\oplus}(M_i\otimes N)$:

$$\begin{aligned}\mathrm{Hom}_A((\underset{i\in I}{\oplus} M_i)\otimes_A N, P) &= \mathrm{Hom}_A(\underset{i\in I}{\oplus} M_i, \mathrm{Hom}_A(N,P)) = \prod_{i\in I}\mathrm{Hom}_A(M_i, \mathrm{Hom}_A(N,P))\\ &= \prod_{i\in I}\mathrm{Hom}_A(M_i\otimes_A N, P) = \mathrm{Hom}_A(\underset{i\in I}{\oplus}(M_i\otimes_A N), P)\end{aligned}$$

Por la unicidad del representante (4.1.4), $(\underset{i\in I}{\oplus} M_i)\otimes_A N = \underset{i\in I}{\oplus}(M_i\otimes N)$.

□

Si $f\colon A\to B$ es un morfismo de anillos entonces B es de modo natural un A-módulo. Cada elemento $b\in B$ define un endomorfismo $1\otimes b\colon M\otimes_A B\to M\otimes_A B$, $m\otimes b' \underset{\text{def}}{\mapsto} m\otimes bb'$. Podemos definir así, una estructura de B-módulo en $M\otimes_A B$ que viene dada por el siguiente producto

$$b\cdot(\sum_i m_i\otimes b_i) = \sum_i m_i\otimes bb_i$$

Se dice que el cambio de base de M por $A\to B$ es $M\otimes_A B$.

Notación: Denotaremos $M\otimes_A B = M_B$ y usualmente denotaremos $f(a) = a$.

Proposición 4.3.2. *Sean $A\to B$ y $B\to C$ morfismos de anillos y M, M' A-módulos y N un B-módulo. Existen isomorfismos naturales*

1. $M_B\otimes_B N = M\otimes_A N$, $(m\otimes b)\otimes n\mapsto m\otimes bn$.
2. $(M\otimes_A M')\otimes_A B = M_B\otimes_B M'_B$, $(m\otimes m')\otimes b\mapsto (m\otimes b)\otimes(m'\otimes 1)$.
3. $(M_B)_C = M_C$, *(i.e.,* $(M\otimes_A B)\otimes_B C = M\otimes_A C$*)*, $(m\otimes b)\otimes c\mapsto m\otimes bc$.

Demostración. Defínanse los morfismos inversos. □

Proposición 4.3.3. *Sea $M'\to M\to M''\to 0$ una sucesión exacta y N un A-módulo. Se cumple que*

$$M'\otimes_A N\to M\otimes_A N\to M''\otimes_A N\to 0$$

es una sucesión exacta. Es decir, "$-\otimes_A N$ es un funtor exacto por la derecha".

Demostración. Sea $M^{\cdot}$ la sucesión exacta inicial. De acuerdo con 4.1.7

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

es una sucesión exacta para todo A-módulo P. De nuevo 4.1.7 nos permite concluir que la sucesión $M^{\cdot}\otimes_A N$ es exacta. □

4.4 Producto exterior

Ahora, nuestro objetivo es definir el producto exterior de un A-módulo.

Definición 4.4.1. Si $A \to B$ es un morfismo de anillos se dice que B es una A-álgebra.

Definición 4.4.2. Un anillo $R = \bigoplus_{n\in\mathbb{Z}} R_n$ diremos que es un álgebra graduada, si los R_n son estables para la suma y dados $r_n \in R_n$, $r_m \in R_m$ entonces $r_n \cdot r_m \in R_{n+m}$. Además, diremos que R es una A-álgebra graduada si R_0 es una A-álgebra.

Los anillos de polinomios son de modo obvio k-álgebras graduadas.

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

Definición 4.4.3. Diremos que $T^{\cdot} M = \bigoplus_{i=0}^{\infty} T^n M$ es el álgebra tensorial de M.

Dados $m_1 \otimes \cdots \otimes m_n \in T^n M$ y $m'_1 \otimes \cdots \otimes m'_r \in T^r M$ definimos

$$(m_1 \otimes \cdots \otimes m_n) \cdot (m'_1 \otimes \cdots \otimes m'_r) = m_1 \otimes \cdots \otimes m_n \otimes m'_1 \otimes \cdots \otimes m'_r \in T^{r+n} M$$

que extendido linealmente a $T^{\cdot} M$, define un producto, con el que es una A-álgebra graduada.

Proposición 4.4.4. *Hay un isomorfismo* $T^n(M \oplus M') = \bigoplus_{i+j=n} T^i M \otimes_A T^j M'$ *natural.*

Demostración. Es consecuencia de que el producto tensorial conmuta con la suma directa. □

Consideremos en $T^n M$ el submódulo

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

Definición 4.4.5. Diremos que $\Lambda^n M = T^n M / M'_n$ es el álgebra exterior n-ésima del A-módulo M. Diremos que $\Lambda^{\cdot} M = \bigoplus_{i=0}^{\infty} \Lambda^i M$ es el álgebra exterior de M

Proposición 4.4.6. *Hay un isomorfismo* $\Lambda^n(M \oplus M') = \bigoplus_{i+j=n} \Lambda^i M \otimes_A \Lambda^j M'$ *natural.*

Demostración. La composición de los morfismos $T^n(M \oplus M') \to \bigoplus_{i+j=n} T^i M \otimes_A T^j M' \to \bigoplus_{i+j=n} \Lambda^i M \otimes_A \Lambda^j M'$ induce un morfismo $\Lambda^n(M \oplus M') \to \bigoplus_{i+j=n} \Lambda^i M \otimes_A \Lambda^j M'$. Recíprocamente, la composición de los morfismos naturales $\bigoplus_{i+j=n} T^i M \otimes_A T^j M' \to \bigoplus_{i+j=n} \to T^n(M \oplus M') \to \Lambda^n(M \oplus M')$ induce el morfismo $\bigoplus_{i+j=n} \Lambda^i M \otimes_A \Lambda^j M' \to \Lambda^n(M \oplus M')$. Fácilmente se comprueba que estos dos morfismos son inversos entre si. □

Ejercicio 4.4.7. Probar que $\Lambda^n A^n \simeq A$.

Es claro que $M'_n \cdot T^r M \subseteq M'_{n+s}$. Por tanto el producto que tenemos definido en $T^{\cdot} M$, define por paso al cociente un producto de $\Lambda^{\cdot} M$. Luego $\Lambda^{\cdot} M$ es un álgebra graduada.

Se suele denotar $m_1 \wedge \cdots \wedge m_n$ a la clase de $m_1 \otimes \overset{n}{\cdots} \otimes m_n$ en $\Lambda^n M$ y $\wedge$ al producto que tenemos definido en $\Lambda^{\cdot} M$. Obeservemos que

$$0 = \cdots \wedge m + m' \wedge \cdots \wedge m + m' \wedge \cdots = (\cdots \wedge m \wedge \cdots \wedge m' \wedge \ldots) + (\cdots \wedge m' \wedge \cdots \wedge m \wedge \ldots)$$

Luego $m_1 \wedge \cdots \wedge m \wedge \cdots \wedge m' \wedge \cdots \wedge m_n = -(m_1 \wedge \cdots \wedge m' \wedge \cdots \wedge m \wedge \cdots \wedge m_n)$. De aquí es fácil concluir que dados $w_n \in \Lambda^n M$ y $w_r \in \Lambda^r M$, entonces $w_r \wedge w_n = (-1)^{rs} w_r \wedge w_n$.

Por tanto, $\Lambda^{\cdot} M$ es una A-álgebra graduada "anticonmutativa".

4.5 Producto tensorial de álgebras

Ahora, nuestro objetivo es definir el producto tensorial de A-álgebras.

Si B y C son A-álgebras, el A-módulo $B \otimes_A C$ tiene tiene una estructura de A-álgebra natural: El producto es el morfismo $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$, $(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'$ inducido por el correspondiente morfismo $B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C$. Con este producto $B \otimes_A C$ es un anillo y por último el morfismo $A \to B \otimes_A C$, $a \mapsto a \otimes 1 = 1 \otimes a$ es un morfismo de anillos.

Definición 4.5.1. Diremos que un morfismo de anillos $f\colon B \to C$ entre A-álgebras, es un morfismo de A-álgebras si $f(a) = a$ para todo $a \in A$.

Proposición 4.5.2. *Sean B, C y D A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc} \mathrm{Hom}_{A-alg}(B \otimes_A C, D) & = & \mathrm{Hom}_{A-alg}(B, D) \times \mathrm{Hom}_{A-alg}(C, D) \\ \phi & \longrightarrow & (\phi_1, \phi_2) \quad \phi_1(b) = \phi(b \otimes 1), \phi_2(c) = \phi(1 \otimes c) \\ \phi\colon (b \otimes c) \mapsto \phi_1(b)\phi_2(c) & \longleftarrow & (\phi_1, \phi_2) \end{array}$$

Consideremos el sistema de ecuaciones

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

Sea $I = (p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n))$ y llamemos $A = \mathbb{C}[x_1, \ldots, x_n]/I$ el anillo de funciones de la variedad de soluciones del sistema de ecuaciones anterior. Observemos que $\mathrm{Hom}_{\mathbb{C}-alg}(A, \mathbb{C})$ se identifica con los puntos de la variedad de soluciones del sistema de ecuaciones anterior. Ya veremos que los puntos cerrados de $\mathrm{Spec}\, A$ se identifica con la variedad de soluciones del sistema de ecuaciones anterior, luego con $\mathrm{Hom}_{\mathbb{C}-alg}(A, \mathbb{C})$.

Dada otra variedad de ecuaciones

$$\begin{aligned} &p'_1(x_1, \ldots, x_n) = 0 \\ &\ldots \\ &p'_s(x_1, \ldots, x_n) = 0 \end{aligned}$$

denotemos $I' = (p'_1(x_1, \ldots, x_n), \ldots, p'_s(x_1, \ldots, x_n))$ y $A' = \mathbb{C}[x_1, \ldots, x_n]/I'$.

La proposición anterior nos dice que $\mathrm{Hom}_{\mathbb{C}-alg}(A, \mathbb{C}) \times \mathrm{Hom}_{\mathbb{C}-alg}(A', \mathbb{C}) = \mathrm{Hom}_{\mathbb{C}-alg}(A \otimes_{\mathbb{C}} A', \mathbb{C})$. Este hecho justificará la definición $\mathrm{Spec}\, A \times \mathrm{Spec}\, A' \underset{\text{def}}{=} \mathrm{Spec}\, A \otimes_{\mathbb{C}} A'$. Así, se interpretará el producto tensorial de anillos "de funciones de variedades" como el anillo del producto de las variedades.

Proposición 4.5.3. *Sean B y C A-álgebras. Se cumple el isomorfismo*

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

Ejercicio 4.5.4. 1. Con las notaciones obvias, pruébese que

$$\mathrm{Hom}_{A-\text{álg grad.}}(T^{\cdot}M, \oplus_i B_i) = \mathrm{Hom}_A(M, B_0)$$

Pruébese también que $\mathrm{Hom}_{A-\text{álg grad. anti.}}(\Lambda^{\cdot}M, \oplus_i B_i) = \mathrm{Hom}_A(M, B_0)$.

2. Probar que $T^{\cdot}M \otimes_A T^{\cdot}M' = T^{\cdot}(M \oplus M')$ y que $\Lambda^{\cdot}M \otimes_A \Lambda^{\cdot}M' = \Lambda^{\cdot}(M \oplus M')$, a partir de las proposiciones 4.4.4, 4.4.6, o de 1.

4.6 Módulos planos y proyectivos

Definición 4.6.1. Diremos que un A-módulo P es plano si para toda sucesión exacta $0 \to N' \to N \to N'' \to 0$ la sucesión $0 \to N' \otimes_A P \to N \otimes_A P \to N'' \otimes_A P \to 0$ es exacta. Es decir, por la proposición 4.3.3, si para toda inyección $N \hookrightarrow M$ entonces $N \otimes_A P \to \otimes_A P$ también es inyectiva.

Dado que $N \otimes_A A^{(I)} = N^{(I)}$ es fácil comprobar que $A^{(I)}$-es un A-módulo plano. Como $N \otimes_A (P \oplus P') = (N \otimes_A P) \oplus (N \otimes_A P')$ es fácil comprobar que una suma directa de módulos es plana si y sólo si cada sumando es plano.

Proposición 4.6.2. *Si P es un A-módulo plano y $A \to B$ es un morfismo de anillos, entonces P_B es un B-módulo plano.*

Demostración. Para todo B-módulo M tenemos que $P_B \otimes_B M = P \otimes_A M$, así que la exactitud del funtor $P_B \otimes_B (-)$ es consecuencia de la exactitud del funtor $P \otimes_A (-)$. □

Proposición 4.6.3. *La condición necesaria y suficiente para que un A-módulo P sea plano es que N_x sea un A_x-módulo plano para todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración. Denotemos toda sucesión exacta $0 \to N' \to N$ de A-módulos por $N^{\cdot}$. P es plano $\iff$ para toda sucesión exacta $N^{\cdot}$ entonces $N^{\cdot} \otimes_A P$ es exacta $\iff$ para todo punto cerrado $x \in \operatorname{Spec} A$ la sucesión $(N^{\cdot} \otimes_A P)_x = N^{\cdot}_x \otimes_{A_x} P_x$ es exacta $\iff$ P_x es un A_x-módulo plano para todo punto cerrado $x \in \operatorname{Spec} A$ □

Lema 4.6.4. *Sea M un módulo finito generado sobre un anillo local $\mathcal{O}$. Si el morfismo natural $I \otimes_{\mathcal{O}} M \to M$, $i \otimes m \mapsto im$, es inyectivo para todo ideal finito generado $I \subseteq A$, entonces M es un $\mathcal{O}$-módulo libre.*

Demostración. Sea $m_1, \ldots, m_r$ un sistema de generadores de M, obtenido por Nakayama (es decir, de modo que $\bar{m}_1, \ldots, \bar{m}_r$ sea una base de $M/\mathfrak{m}M$, donde $\mathfrak{m}$ es el ideal maximal de $\mathcal{O}$). Dada una relación $a_1 m_1 + \cdots + a_r m_r = 0$, consideremos el ideal $I = (a_1, \ldots, a_r)$. Por hipótesis el morfismo natural $I \otimes_{\mathcal{O}} M \to M$ es inyectivo, así que $a_1 \otimes m_1 + \cdots + a_r m_r = 0$. En el $\mathcal{O}/\mathfrak{m}$-espacio vectorial

$$\begin{aligned}(I \otimes_{\mathcal{O}} M)/\mathfrak{m}(I \otimes_{\mathcal{O}} M) &= (I \otimes_{\mathcal{O}} M) \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = (I \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}) \otimes_{\mathcal{O}/\mathfrak{m}} (M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}) \\ &= I/\mathfrak{m}I \otimes_{\mathcal{O}/\mathfrak{m}} M/\mathfrak{m}M\end{aligned}$$

tendremos que $\overline{a_1 \otimes m_1 + \cdots + a_r m_r} = \bar{a}_1 \otimes \bar{m}_1 + \cdots + \bar{a}_r \otimes \bar{m}_r = 0$. Pero $\bar{m}_1, \ldots, \bar{m}_r$ es una base de $M/\mathfrak{m}M$, por tanto $\bar{a}_1 = \cdots = \bar{a}_r = 0$. Luego $I/\mathfrak{m}I = 0$ y por Nakayama $I = 0$. En conclusión, $m_1, \ldots, m_r$ es una base de M y M es libre. □

Teorema 4.6.5 (Criterio del ideal de platitud). *Sea M un A-módulo finito generado. Si el morfismo natural $I \otimes_A M \to M$ es inyectivo para todo ideal $I \subseteq A$, entonces M es un A-módulo plano.*

Demostración. En cada punto cerrado $x \in \operatorname{Spec} A$ tenemos que el morfismo natural

$$I_x \otimes_{A_x} M_x = (I \otimes_A M)_x \to M_x$$

es inyectivo. Como cada ideal finito generado de A_x es localización de un ideal finito generado de A, el lema anterior permite concluir que M_x es un A_x-módulo libre y, por tanto, plano. Luego M es un A-módulo plano. □

Teorema 4.6.6. *Un A-módulo finito generado es plano si y sólo si es localmente libre.*

Demostración. Es consecuencia inmediata de 4.6.3 y 4.6.4. □

Definición 4.6.7. Se dice que un A-módulo P es proyectivo si para todo epimorfismo $\pi\colon M \to M''$ entonces $\pi_*\colon \operatorname{Hom}_A(P, M) \to \operatorname{Hom}_A(P, M'')$ es un epimorfismo. Es decir (por el teorema 4.1.6), P es proyectivo si la toma de $\operatorname{Hom}_A(P, -)$ conserva sucesiones exactas (es decir, "$\operatorname{Hom}_A(P, -)$ es un funtor exacto").

Como $\operatorname{Hom}_A(A^{(I)}, M) = \prod_I M$ es fácil demostrar que los A-módulos libres son proyectivos.

Proposición 4.6.8. *Un A-módulo es proyectivo si y sólo si es sumando directo de un libre.*

Demostración. Supongamos que P es un A-módulo proyectivo. Consideremos un epimorfismo $\pi\colon A^{(I)} \to P$. Si consideramos el morfismo $\mathrm{Id}\colon P \to P$ sabemos que levanta a un morfismo $s\colon P \to A^{(I)}$, tal que $s \circ \pi = \mathrm{Id}$, por ser P proyectivo. Por el ejercicio 2.1.5, $A^{(I)} = \operatorname{Ker} \pi \oplus P$.

Recíprocamente, sea M es un sumando directo de un libre, es decir $A^{(I)} = M \oplus M'$. $A^{(I)}$ es un módulo proyectivo, por tanto $M \oplus M'$ es proyectivo. Ahora bien, como $\operatorname{Hom}_A(M \oplus M', -) = \operatorname{Hom}_A(M, -) \times \operatorname{Hom}_A(M', -)$ es fácil probar que una suma directa de módulos es un módulo proyectivo si y sólo si lo es cada sumando. En conclusión, M es proyectivo. □

Proposición 4.6.9. *Los módulos proyectivos son planos.*

Demostración. Los módulos proyectivos son sumandos directos de un libre, que es plano, luego los módulos proyectivos son planos. □

Definición 4.6.10. Un A-módulo M se dice que es de presentación finita si existe una sucesión exacta de la forma $A^m \to A^n \to M \to 0$.

Si A es un anillo noetheriano (más adelante estudiados) un A-módulo es de presentación finita si y sólo si es finito generado.

Proposición 4.6.11. *Sea M un A-módulo de presentación finita y $S \subset A$ un sistema multiplicativo. Entonces para todo A-módulo N se cumple que*

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

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

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

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

Localizando por S tenemos la sucesión exacta

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

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

□

Teorema 4.6.12. *Un módulo de presentación finita es proyectivo si y sólo si es localmente proyectivo. Es decir, P es un A-módulo proyectivo si y sólo si para todo punto cerrado $x \in \mathrm{Spec}\, A$ se cumple que P_x es un A_x-módulo proyectivo.*

Demostración. Denotemos la sucesión exacta $0 \to N' \to N \to N'' \to 0$ por $N^\cdot$. Digamos que un módulo P es proyectivo si y sólo si para toda sucesión exacta $N^\cdot$ de A-módulos entonces la sucesión $\mathrm{Hom}_A(P, N^\cdot)$ es exacta. Con estas convenciones tenemos: P es proyectivo $\iff$ para toda sucesión exacta $N^\cdot$ de A-módulos $\mathrm{Hom}_A(P,N^\cdot)$ es exacta $\iff$ para toda sucesión exacta $N^\cdot$ de A-módulos $\mathrm{Hom}_A(P,N^\cdot)_x = \mathrm{Hom}_{A_x}(P_x, N_x^\cdot)$ es exacta para todo punto cerrado $x \in \mathrm{Spec}\, A$ $\iff$ P_x es un A_x-módulo proyectivo (pues toda sucesión exacta de A_x-módulos $N'^\cdot$ es localización de una sucesión exacta de A-módulos, explícitamente $(N'^\cdot)_x = N'^\cdot$). □

Teorema 4.6.13. *Sea M un módulo de presentación finita. Las condiciones de ser plano, localmente libre y proyectivo son equivalentes.*

Demostración. Si M es plano entonces es localmente libre por 4.6.6.

Si M es localmente libre entonces es localmente proyectivo. Como la propiedad de ser proyectivo es local será proyectivo.

Si M es proyectivo por 4.6.9 es plano. □

4.7 Módulos inyectivos. Criterio del ideal para módulos inyectivos

Definición 4.7.1. Diremos que un A-módulo M es inyectivo si el functor contravariante $\mathrm{Hom}_A(-,M)$ es exacto en la categoría de A-módulos; es decir, si transforma inyecciones en epiyecciones.

Se verifican trivialmente las siguientes propiedades:

a) El producto directo de módulos inyectivos es inyectivo.

b) Un sumando directo de un módulo inyectivo es también inyectivo.

Proposición 4.7.2 (Criterio del ideal). *Un A-módulo M es inyectivo si y sólo si para todo ideal $I \subset A$ el morfismo* $\mathrm{Hom}_A(A, M) \to \mathrm{Hom}_A(I, M)$ *es epiyectivo.*

Demostración. Basta ver el recíproco. Dada una inclusión $N' \hookrightarrow N$ y un morfismo $f' \colon N' \to M$ tenemos que demostrar que f extiende a un morfismo $f \colon N \to M$. Sea N'' un submodulo de N que contiene a N' y maximal con la condición de que exista una extensión $f'' \colon N'' \to M$ de f'. La existencia de N'' se debe al lema de Zorn. Tenemos que probar que $N'' = N$. Sea $n \in N$ e $I = \{a \in A : a \cdot n \in N''\}$. Tenemos definido un morfismo $g \colon I \to M, a \mapsto f''(a \cdot n)$, que por hipótesis extiende a un morfismo $g' \colon A \to M$. El morfismo $\langle n \rangle \to M, a \cdot n \mapsto g'(a)$ etá bien definido, coincide con f'' sobre $\langle n \rangle \cap N'' = I \cdot n$, luego define un morfismo $f''' \colon N'' + \langle n \rangle \to M, n'' + an \mapsto f''(n'') + g'(a)$. Por maximalidad de N'' ha de verificarse que $n \in N''$, luego $N'' = N$. □

Definición 4.7.3. Sea A un dominio de integridad. Un A-módulo M se dice de división si para todo $a \in A$ no nulo, el morfismo $M \xrightarrow{\cdot a} M$ es epiyectivo.

Teorema 4.7.4. *Sea A íntegro. Todo módulo inyectivo es de división. Si A es un dominio de ideales principales, entonces un módulo es inyectivo precisamente si es de división.*

Demostración. Tómese la sucesión exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & aA & \hookrightarrow & A & \longrightarrow & A/aA & \longrightarrow & 0 \\ & & \downarrow \wr & & \| & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{\cdot a} & A & \longrightarrow & A/aA & \longrightarrow & 0 \end{array}$$

y $\mathrm{Hom}_A(\ \ , M)$.

□

Así, por ejemplo, $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son $\mathbb{Z}$-módulos inyectivos, y por tanto $R = \mathbb{Q} \oplus \mathbb{Q}/\mathbb{Z}$ es inyectivo.

4.7.1 Integrabilidad de los sistemas de ecuaciones diferenciales en derivadas parciales lineales

El objetivo de esta sección es dar las condiciones necesarias y suficientes para que el sistema de ecuaciones diferenciales

$$P_i\left(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right) v(x_1, \ldots, x_n) = u_i(x_1, \ldots, x_n), \quad i = 1, \ldots, m \qquad (*)$$

con $P_i(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ y $u_i(x_1, \ldots, x_n) \in \mathbb{R}[[x_1, \ldots, x_n]]$, sea integrable, es decir, exista $v(x_1, \ldots, x_n) \in \mathbb{R}[[x_1, \ldots, x_n]]$ verificando el sistema anterior.

Si consideramos una sucesión exacta

$$\mathbb{R}[[x_1, \ldots, x_n]] \xrightarrow{\bigoplus_i P_i\left(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right)} \bigoplus_{i=1}^{m} \mathbb{R}[[x_1, \ldots, x_n]] \xrightarrow{\pi} \mathrm{Coker}$$

la existencia de $v(x_1, \ldots, x_n)$ verificando el sistema anterior, equivale a decir que $\pi(u_1, \ldots, u_m) = 0$. Vamos a ver que se puede obtener esta sucesión exacta como dual de otra bien conocida.

Lema 4.7.5. *Consideremos* $\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$ *como el anillo obvio, isomorfo a* $\mathbb{R}[x_1,\dots,x_n]$. *Consideremos* $\mathbb{R}[[x_1,\dots,x_n]]$ *como* $\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$*-módulo del modo obvio:*

$$P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})\cdot v(x_1,\dots,x_n) = P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})v(x_1,\dots,x_n)$$

Con esta estructura de $\mathbb{R}[x_1,\dots,x_n]$*-módulo, se cumple que* $\mathbb{R}[[x_1,\dots,x_n]]$ *es el representante del funtor* $\mathrm{Hom}_{\mathbb{R}}(-,\mathbb{R})$ *en la categoría de* $\mathbb{R}[x_1,\dots,x_n]$*-módulos. En particular,* $\mathbb{R}[[x_1,\dots,x_n]]$ *es un* $\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$*-módulo inyectivo.*

Demostración. Sea A una k-álgebra. Empecemos probando que el A-módulo $\mathrm{Hom}_k(A,k)$ es inyectivo.

En la categoría de A-módulos, se cumple el isomorfismo de funtores

$$\mathrm{Hom}_k(-,k) \xrightarrow{\quad\varphi\quad} \mathrm{Hom}_A(-,\mathrm{Hom}_k(A,k))$$

$$w \longrightarrow (\varphi(w)(m))(a) = w(am)$$

$$\varphi^{-1}(w)(m) = (w(m))(1) \longleftarrow w$$

Como el funtor $\mathrm{Hom}_k(-,k)$ es exacto, tenemos que $\mathrm{Hom}_k(A,k)$ es un A-módulo inyectivo.

Por otra parte, es una sencilla comprobación, el ver que el morfismo

$$\mathbb{R}[[x_1,\dots,x_n]] \xrightarrow{\phi} \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}],\mathbb{R})$$

definido por

$$\phi(s(x_1,\dots,x_n))(P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})) = (P(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})s(x_1,\dots,x_n))(0,\dots,0)$$

es un isomorfismo de $\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$-módulos. Con todo, $\mathbb{R}[[x_1,\dots,x_n]]$ es un $\mathbb{R}[\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n}]$-módulo inyectivo. □

Consideremos la sucesión exacta

$$\overset{r}{\oplus}\mathbb{R}[x_1,\dots,x_n] \xrightarrow{(p_{ij})} \overset{m}{\oplus}\mathbb{R}[x_1,\dots,x_n] \xrightarrow{\sum P_i\cdot} \mathbb{R}[x_1,\dots,x_n] \to \mathbb{R}[x_1,\dots,x_n]/(P_1,\dots,P_m) \to 0$$

Aplicando el funtor $\mathrm{Hom}_{\mathbb{R}}(-,\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}[x_1,\dots,x_n]}(-,\mathbb{R}[[x_1,\dots,x_n]])$ obtenemos la sucesión exacta

$$(\mathbb{R}[x_1,\dots,x_n]/(P_1,\dots,P_m))^* \hookrightarrow \mathbb{R}[[x_1,\dots,x_n]] \xrightarrow{\oplus P_i(\frac{\partial}{\partial x_1},\dots,\frac{\partial}{\partial x_n})} \overset{m}{\oplus}\mathbb{R}[[x_1,\dots,x_n]] \xrightarrow{(p_{ij})^t} \overset{m}{\oplus}\mathbb{R}[[x_1,\dots,x_n]]$$

Así pues, el sistema diferencial $(*)$ es integrable si y sólo si $(p_{ij})^t(u_1,\dots,u_n) = 0$. Además, observemos que si hay soluciones, la dimensión del espacio de soluciones es $\dim_{\mathbb{R}}(\mathbb{R}[x_1,\dots,x_n]/(P_1,\dots,P_m))$.

Dejamos como ejercicio que el lector pruebe las siguientes afirmaciones. Consideremos la sucesión exacta de $\mathbb{R}[x_1,\dots,x_n]$-módulos

$$0 \to \mathbb{R}[x_1,\dots,x_n]\cdot x_1\wedge\cdots\wedge x_n \xrightarrow{\delta} \bigoplus_i \mathbb{R}[x_1,\dots,x_n]\cdot x_1\wedge\cdots\wedge\hat{x}_i\wedge\cdots\wedge x_n \to \cdots$$
$$\xrightarrow{\delta} \bigoplus_i \mathbb{R}[x_1,\dots,x_n]\cdot x_i \xrightarrow{\delta} \mathbb{R}[x_1,\dots,x_n] \to \mathbb{R} \to 0$$

donde $\delta(x_{i_1}\wedge\cdots\wedge x_{i_r}) = \sum_k (-1)^k x_{i_k}\cdot x_{i_1}\wedge\cdots\wedge\widehat{x_{i_k}}\wedge\cdots\wedge x_{i_r}$. Aplicando el funtor $\mathrm{Hom}_{\mathbb{R}}(-,\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}[x_1,\dots,x_n]}(-,\mathbb{R}[[x_1,\dots,x_n]])$ obtenemos la sucesión exacta de De Rham

$$\mathbb{R} \to \mathbb{R}[[x_1,\dots,x_n]] \xrightarrow{d} \bigoplus_i \mathbb{R}[[x_1,\dots,x_n]]\cdot dx_i \xrightarrow{d} \cdots \xrightarrow{d} \bigoplus_i \mathbb{R}[[x_1,\dots,x_n]]\cdot dx_1\wedge\cdots\wedge\widehat{dx_i}\wedge\cdots\wedge dx_n$$
$$\xrightarrow{d} \mathbb{R}[[x_1,\dots,x_n]]\cdot dx_1\wedge\cdots\wedge dx_n \to 0$$

4.8 Problemas

1. Probar que si E es un k-espacio vectorial de dimensión n y E' es un k-espacio vectorial de dimensión m, entonces $E\otimes_k E'$ es un k-espacio vectorial de dimensión $n\cdot m$.
2. Probar que $M\otimes_A A[x] = M[x]$.
3. Probar que $\mathbb{R}[x]/(p(x))\otimes_{\mathbb{R}}\mathbb{C} = \mathbb{C}[x]/(p(x))$.
4. Probar que $(A[x_1,\dots,x_n]/I)\otimes_A B = B[x_1,\dots,x_n]/I\cdot B[x_1,\dots,x_n]$.
5. (a) Sea $N'\subset N$ un A-submódulo y $M = N/N'$. Probar que si $N\otimes_A N = 0$ entonces $M\otimes_A M = 0$.
   (b) Sea I un ideal de A, calcular $A/I\otimes_A A/I$.
   (c) Probar que si M es un A-módulo finito distinto de cero entonces $M\otimes_A M$ es distinto de cero.
6. Probar que $(\mathbb{Q}/\mathbb{Z})\otimes_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) = 0$.
7. Sea $A\to B$ un morfismo de anillos, M un A-módulo y N, P B-módulos. Probar que
$$(M\otimes_A N)\otimes_B P = M\otimes_A (N\otimes_B P)$$
8. Definir un morfismo natural $M^*\otimes_A N\to \mathrm{Hom}_A(M,N)$. Demostrar que si N es un módulo de tipo finito y libre entonces $M^*\otimes_A N^* = Bil_A(M,N;A)$.
9. Si $M_1,\dots,M_n$ son A-módulos libres finito generados probar que $M_1^*\otimes_A\cdots\otimes_A M_n^* = Multil_A(M_1,\dots,M_n;A)$.
10. Probar que si $\mathrm{Spec}\, A = U_1\coprod U_2$, y M es un A-módulo, entonces $M = M_{U_1}\times M_{U_2}$.
11. Sea $A\to B$ un morfismo de anillos. Sean M y M' dos B-módulos, en particular son A-módulos. Sea el A-submódulo de $M\otimes_A M'$, $N = \langle bm\otimes m' - m\otimes bm' \mid m\in M, m'\in M', b\in B\rangle$. Probar que existe un isomorfismo de B-módulos
$$(M\otimes_A M')/N \simeq M\otimes_B M'$$
12. Probar que $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} = \mathbb{C}\times\mathbb{C}$ como $\mathbb{C}$-álgebra.

13. Calcular $\mathrm{Hom}_{\mathbb{R}-\text{álg.}}(\mathbb{C},\mathbb{C})$.

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

15. Sea A íntegro y M un A-módulo de presentación finita. Probar que existe un abierto $U \subseteq \mathrm{Spec}\, A$ no vacío tal que M_U es un A_U-módulo libre.

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

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

18. Probar que $k[x,y]/(x)$ no es un $k[x,y]$-módulo plano. Sea $k[x] \to k[x,y]/(y^2-x)$ el morfismo natural, probar que $k[x,y]/(y^2-x)$ es una $k[x]$-álgebra plana.

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

20. Sea A un anillo local y M un A-módulo proyectivo. Probar que M es un A-módulo libre.

21. Probar que existe un isomorfismo $\mathrm{Hom}_k(k[x]/(p(x)),k) \simeq k[x]/(p(x))$, de $k[x]/(p(x))$-módulos. Probar que $k[x]/(p(x))$ es un $k[x]/(p(x))$-módulo inyectivo. Dar una nueva demostración del tercer teorema de descomposición de los $k[x]$-módulos finitos.

Capítulo 5

Anillos noetherianos

5.1 Módulos noetherianos

La introducción de los módulos la justificabamos 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.

Definición 5.1.1. [1] Un A-módulo M se dice que es un A-módulo noetheriano si todo submódulo suyo (propio o no) es finito generado.

Definición 5.1.2. [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 $M_m = M_{m+1} = \cdots$.

Proposición 5.1.3. *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 $M' = \overset{\infty}{\underset{i=1}{\cup}} M_i \subseteq M$. Como M' es un submódulo de M, es finito generado. Escribamos $M' = \langle m_1, \ldots, m_r \rangle$, con $m_j \in M_{i_j}$. 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 $\langle m_1, \ldots, m_m\rangle = M'$.

□

Ejemplo 5.1.4. Los k-espacios vectoriales de dimensión finita son k-módulos noetherianos.

Proposición 5.1.5. *Todo submódulo de un módulo noetheriano es noetheriano.*

Proposición 5.1.6. *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, $\bar{M} = \langle \pi(m_1), \ldots, \pi(m_r)\rangle$. □

Proposición 5.1.7. *Sea*

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

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

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

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

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

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

□

Ejercicio 5.1.8. Probar que M y M' son noetherianos si y sólo si $M \oplus M'$ es noetheriano.

Definición 5.1.9. 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.

Ejemplo 5.1.10. 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.

Corolario 5.1.11. *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 5.1.7. 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.

Ejercicio 5.1.12. Si A es noetheriano A_S es noetheriano

Ejercicio 5.1.13. Demostrar que $\mathbb{Q}[x, x_1, \ldots, x_n, \ldots]/((x-n)x_n)_{\{n\in\mathbb{N}\}}$ es localmente noetheriano pero no es noetheriano.

Proposición 5.1.14. *Si A es un anillo noetheriano, entonces* 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, $C_m = C_{m+1} = \cdots$.

□

Ejercicio 5.1.15. 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.

Ejercicio 5.1.16. Probar que en un anillo noetheriano el número de ideales primos minimales es finito.

5.2 Teorema de la base de Hilbert

Teorema 5.2.1 (de la base de Hilbert). *Si A es un anillo noetheriano entonces $A[x]$ es un anillo noetheriano.*

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

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

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

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

Recurrentemente obtendré que

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

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

□

Definición 5.2.2. 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

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

es epiyectivo.

Corolario 5.2.3. *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.

□

Definición 5.2.4. 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, $f\colon A \to B$ 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.

5.3 Ideal primario. Interpretación geométrica

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

Definición 5.3.1. Sea A un anillo. Un ideal $\mathfrak{q} \neq A$ es primario si

$$ab \in \mathfrak{q}\,,\ a \notin \mathfrak{q} \ \Rightarrow\ b^n \in \mathfrak{q} \text{ para algún } n \geq 1$$

Es decir, cuando en $A/\mathfrak{q}$ todo divisor de cero sea nilpotente.

Ejemplo 5.3.2.

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 $k[x]$

Definición 5.3.3. Dado un ideal $I \subseteq A$, llamaremos radical y denotaremos $r(I)$ a

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

Observemos que si $\pi\colon A \to A/I$ es el morfismo de paso al cociente, entonces $\pi^{-1}(\operatorname{rad} A/I) = r(I)$.

El radical de un ideal primario es un ideal primo. En efecto, sea $\mathfrak{p}$ el radical de un ideal primario $\mathfrak{q}$. Si $ab \in \mathfrak{p}$ y $a \notin \mathfrak{p}$, entonces $a^n b^n \in \mathfrak{q}$ para algún $n \geq 1$. Como $a^n \notin \mathfrak{q}$, se sigue que alguna potencia de b^n ha de estar en $\mathfrak{q}$, lo que implica que $b \in \mathfrak{p} = r(\mathfrak{q})$.

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 $B \to A$ es un morfismo de anillos, es sencillo comprobar que $B \cap \mathfrak{q}$ es un ideal $(B \cap \mathfrak{p})$-primario de B.

Sea $\mathfrak{m}$ un ideal maximal de un anillo A. Los ideales $\mathfrak{m}$-primarios de A son los ideales de radical $\mathfrak{m}$. En efecto, si $\mathfrak{m}$ es el radical de un ideal I, entonces es el único ideal primo de A que contiene a I. Se sigue que el anillo A/I tiene un único ideal primo; luego todo elemento de A/I es invertible o nilpotente y concluimos que en A/I todo divisor de cero es nilpotente. En particular, todas las potencias $\mathfrak{m}^n$ son ideales $\mathfrak{m}$-primarios.

Si el anillo A es noetheriano, cada ideal contiene una potencia de su radical, así que todo ideal $\mathfrak{m}$-primario es de la forma $\pi^{-1}(\bar{\mathfrak{q}})$ para algún ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}^r$ (donde $\pi\colon A \to A/\mathfrak{m}^r$ es el morfismo de paso al cociente). En el caso del anillo $A = \mathbb{C}[x_1, \ldots, x_n]$, si consideramos el ideal maximal $\mathfrak{m}$ formado por todos los polinomios que se anulan en cierto punto racional $(a_1, \ldots, a_n)$ y ponemos $t_i = x_i - a_i$, entonces

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

y la reducción módulo $\mathfrak{m}^r$ de cualquier polinomio coincide con el clásico desarrollo de Taylor hasta el orden $r-1$ en el punto $(a_1, \ldots, a_n)$. 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 lo que 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 $\{\omega_\alpha = \frac{\partial^{|\alpha|}}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n}, \alpha_1 + \cdots + \alpha_n < r\}$, que vienen definidas por $\omega_\alpha(\bar{f}) = \frac{\partial^{|\alpha|} f}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n}(a_1, \ldots, a_n)$. 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 ecuaciones de s-ecuaciones

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

(variando r,$\lambda_{i,\alpha}$ 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 $(a_1, \ldots, a_n)$.

Proposición 5.3.4. *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, para que dos ideales $\mathfrak{p}_x$-primarios coincidan es suficiente que coincidan 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 $\mathfrak{q}$, por tanto, $f \in \mathfrak{q}$. Concluimos que $A \cap (\mathfrak{q}A_S) \subseteq \mathfrak{q}$. La inclusión $\mathfrak{q} \subseteq A \cap (\mathfrak{q}A_S)$ es evidente. □

En general, sea $\mathfrak{p}_x$ el ideal primo de un punto $x \in \operatorname{Spec} A$. Los ideales de A_x de radical $\mathfrak{p}_x = \mathfrak{p}_x A_x$ (que deben llamarse ideales de condiciones infinitesimales en el punto x, pues en el caso noetheriano vienen determinados por los ideales de los anillos $A_x/\mathfrak{p}_x^{r+1}A_x$) son precisamente los ideales $\mathfrak{p}_x$-primarios, porque $\mathfrak{p}_x$ es un ideal maximal de A_x. Por tanto, si $\mathfrak{q}_x$ es uno de estos ideales, $A \cap \mathfrak{q}_x$ es un ideal $\mathfrak{p}_x$-primario de A. Si denotamos $\pi\colon A \to A_x/\mathfrak{p}_x^r A_x$ por el morfismo natural, todo ideal $\mathfrak{p}_x$-primario es de la forma $\pi^{-1}(\bar{\mathfrak{q}})$, donde $\bar{\mathfrak{q}}$ es un ideal de $A_x/\mathfrak{p}_x^r A_x$. Así se obtienen todos los ideales $\mathfrak{p}_x$-primarios de A; es decir, *los ideales $\mathfrak{p}_x$-primarios son los ideales definidos por condiciones infinitesimales en el punto x.*

Ejemplo 5.3.5. 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 y una recta que pase por él. Sea $\mathfrak{m}$ el ideal maximal del punto y $\mathfrak{p}$ el ideal primo del punto genérico de la recta. Consideremos ahora el ideal $I = \mathfrak{m}^2 \cap \mathfrak{p}$ formado por los polinomios que se anulan en el punto genérico de la recta y sus derivadas parciales se anulan en el punto fijado. El radical de I es

$$r(I) = r(\mathfrak{m}^2) \cap r(\mathfrak{p}) = \mathfrak{m} \cap \mathfrak{p} = \mathfrak{p}$$

pero el ideal I no es primario: el producto de la ecuación de la recta fijada por la de otra recta que pase por el punto está en I, la ecuación de la recta fijada no está en I y la ecuación de la otra recta no está en $\mathfrak{p} = r(I)$. Esto se debe a que el ideal I no está definido por condiciones infinitesimales en un solo punto del espectro sino en dos: en el punto fijado y en el punto genérico de la recta dada.

Incluso puede darse el caso de que una potencia de un ideal primo no sea un ideal primario. Por ejemplo, sea A el anillo de las funciones algebraicas sobre un cono en $\mathbb{A}_3$ y sea $\mathfrak{p}_x$ el ideal primo de A definido por una generatriz.

El ideal ${\mathfrak{p}_x}^2$ no viene definido por condiciones infinitesimales en el punto genérico de tal generatriz; es decir, ${\mathfrak{p}_x}^2$ no coincide con $A \cap {\mathfrak{p}_x}^2 A_x$ sino que involucra además condiciones en el vértice del cono, pues las funciones de ${\mathfrak{p}_x}^2$ 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 directriz está en $A \cap {\mathfrak{p}_x}^2 A_x$; pero no está en ${\mathfrak{p}_x}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal ${\mathfrak{p}_x}^2$ no es primario.

5.4 Existencia de las descomposiciones primarias

Definición 5.4.1. 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 ($I \neq \mathfrak{q}_1 \cap \ldots \cap \widehat{\mathfrak{q}_i} \cap \ldots \cap \mathfrak{q}_n$ para todo $1 \leq i \leq n$) ni componentes asociadas a un mismo ideal primo ($r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ cuando $i \neq j$).

Proposición 5.4.2. *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: *si un ideal admite una descomposición primaria, admite una descomposición primaria reducida.*

Definición 5.4.3. Diremos que un ideal $\mathfrak{q}$ de un anillo A es irreducible si no es intersección de dos ideales estrictamente mayores; es decir, si el ideal 0 del anilo cociente $A/\mathfrak{q}$ no es intersección de dos ideales no nulos.

Lema 5.4.4 (Fundamental). *Sea* A *un anillo noetheriano. Todo ideal irreducible* $\mathfrak{q} \neq A$ *es primario.*

Demostración. Para ver que $\mathfrak{q}$ es primario, tenemos que probar que los divisores de cero de $A/\mathfrak{q}$ son nilpotentes. Sea $b \in A/\mathfrak{q}$ divisor de cero. Consideremos los núcleos de los morfismos de A-módulos $b^n\cdot\colon A/\mathfrak{q} \to A/\mathfrak{q}$:

$$0 \neq \operatorname{Ker} b \subseteq \operatorname{Ker} b^2 \subseteq \cdots \subseteq \operatorname{Ker} b^n \subseteq \cdots$$

Como $A/\mathfrak{q}$ es noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún exponente n. Luego $(\operatorname{Ker} b) \cap (\operatorname{Im} b^n) = 0$. Por ser $\mathfrak{q}$ irreducible y $\operatorname{Ker} b \neq 0$ $\operatorname{Im} b^n$ es nulo. Entonces $0 = b^n \cdot 1 = b^n$ y b es nilpotente en $A/\mathfrak{q}$. Concluimos que el ideal $\mathfrak{q}$ es primario. □

Teorema 5.4.5 (de existencia). *Sea* A *un anillo noetheriano. Todo ideal* $I \neq A$ *es intersección finita de ideales primarios de* A*; es decir, está definido por condiciones infinitesimales en un número finito de puntos de* $\operatorname{Spec} A$*.*

Demostración. Si I no es un ideal primario, por el lema anterior, no es irreducible. Entonces $I = I_1 \cap J_1$ con con $I \underset{\neq}{\subset} I_1, J_1$. Si I_1 no es primario, de nuevo, existirán I_2, J_2 tales que $I_1 = I_2 \cap J_2$ con $I_1 \underset{\neq}{\subset} I_2, J_2$ y $I = I_2 \cap (J_2 \cap J_1)$. Si $J_2 \cap J_1 \neq I$, tenemos I como intersección propia de los dos ideales $I_2, (J_2 \cap J_1)$ y $I_1 \underset{\neq}{\subset} I_2$. Si $J_2 \cap J_1 = I$, redenotaremos $J_2 = I_2$ y de nuevo tenemos I como intersección de dos ideales I_2, J_1, con $I_1 \underset{\neq}{\subset} I_2$. Si I_2 no es primario repetimos el proceso. Así tendremos una cadena

$$I_1 \underset{\neq}{\subset} I_2 \underset{\neq}{\subset} I_3 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} I_n$$

que por noetherianidad ha de ser finita. Luego, para $n >> 0$, I_n es primario.

En conclusión, podemos escribir $I = I_1 \cap J_1$ con $I \underset{\neq}{\subset} I_1, J_1$ e I_1 primario. Si J_1 no es primario, de nuevo, $J_1 = I_2 \cap J_2$ con $J_1 \underset{\neq}{\subset} I_2, J_2$ e I_2 primario. Por tanto, $I = I_1 \cap I_2 \cap J_2$, con I_1, I_2 primario y $I \underset{\neq}{\subset} J_1 \underset{\neq}{\subset} J_2$. Repitiendo este proceso, obtenemos la cadena

$$I \underset{\neq}{\subset} J_1 \underset{\neq}{\subset} J_2 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} J_n$$

que ha de ser finita, por noetherianidad. Luego, para $n >> 0$, J_n es primario y $I = I_1 \cap \cdots \cap I_{n-1} \cap J_n$, que es una intersección de ideales primarios.

Demos otra demostración, menos algorítmica, pero argumentalmente más simple. De acuerdo con el lema anterior, bastará probar que todo ideal I de A es intersección finita de ideales irreducibles.

Si I no es intersección de un número finito de ideales irreducibles entonces $I = I_1 \cap I_2$ con $I \underset{\neq}{\subset} I_1$, $I \underset{\neq}{\subset} I_2$ y I_1 ó I_2 (digamos I_1) no es intersección de un número finito de ideales irreducibles. De nuevo, $I_1 = I_{11} \cap I_{12}$ con $I_1 \underset{\neq}{\subset} I_{11}$, $I_1 \underset{\neq}{\subset} I_{12}$ y I_{11} ó I_{12} (digamos I_{11}) no es intersección de un número finito de ideales irreducibles. Obtenemos así una cadena de inclusiones estrictas

$$I_1 \underset{\neq}{\subset} I_{11} \underset{\neq}{\subset} I_{111} \underset{\neq}{\subset} \cdots$$

lo que contradice la noetherianidad de A. Luego I es intersección de un número finito de ideales irreducibles.

□

5.5 Unicidad en la descomposición primaria

Teorema 5.5.1. *Sea A un anillo y sea $0 = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ una descomposición primaria reducida del ideal 0. Los divisores de cero de A son las funciones que se anulan en alguno de los puntos definidos por los ideales primos asociados $\mathfrak{p}_i = r(\mathfrak{q}_i)$:*

$$\{\textit{Divisores de cero de } A\} = \bigcup_{i=1}^{n} \mathfrak{p}_i$$

Demostración. Sea $a \in A$ un divisor de cero: $ab = 0$ para algún $b \in A$ no nulo. Luego $b \notin \mathfrak{q}_i$ para algún índice i, porque la descomposición primaria es reducida, y concluimos que $a \in r(\mathfrak{q}_i) = \mathfrak{p}_i$.

Recíprocamente, si $a \in \mathfrak{p}_1$, entonces alguna potencia $a^n \in \mathfrak{q}_1$, de modo que $a^n b = 0$ para cualquier $b \in \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_n$ no nulo, y concluimos que a es un divisor de cero. □

Lema 5.5.2. *Sean $\mathfrak{p}_{x_1}, \ldots, \mathfrak{p}_{x_n}$ ideales primos de un anillo A e I un ideal de A. Si*

$$I \subseteq \mathfrak{p}_{x_1} \cup \ldots \cup \mathfrak{p}_{x_n}$$

entonces $I \subseteq \mathfrak{p}_{x_i}$ para algún índice i.

Demostración. Podemos suponer que los $\mathfrak{p}_{x_i} \not\subseteq \mathfrak{p}_{x_j}$ para todo $i \neq j$. Es decir, podemos suponer que $x_i \notin \bar{x}_j$ para todo $i \neq j$. Si $I \not\subseteq \mathfrak{p}_{x_i}$ entonces $x_i \notin (I)_0$ y existe una función f_i que se anula en $(I)_0$ y en todo x_j salvo en x_i. Por tanto, $f = f_1 + \cdots + f_n$ se anula en $(I)_0$ y no se anula en ninguno de los $\{x_i\}_{1 \leq i \leq n}$. Por tanto, tendríamos que $f^n \in I$ y $f^n \notin \mathfrak{p}_{x_i}$ para todo i y $n >> 0$. Contradicción.

□

Teorema 5.5.3 (de unicidad (de los primos asociados)). *Si un ideal I de un anillo A admite una descomposición primaria reducida $I = \cap_i \mathfrak{q}_i$, los ideales primos asociados $\mathfrak{p}_i = r(\mathfrak{q}_i)$ no dependen de la descomposición.*

Demostración. Veamos primero el caso $I = 0$. Sean

$$0 = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \ldots \cap \mathfrak{q}'_m$$

dos descomposiciones primarias reducidas del ideal 0 y sea $\mathfrak{p}$ el ideal primo asociado a una componente de la segunda descomposición. Bastará ver que $\mathfrak{p}$ coincide con $\mathfrak{p}_i = r(\mathfrak{q}_i)$ para algún índice i. Además,

por 5.3.4, localizando en $\mathfrak{p}$ podemos suponer que el anillo A es local y que $\mathfrak{p}$ es su único ideal maximal $\mathfrak{m}$. Ahora, por el teorema anterior

$$\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n = \mathfrak{m}$$

pues ambos términos coinciden con el conjunto de los divisores de cero de A, y concluimos al aplicar el lema anterior.

En el caso de un ideal I arbitrario, cada ideal $\mathfrak{q} \supseteq I$ se corresponde con un ideal $\bar{\mathfrak{q}}$ de A/I, y $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario precisamente cuando $\bar{\mathfrak{q}}$ es un ideal $\bar{\mathfrak{p}}$-primario, porque $A/\mathfrak{q} = (A/I)/\bar{\mathfrak{q}}$ y $\bar{\mathfrak{p}}$ es el radical de $\bar{\mathfrak{q}}$. Por tanto, cada descomposición primaria reducida $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ define una descomposición primaria reducida $0 = \bar{I} = \bar{\mathfrak{q}}_1 \cap \ldots \cap \bar{\mathfrak{q}}_n$ del ideal 0 del anillo A/I. Luego los ideales primos $\bar{\mathfrak{p}}_i$ no dependen de la descomposición y concluimos que los ideales primos $\mathfrak{p}_i$ tampoco. □

Definición 5.5.4. 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.

Teorema 5.5.5 (de unicidad de las componentes no-sumergidas). *Sea I un ideal de un anillo A y sea $\mathfrak{p}_x$ el ideal primo de una componente irreducible de $(I)_0$. Si I admite una descomposición primaria reducida $I = \cap_i \mathfrak{q}_i$, entonces $\mathfrak{p}_x$ es el radical de alguna componente $\mathfrak{q}_i$ y*

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

Luego tal componente $\mathfrak{q}_i$ no depende de la descomposición elegida.

Demostración. Cuando $j \neq i$, tenemos que $\mathfrak{q}_j A_x = A_x$, porque $r(\mathfrak{q}_j)$ corta al sistema multiplicativo $A - \mathfrak{p}_x$ por el que localizamos. Luego

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

y, por 5.3.4, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_x) = A \cap (IA_x)$. □

Sea $I = \cap_i \mathfrak{q}_i$ una descomposición primaria reducida de un ideal I de un anillo A. Según el teorema anterior, si un ideal primo $\mathfrak{p}$ es minimal entre los ideales primos de A que contienen a I, entonces $\mathfrak{p}$ es el radical de alguna componente $\mathfrak{q}_i$ y diremos que $\mathfrak{q}_i$ es una componente no sumergida. Es decir, una componente $\mathfrak{q}_j$ está sumergida cuando sus ceros están contenidos estrictamente en los ceros de alguna otra componente: $\overline{(\mathfrak{q}_j)_0 \subset (\mathfrak{q}_i)_0}$. Las componentes no-sumergidas corresponden a los puntos genéricos de las componentes irreducibles de $(I)_0$ (que de nuevo obtenemos que son un número finito), mientras que las componentes sumergidas están asociadas a puntos más pequeños de $(I)_0$.

Corolario 5.5.6. *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.*

5.6 Una descomposición primaria canónica

Proposición 5.6.1. *Sea $I \subset A$ un ideal y $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria reducida, de primos asociados $r(\mathfrak{q}_i) = \mathfrak{p}_{x_i}$. Dado $\mathfrak{p}_{x_j}$ supongamos reordenando que $\mathfrak{q}_i \subseteq \mathfrak{p}_{x_j}$ si y sólo si $i \leq j$. Se cumple que*

$$A \cap I_{x_j} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

Por tanto, la intersección $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$ no depende de los primarios de la descomposición primaria escogida.

Demostración. $I_{x_j} = \mathfrak{q}_{1,x_j} \cap \cdots \cap \mathfrak{q}_{j,x_j}$. Por tanto,

$$A \cap I_{x_j} = (A \cap \mathfrak{q}_{1,x_j}) \cap \cdots \cap (A \cap \mathfrak{q}_{j,x_j}) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_j$$

□

Corolario 5.6.2. *Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$ dos descomposiciones primarias reducidas, de primos asociados $r(\mathfrak{q}'_i) = r(\mathfrak{q}_i) = \mathfrak{p}_{x_i}$. Se cumple que*

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

para cualquier j. En consecuencia, si $\{\mathfrak{q}''_i\}_{1 \leq i \leq n}$ son ideales $\mathfrak{p}_{x_i}$-primarios que aparecen cada uno en alguna descomposición primaria de I, entonces

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

Demostración. Reordenado, como en la proposición anterior, podemos suponer que $\mathfrak{q}_i \subseteq \mathfrak{p}_{x_j}$ si y sólo si $i \leq j$. Se deduce de la proposición anterior que $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{j-1} = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{j-1}$. Por tanto,

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

Cortando con $\mathfrak{q}_{j+1} \cap \cdots \cap \mathfrak{q}_n$, obtenemos

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

□

Proposición 5.6.3. *Sea A un anillo noetheriano. Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m \subset A$ una descomposición primaria reducida de I. Sea $r(\mathfrak{q}_i) = \mathfrak{p}_{x_i}$. Existe $n_i \in \mathbb{N}$ de modo que $\mathfrak{p}_{x_i}^{n_i} \subseteq \mathfrak{q}_i$. Denotemos por $\mathfrak{p}_i^{n_i}$ el ideal $\mathfrak{p}_{x_i}$-primario antiimagen de $(I_{x_i} + \mathfrak{p}_{x_i}^{n_i}) \cdot A_{x_i}$ en el morfismo de localización $A \to A_{x_i}$, entonces*

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

Demostración. Tenemos $I \subseteq \mathfrak{p}_i^{n_i} \subseteq \mathfrak{q}_i$, por tanto,

$$I = I \cap \mathfrak{q}_1 \cap \cdots \cap \widehat{\mathfrak{q}_i} \cap \cdots \cap \mathfrak{q}_m \subseteq \mathfrak{p}_i^{n_i} \cap \mathfrak{q}_1 \cap \cdots \cap \widehat{\mathfrak{q}_i} \cap \cdots \cap \mathfrak{q}_m \subseteq \mathfrak{q}_i \cap \mathfrak{q}_1 \cap \cdots \cap \widehat{\mathfrak{q}_i} \cap \cdots \cap \mathfrak{q}_m = I$$

luego las inclusiones son igualdades y concluimos.

□

Con palabras, el ideal $\mathfrak{p}_i^{n_i}$ es el ideal de funciones de A cuyos desarrollos de Taylor en x_i hasta orden n_i, son desarrollos de Taylor en x_i, hasta orden n_i, de funciones de I.

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

$$I = \mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_m^{n_m}$$

Demos un método de cálculo. Dado $\mathfrak{p}_{x_j}$, supongamos que ya tenemos calculados los $\mathfrak{p}_i^{n_i}$, cuando $\mathfrak{p}_{x_i} \subset \mathfrak{p}_{x_j}$, reordenando digamos que son $\mathfrak{p}_1^{n_1}, \ldots, \mathfrak{p}_{j-1}^{n_{j-1}}$.

Bien, n_j es el mínimo número natural de modo que $\mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_{j-1}^{n_{j-1}} \cap \mathfrak{p}_j^{n_j} \subseteq I_{x_j}$, que equivale a decir que $(\mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_{j-1}^{n_{j-1}} \cap \mathfrak{p}_j^{n_j})_{x_j} = I_{x_j}$. [1]

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

$$I = \mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_m^{n_m}$$

5.7 Problemas

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

2. 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.

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

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

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

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

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

8. Demostrar que $\prod_{\infty}\mathbb{Z}$ no es un anillo noetheriano.

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

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

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

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

13. Probar que el ideal $(x^2 + y^2 - z^2, y - z) \subset k[x, y, z]$ es primario.

14. Probar que $(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$ es primario pero no irreducible.

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

16. 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?

[1] Equivalentemente, n_j es el mínimo número natural que cumple que $\overline{(\mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_{j-1}^{n_{j-1}})} \cap (\overline{\mathfrak{p}_{x_j}^{n_j}}) \subseteq (\bar{I})$ en $A_{x_j}/\mathfrak{p}_{x_j}^{n_j+1}$.

17. 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.

18. 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 $\mathcal{O}/\mathfrak{m}^{r+1}$.

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

20. 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 $\mathbb{C}[x, y]$.

21. 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.

Capítulo 6

Variedades algebraicas afines

6.1 Introducción

Entendamos ahora 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. En este capítulo probaremos 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.

En este capítulo desarrollaremos la teoría de la dimensión en variedades 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.

6.2 Morfismos finitos

Definición 6.2.1. 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 ($a \cdot b \underset{\text{def}}{=} f(a) \cdot b$). En este caso, también se dice que B es una A-álgebra finita.

Ejemplo 6.2.2. $\mathbb{R} \hookrightarrow \mathbb{C}$ es un morfismo finito.

Proposición 6.2.3. *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,

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

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

□

Proposición 6.2.4. *Sea $A \to B$ un morfismo finito y $A \to C$ un morfismo de anillos. Se verifica que $C = A \otimes_A C \to B \otimes_A C$ es un morfismo finito.*

Corolario 6.2.5. *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*

Definición 6.2.6. Sea $A \to B$ un morfismo de anillos. Se dice que $b \in B$ es entero sobre A si verifica una relación del tipo

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

Proposición 6.2.7. *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. $\Rightarrow$) Sea $b_1, \ldots, b_n$ un sistema generador del A-módulo $A[b]$. Consideremos el endomorfismo de A-módulos

$$\begin{aligned} A[b] &\xrightarrow{\cdot b} A[b] \\ c &\longmapsto c \cdot b \end{aligned}$$

Sea (a_{ij}) una matriz asociada $\cdot b$ en el sistema generador $b_1, \ldots, b_n$. Sea $p_c(x) = |(a_{ij} - x \cdot \mathrm{Id}| = x^n + a_1 x^{n-1} + \cdots + a_n$, con $a_i \in A$. Se verifica que $p_c(\cdot b) = 0$, luego $p_c(b) = p_c(\cdot b)(1) = 0$ y b es entero sobre A.

$\Leftarrow$) Sea $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, con $a_i \in A$, tal que $p(b) = 0$. El epimorfismo $A[x]/(p(x)) \to A[b]$, $q(\bar{x}) \mapsto q(b)$ está bien definido. Por tanto, sólo tenemos que demostrar que $A[x]/(p(x))$ es un A-módulo finito generado.

Veamos que $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ es un sistema generador de $A[x]/(p(x))$ (de hecho, es una base):

$$\begin{aligned} &\bar{x}^n = -(a_1 \bar{x}^{n-1} + \ldots + a_n) \in \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle \\ &\bar{x}^{n+1} = -(a_1 \bar{x}^n + \ldots + a_n \bar{x}) \in \langle \bar{x}, \bar{x}, \ldots, \bar{x}^n \rangle \subseteq \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle \\ &\ldots \end{aligned}$$

□

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

Definición 6.2.8. Dada una extensión de cuerpos $k \to K$ y $\alpha \in K$, decimos que α es algebraico sobre k, si es entero sobre k, que equivale a decir que α es raíz de un polinomio con coeficientes en k.

Ejemplo 6.2.9. Si α es una raíz n-ésima de la unidad, entonces $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ es un morfismo finito.

Ejemplo 6.2.10. 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.

Proposición 6.2.11. *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 6.2.3 $A \to A[b_1, b_2]$ 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. Hemos concluido.

□

Lema 6.2.12. *Sea k un cuerpo. Las k-álgebras finitas íntegras son cuerpos.*

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 inyectivo por la integridad de A. Por tanto, por dimensiones, es isomorfismo. Luego a es invertible y A es cuerpo.

□

Lema 6.2.13. *Sea k un cuerpo. 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 el lema anterior. Por tanto, los ideales primos minimales son maximales y hemos concluido.

□

Corolario 6.2.14. *Sea A una k-álgebra finita y $\{x_1, \dots, x_n\} = \operatorname{Spec} A$. Se cumple que el morfismo natural*

$$A \to A_{x_1} \times \cdots \times A_{x_n}$$

es un isomorfismo. Luego toda k-álgebra finita es un producto de un número finito de k-álgebras finitas locales.

Demostración. Para probar que un morfismo es isomorfismo basta verlo localmente. $(A_{x_1} \times \cdots \times A_{x_n})_{x_i} = A_{x_i}$ porque $(A_{x_j})_{x_i} = 0$ si $i \neq j$ y $(A_{x_i})_{x_i} = A_{x_i}$. Se concluye inmediatamente. □

Lema 6.2.15. *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.*

Demostración. 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. □

Definición 6.2.16. 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 $\dim A$.

Ejercicio 6.2.17. Demostrar que la dimensión de Krull de $\mathbb{C}[x, y]$ es dos.

Teorema 6.2.18. *Si $f\colon A \to B$ es un morfismo finito entonces el morfismo inducido $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación cerrada de fibras de dimensión cero y finitas.*

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

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A/J \cap A & \longrightarrow & B/J \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ (J \cap A)_0 = \operatorname{Spec} A/J \cap A & \xleftarrow{{f^*}_{|C}} & \operatorname{Spec} B/J = C \end{array}$$

Basta ver que ${f^*}_{|C}$ es epiyectiva. Ahora bien, como $A/J \cap A \hookrightarrow B/J$ es un morfismo finito inyectivo, por el lema anterior concluimos que ${f^*}_{|C}$ es epiyectiva.

La fibra de un punto $x \in \operatorname{Spec} A$ es ${f^*}^{-1}(x) = \operatorname{Spec} B_x/\mathfrak{p}_x B_x$. Observemos que si ${f^*}^{-1}(x) \neq \emptyset$ entonces $B_x/\mathfrak{p}_x B_x$ es una $A_x/\mathfrak{p}_x$-álgebra finita. Concluimos por el lema 6.2.13 □

Ejercicio 6.2.19. Probar que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

Teorema 6.2.20 (del ascenso). *Sea $f\colon A \to B$ un morfismo finito. Sean $\mathfrak{p}_x \subset \mathfrak{p}_{x'} \subset A$ y $\mathfrak{p}_y \subset B$ ideales primos, de modo que $f^{-1}(\mathfrak{p}_y) = \mathfrak{p}_x$. Existe un ideal primo $\mathfrak{p}_{y'} \subset B$, de modo que $\mathfrak{p}_y \subset \mathfrak{p}_{y'}$ y $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$.*

Demostración. Por el teorema anterior $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación cerrada. Por tanto, $f^*(\bar{y}) = \bar{x}$. Luego como $x' \in \bar{x}$, existe un $y' \in \bar{y}$ tal que $f^*(y') = x'$. Es decir, $\mathfrak{p}_y \subset \mathfrak{p}_{y'}$ y $f^{-1}(\mathfrak{p}_{y'}) = \mathfrak{p}_{x'}$. □

Corolario 6.2.21. *Si $f\colon A \hookrightarrow B$ es un morfismo finito de modo que $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo (por ejemplo, si f es inyectivo) entonces* $\dim A = \dim B$.

Demostración. Dada una cadena estricta de cerrados irreducibles $\bar{y}_1 \subset \bar{y}_2 \subset \cdots \subset \bar{y}_n$ de $\operatorname{Spec} B$, $\overline{f^*(y_1)} \subset \overline{f^*(y_2)} \subset \cdots \subset \overline{f^*(y_n)}$ es una cadena de cerrados irreducibles estricta de $\operatorname{Spec} A$, pues las fibras son de dimensión cero (6.2.18). Por tanto, $\dim B \leq \dim A$.

Sea ahora una cadena estricta de cerrados irreducibles $\bar{x}_1 \subset \bar{x}_2 \subset \cdots \subset \bar{x}_n$ de $\operatorname{Spec} A$. Sea $y_n \in \operatorname{Spec} B$, tal que $f^*(y_n) = x_n$. Por el teorema del ascenso, existe $y_{n-1} \in \bar{y}_n$ tal que $f^*(y_{n-1}) = x_{n-1}$. Así sucesivamente, obtendremos una cadena estricta de cerrados irreducibles $\bar{y}_1 \subset \bar{y}_2 \subset \cdots \subset \bar{y}_n$ de $\operatorname{Spec} B$ (de imagen por f^*, la cadena de $\operatorname{Spec} A$). Por tanto, $\dim A \leq \dim B$, luego $\dim A = \dim B$. □

Como curiosidad veamos el siguiente ejercicio.

Definición 6.2.22. Sea $\phi\colon X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ un morfismo de variedades. Dado $x \in Y$ denotemos $k(x) = A_x/\mathfrak{p}_x A_x$. Diremos que el número de puntos de la fibra de x es

$$\dim_{k(x)} B_x/\mathfrak{p}_x B_x$$

(Recordemos que la fibra de x es $\operatorname{Spec} B_x/\mathfrak{p}_x B_x$).

Ejercicio 6.2.23. Sea $\operatorname{Spec} A$ una curva íntegra y $\pi\colon \operatorname{Spec} A \to \operatorname{Spec} k[x]$ un morfismo de k-variedades. Se cumple que π es finito $\iff$ el número de puntos de las fibras es finito y constante.

Resolución: $\Rightarrow$) A es un $k[x]$-módulo finito sin torsión, por tanto, por 3.2.4, $A \simeq k[x] \oplus \overset{n}{\cdots} \oplus k[x]$. Dado un punto $x \in \operatorname{Spec} k[x]$, localizando en x, obtenemos $A_x \simeq k[x]_x \oplus \overset{n}{\cdots} \oplus k[x]_x$ Tensorializando por $\otimes_{k[x]_x} k(x)$, obtenemos

$$\dim_{k(x)} A_x/\mathfrak{p}_x A_x = \dim_{k(x)} k(x) \oplus \overset{n}{\cdots} \oplus k(x) = n$$

que no depende del punto x.

$\Leftarrow$) Sea n el número de puntos de cualquier fibra. Dado $x \in \operatorname{Spec} k[x]$, veamos que A_x es un $k[x]_x$-módulo libre de rango n. Sea $m_1, \ldots, m_n \in A_x$, de modo que $\bar{m}_1, \ldots, \bar{m}_n$ sea una base de $A_x/\mathfrak{p}_x A_x$. Tenemos que $\langle m_1, \ldots, m_n\rangle_{k[x]_x}$ es un $k[x]_x$-módulo libre porque es finito y sin torsión; de rango n porque $\langle m_1, \ldots, m_n\rangle/\mathfrak{p}_x\langle m_1, \ldots, m_n\rangle$ es de dimensión n, porque es igual a $A_x/\mathfrak{p}_x A_x$. Dado $m \in A_x$, se cumple que $\langle m_1, \ldots, m_n, m\rangle_{k[x]_x}$ es un módulo libre de rango menor o igual que n, porque localizando en el punto genérico de $k[x]$, g, está incluido en A_g, que es de rango n. Ahora ya, se tiene que $\langle m_1, \ldots, m_n\rangle_{k[x]_x} = \langle m_1, \ldots, m_n, m\rangle_{k[x]_x}$ porque $\bar{m}_1, \ldots, \bar{m}_n$ son linealmente independientes en $\langle m_1, \ldots, m_n, m\rangle/\mathfrak{p}_x\langle m_1, \ldots, m_n, m\rangle$ ya que lo son en $A_x/\mathfrak{p}_x A_x$ y por dimensiones forman una base. Por tanto, $A_x = \langle m_1, \ldots, m_n\rangle_{k[x]_x}$.

Observemos, que $A_g = \langle m_1, \ldots, m_n \rangle_{k[x]_g}$. Dado $\xi \in A$, el polinomio característico del endomorfismo $A_x \xrightarrow{\cdot\xi} A_x$, coincide con el polinomio característico de $A_g \xrightarrow{\cdot\xi} A_g$, para todo $x \in \operatorname{Spec} k[x]$. Por tanto, el polinomio característico tiene coeficientes en $k[x]$, anula a ξ, luego ξ es entero sobre $k[x]$. En conclusión A es un $k[x]$-módulo finito.

Ejercicio 6.2.24. Sean A y B k-álgebras de tipo finito íntegras de dimensión 1, supongamos además que B es anillo de ideales principales. Sea $\pi\colon \operatorname{Spec} A \to \operatorname{Spec} B$ un morfismo de k-variedades. Se cumple que π es finito $\iff$ el número de puntos de las fibras de π es finito y constante.

6.3 Normalización de Noether y ceros de Hilbert

Definición 6.3.1. Sea A una k-álgebra. Diremos que $\xi_1, \ldots, \xi_n \in A$ son algebraicamente independientes sobre k cuando el morfismo de k-álgebras $k[x_1, \ldots, x_n] \to A$, $p(x_1, \ldots, x_n) \mapsto p(\xi_1, \ldots, \xi_n)$ sea 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.

Lema 6.3.2 (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 inyectivo*

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

"Toda variedad algebraica afín se proyecta de modo finito en un espacio afín".

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

Sea r el número máximo de $\{\xi_i\}$ algebraicamente independientes entre sí. Si $r = n$, entonces $k[\xi_1, \ldots, \xi_n] = k[x_1, \ldots, x_n]$. Podemos suponer entonces que ξ_n es algebraico sobre $k[\xi_1, \ldots, \xi_{n-1}]$. Luego existe un $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, donde la variable x_n aparece, de modo 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

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

Así pues, si eligimos $\lambda_1, \ldots, \lambda_{n-1} \in k$ de modo que $p_s(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$, tendremos que ξ_n es entero sobre $k[\xi_1', \ldots, \xi_{n-1}']$. 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 el morfismo finito buscado. □

Definición 6.3.3. Sea A una k-álgebra, diremos que $x \in \operatorname{Spec} A$ es un punto racional si $A/\mathfrak{p}_x = k$.

Proposición 6.3.4. *Sea $A = k[x_1, \ldots, x_n]/I$ e $I = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$. Se cumple que los puntos racionales de* $\operatorname{Spec} A$ *se correspoden biyectivamente con las soluciones del sistema de ecuaciones*

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

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

Demostración. Sea $x \in \operatorname{Spec} k[x_1, \ldots, x_n]$. Si $k[x_1, \ldots, x_n]/\mathfrak{p}_x = k$, entonces $\bar{x}_i = \alpha_i \in k$. Por tanto, $x_i - \alpha_i \in \mathfrak{p}_x$ y se cumple que $\mathfrak{p}_x = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Además, se cumple la inclusión $I = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)) \subseteq \mathfrak{p}_x$ si y sólo si $p_1(\alpha_1, \ldots, \alpha_n) = 0, \ldots, p_m(\alpha_1, \ldots, \alpha_n) = 0$. En conclusión, como los puntos racionales de A, se corresponden con los puntos racionales de $k[x_1, \ldots, x_n]$ que contienen a I, los puntos racionales de A se corresponden biyectivamente con las soluciones del sistema de ecuaciones

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

□

Teorema 6.3.5 (Teorema de los ceros de Hilbert). *Sea $k[\xi_1, \ldots, \xi_n]$ una k-álgebra de tipo finito y $\mathfrak{m}$ un ideal maximal. Entonces $k[\xi_1, \ldots, \xi_n]/\mathfrak{m}$ es una extensión finita de k. En particular, si k es algebraicamente cerrado $k = k[\xi_1, \ldots, \xi_n]/\mathfrak{m}$. "Todo punto cerrado de una variedad algebraica afín sobre un cuerpo algebraicamente cerrado es racional".*

Demostración. Obviamente $k[\xi_1, \ldots, \xi_n]/\mathfrak{m}$ es una k-álgebra de tipo finito sobre k. Por el lema de normalización de Noether, existe un morfismo finito

$$k[x_1, \ldots, x_r] \hookrightarrow k[\xi_1, \ldots, \xi_n]/\mathfrak{m}$$

Por tanto, el término de la izquierda de la flecha ha de tener dimensión cero, luego $r = 0$ y concluimos. □

Ejercicio 6.3.6. Calcular los ideales maximales de $\mathbb{C}[x_1, \ldots, x_n]$ y los de $\mathbb{C}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - 1)$.

Ejercicio 6.3.7. Sean $X = \operatorname{Spec} A$ y $Y = \operatorname{Spec} B$ dos variedades algebraicas sobre un cuerpo algebraicamente cerrado k. Definamos $X \times_k Y \underset{\text{def}}{=} \operatorname{Spec} A \otimes_k B$. Probar que los puntos cerrados de la variedad algebraica $X \times_k Y$ son el producto cartesiano de los puntos cerrados de X pos los de Y.

Proposición 6.3.8. *Sea $f^* \colon X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ un morfismo entre variedades algebraicas afines. La imagen por f^* de un punto cerrado es un punto cerrado.*

Demostración. Dado un punto cerrado $x \in X$ y $f^*(x) = y$, tenemos que $\mathfrak{p}_y = f^{-1}\mathfrak{p}_x$, luego el morfismo $A/\mathfrak{p}_y \hookrightarrow B/\mathfrak{p}_x$ es inyectivo. Por el teorema de los ceros de Hilbert, $B/\mathfrak{p}_x$ es una extensión finita de k, por tanto $A/\mathfrak{p}_y$ también, luego es un cuerpo. Es decir, $f^*(x) = y$ es un punto cerrado. □

Corolario 6.3.9. *Sea $U \subset X$ un abierto de una variedad algebraica afín. Los puntos cerrados de U se corresponden con los puntos cerrados de X que yacen en U.*

Demostración. Sea $x \in U$ un punto cerrado, sea $U_a = \operatorname{Spec} A_a \subset X = \operatorname{Spec} A$ un abierto básico conteniendo a x, tal que $U_a \subseteq U$. Obviamente x es un punto cerrado de U_a. $A_a = A[\frac{1}{a}]$ es una k-álgebra de tipo finito, luego $U_a = \operatorname{Spec} A_a$ es una variedad algebraica. Por la proposición anterior aplicada a la inclusión $U_a \subset X$, tenemos que x es un punto cerrado de X. Hemos concluido. □

Corolario 6.3.10 (forma fuerte de los ceros de Hilbert). *Sea $k[\xi_1, \ldots, \xi_n]$ una k-álgebra de tipo finito y $f \in k[\xi_1, \ldots, \xi_n]$. Si f se anula en todo ideal maximal entonces es nilpotente. En particular, si una función se anula en todos los puntos racionales de una variedad algebraica afín íntegra, sobre un cuerpo algebraicamente cerrado, entonces es nula.*

Demostración. Por el corolario anterior, el conjunto de los ideales maximales de $k[\xi_1,\dots,\xi_n]_f$, se corresponde biyectivamente con el conjunto de los ideales maximales de $k[\xi_1,\dots,\xi_n]$ que no contienen a f. Como este último conjunto es vacío, tenemos que $k[\xi_1,\dots,\xi_n]_f = 0$, es decir, f es nilpotente. □

Definición 6.3.11. Diremos que $X = \operatorname{Spec} A$ es íntegra si A es un anillo íntegro.

Corolario 6.3.12. *Las subvariedades algebraicas íntegras están determinadas por sus puntos cerrados.*

Demostración. Sea $X = \operatorname{Spec} A$ una variedad algebraica y $Y \subseteq X$ una subvariedad algebraica íntegra. Sea $\mathfrak{p}$ el ideal primo de las funciones que se anulan en Y. Basta ver

$$\mathfrak{p} = \bigcap_{\substack{\bar{x}=x \\ \mathfrak{p}\subseteq\mathfrak{m}_x}} \mathfrak{m}_x$$

Obviamente el primer término de la igualdad está incluido en el segundo. Haciendo cociente por $\mathfrak{p}$, tenemos $0 \subseteq \bigcap_{\bar{x}=x} \mathfrak{m}_x$ en $A/\mathfrak{p}$. Por el corolario anterior $\bigcap_{\bar{x}=x} \mathfrak{m}_x$ son los nilpotentes. Ahora bien $A/\mathfrak{p}$ es íntegra, luego $0 = \bigcap_{\bar{x}=x} \mathfrak{m}_x$. Hemos concluido.

□

6.4 Grado de trascendencia y dimensión

Definición 6.4.1. Un morfismo de cuerpos $K \to K'$ diremos que es algebraico, si todo elemento de K' es entero sobre K.

Sea Σ una extensión de un cuerpo k y $\xi_1,\dots,\xi_n \in \Sigma$. Diremos que ξ_n depende algebraicamente de $\xi_1,\dots,\xi_{n-1}$ si ξ_n es entero sobre $k(\xi_1,\dots,\xi_{n-1})$.

Definición 6.4.2. Sea Σ una extensión de un cuerpo k. Diremos que $\xi_1,\dots,\xi_n \in \Sigma$ forman una base de trascendencia de Σ sobre k cuando sean algebraicamente independientes y Σ sea una extensión algebraica de $k(\xi_1,\dots,\xi_n)$; es decir, si son algebraicamente independientes sobre k y todo elemento de Σ depende algebraicamente de $\xi_1,\dots,\xi_n$.

Teorema 6.4.3. *Sea Σ una extensión de un cuerpo k generada por un número finito de elementos. Existen bases de trascendencia de Σ sobre k y todas tienen el mismo número de elementos, llamado grado de trascendencia de Σ sobre k.*

Demostración. Sea $\Sigma = k(\xi_1,\dots,\xi_r)$. Reordenando los generadores si fuera preciso, podemos suponer que $\xi_1,\dots,\xi_n$ son algebraicamente independientes sobre k y ξ_i depende algebraicamente de $\xi_1,\dots,\xi_n$ para todo $n+1 \le i \le r$. Por 6.2.3, $k(\xi_1,\dots,\xi_n,\dots,\xi_r) = \Sigma$ es una extensión algebraica de $k(\xi_1,\dots,\xi_n)$ y concluimos que $\{\xi_1,\dots,\xi_n\}$ es una base de trascendencia de Σ sobre k. Por otra parte, si $\{y_1,\dots,y_m\}$ es otra base de trascendencia de Σ sobre k, probaremos por inducción sobre i que, reordenándola si fuera preciso, Σ es una extensión algebraica de $k(\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m)$. Cuando $i = 0$ es cierto, pues Σ es una extensión algebraica de $k(y_1,\dots,y_m)$. Si $i \ge 1$, por hipótesis de inducción ξ_i es algebraico sobre $k(\xi_1,\dots,\xi_{i-1},y_i,\dots,y_n)$, así que $\xi_1,\dots,\xi_i,y_i,\dots,y_m$ son algebraicamente dependientes sobre k. 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 hipótesis de inducción Σ es algebraico sobre $k(\xi_1,\dots,\xi_i,y_i,\dots,y_m)$ y concluimos que Σ también es algebraico sobre el cuerpo $k(\xi_1,\dots,\xi_i,y_{i+1},\dots,y_m)$. 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 $m \ge n$. Por igual razón $n \ge m$ y $n = m$. □

Ejemplo 6.4.4. Sea k un cuerpo. El cuerpo $k(x_1, \ldots, x_n)$ de las funciones racionales en el espacio afín $\mathbb{A}_n$ tiene grado de trascendencia n, porque las funciones $x_1, \ldots, x_n$ forman claramente una base de trascendencia sobre k.

Ejemplo 6.4.5. Sea $p(x_1, \ldots, x_n)$ un polinomio irreducible con coeficientes en un cuerpo k. Si el grado de p en x_n es ≥ 1, entonces el cuerpo $k(\xi_1, \ldots, \xi_n)$ de las funciones racionales sobre la hipersuperficie $p(x_1, \ldots, x_n) = 0$ tiene grado de trascendencia $n-1$ sobre k, porque una base de trascendencia es $\{\xi_1, \ldots, \xi_{n-1}\}$.

Notación: Denotaremos por $\operatorname{gr\,tr} K$ por el grado de trascendencia de K.

Teorema 6.4.6. *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 de A es cero, entonces éste es una k-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. Así pues podemos suponer que el grado de trascendencia del cuerpo de funciones de A es mayor que cero.

Por el lema de Noether existe un morfismo finito $k[x_1, \ldots, x_n] \hookrightarrow A$. Localicemos en el punto genérico de $k[x_1, \ldots, x_n]$ y escribamos $S = k[x_1, \ldots, x_n] - 0$

$$k(x_1, \ldots, x_n) \overset{\text{finito}}{\hookrightarrow} A_S, \text{ íntegra}$$

Por 6.2.12 el anillo A_S es un cuerpo, luego A_S es el cuerpo de fracciones de A. Por tanto, $\operatorname{gr\,tr} A_S = \operatorname{gr\,tr} k(x_1, \ldots, x_n) = n$. Por otra parte, $\dim k[x_1, \ldots, x_n] = \dim A$, por 6.2.21.

Así pues, podemos suponer que $A = k[x_1, \ldots, x_n]$ y tenemos que ver que su dimensión de Krull es n. Sea

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

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

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

Luego $m - 1 \leq n - 1$. Ahora bien, en $k[x_1, \ldots, x_n]$ hay una cadena de longitud n

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

Luego $n \geq m$. En conclusión $n = m$ es la dimensión de Krull $k[x_1, \ldots, x_n]$. □

Ejercicio 6.4.7. Sean $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $X \times_k Y \overset{\text{def}}{=} \operatorname{Spec} A \otimes_k B$ variedades algebraicas. Demostrar que

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

Ejercicio 6.4.8. Sea $f\colon X \to Y$ un morfismo entre variedades algebraicas. Sea $C \subset X$ un cerrado. Demostrar que

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

6.5 Catenariedad de las variedades algebraicas

Teorema 6.5.1 (del ideal principal de Krull). *Sea $X = \operatorname{Spec} A$ una variedad algebraica íntegra. Sea $f \in A$, no nula y no invertible. Se verifica que la dimensión de toda componente irreducible de $(f)_0$ es $\dim X - 1$.*

Demostración. Podemos suponer que $(f)_0$ sólo tiene una componente irreducible: Sea $(f)_0 = C_1 \cup \cdots \cup C_r$ la descomposición de $(f)_0$ en sus componentes irreducibles. Sea $g \in A$ una función que se anule en $C_2 \cup \cdots \cup C_r$ pero no en C_1. Sea $U = \operatorname{Spec} A - (g)_0 = \operatorname{Spec} A_g$. U es una variedad algebraica íntegra de la misma dimensión que X, ya que tienen el mismo cuerpo de funciones. Además $(f)_{0|U} = C_{1|U}$. Sustituyendo X por U, podemos suponer que $(f)_0$ sólo tiene una componente irreducible.

Sea por el lema de normalización de Noether $k[x_1, \ldots, x_n] \hookrightarrow A$ un morfismo finito inyectivo. Veamos que podemos suponer que A es $k[x_1, \ldots, x_n][f]$: El morfismo $k[x_1, \ldots, x_n][f] \hookrightarrow A$ es un morfismo finito e inyectivo. Denotemos

$$\pi^* \colon \operatorname{Spec} A \to \operatorname{Spec} k[x_1, \ldots, x_n][f] \text{ (finito, y epiyectivo)}$$

el morfismo inducido en los espectros. Se tiene que $\pi^{*-1}((f)_0) = (f)_0$. Por tanto, $\dim (f)_0$ en $\operatorname{Spec} A$ es igual a $\dim (f)_0$ en $\operatorname{Spec} k[x_1, \ldots, x_n][f]$.

Así pues, podemos suponer que $A = k[x_1, \ldots, x_n][f]$. Consideremos el morfismo

$$k[x_1, \ldots, x_n] \hookrightarrow k[x_1, \ldots, x_n][f] \text{ (finito e inyectivo)}$$

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,

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

Sólo nos falta ver la igualdad $*$. Escribamos $p(x_1, \ldots, x_n, 0) = p_1 \cdot \cdots \cdot p_r$ como producto de irreducibles. Tenemos que $\dim (p_i)_0 = \dim k[x_1, \ldots, x_n]/(p_i) = n - 1$ porque el grado de trascendencia del cuerpo de funciones de $k[x_1, \ldots, x_n]/(p_i)$ es $n - 1$. Por tanto,

$$\dim k[x_1, \ldots, x_n]/(p(x_1, \ldots, x_n, 0)) = \dim (p)_0 = \dim (\textstyle\bigcup_i (p_i)_0) = n - 1$$

□

Definición 6.5.2. Una cadena de cerrados irreducibles diremos que es maximal si no está incluida en ninguna otra mayor.

Corolario 6.5.3. *Toda cadena de cerrados irreducibles maximal de una variedad algebraica irreducible tiene la misma longitud.*

Demostración. Sea $X = \operatorname{Spec} A$ la variedad algebraica irreducible. Sea x el punto genérico de X. Obviamente X es homeomorfo como espacio topológico a $\operatorname{Spec} A/\mathfrak{p}_x$. Por tanto, 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. Sea $(f)_0 = Y_1 \cup \cdots \cup Y_r$ la descomposición de $(f)_0$ en cerrados irreducibles, obviamente X_1 aparece. 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 $m = \dim X$.

□

Definición 6.5.4. Se dice que una variedad algebraica es catenaria si toda cadena de cerrados irreducibles maximal con extremos cualesquiera prefijados tiene la misma longitud.

Corolario 6.5.5. *Las variedades algebraicas son catenarias.*

Demostración. Sean $Y \supset Y'$ cerrados irreducibles de una variedad algebraica X. Sea $Y' \supset Y'_1 \supset \cdots \supset Y'_m$ una cadena de cerrados irreducible maximal de Y'. Toda cadena de cerrados irreducibles maximal de extremos Y, Y', junto con esta cadena, define una cadena maximal de Y "ampliada". Como las cadenas "ampliadas" son todas de la misma longitud, por el corolario anterior aplicado a Y, concluimos que toda las cadenas maximales de cerrados irreducibles de extremos Y, Y', tienen la misma longitud.

□

Ejercicio 6.5.6. Sean Y, Y' subvariedades irreducibles de $\mathbb{A}^n$. Supongamos que $Y \cap Y' \neq \emptyset$. Demuéstrese que

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

Ejercicio 6.5.7. Sea $f\colon X \to Y$ un morfismo entre variedades algebraicas irreducibles. Sea $y \in f(X)$ un punto cerrado. Demuéstrese que

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

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

5. Sean X, Y variedades algebraicas íntegras sobre un cuerpo k y sean Σ_X, Σ_Y sus respectivos cuerpos de funciones racionales. Si $\phi\colon Y \to X$ es un morfismo que transforma el punto genérico de Y en el punto genérico de X (lo que equivale a que tenga imagen densa), induce un morfismo de k-álgebras $\Sigma_X \to \Sigma_Y$. Diremos que ϕ es un morfismo de *grado* n cuando Σ_Y sea una extensión finita de grado n de Σ_X. Los morfismos de grado 1 se llaman morfismos birracionales. Diremos que X e Y son birracionalmente equivalentes si sus cuerpos de funciones racionales son extensiones de k isomorfas: $\Sigma_X \simeq \Sigma_Y$. Las variedades algebraicas birracionalmente equivalentes a un espacio afín se llaman racionales. Es decir, una variedad algebraica sobre k es racional si su cuerpo de funciones racionales es isomorfo a un cuerpo de fracciones racionales $k(x_1, \ldots, x_n)$ con coeficientes en k.

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

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

6. 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.

7. 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.

8. Sea $A \to B$ un morfismo de anillos de modo que $B = \cup B_i$, donde B_i son sub-A-álgebras finitas de B (es decir, "$A \to B$ es un morfismo entero"). Probar que el morfismo $\operatorname{Spec} B \to \operatorname{Spec} A$ es cerrado de fibras de dimensión cero.

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

10. Probar que el morfismo $\operatorname{Spec} \mathbb{C}[z] \to \operatorname{Spec} \mathbb{C}[x, y]/(y^2 - x^2 + x^3)$, $\alpha \mapsto (-\alpha^2 + 1, (-\alpha^2 + 1)\alpha)$ es finito.

11. Probar que el morfismo $\phi\colon \mathbb{C}[x, y] \to \mathbb{C}[x, z]$, $\phi(x) = x$, $\phi(y) = xz$, no es finito.

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

13. 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 de las fibras de π es constante.

14. 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.

15. 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 los polinomios en dos variables de grado menor o igual que n son irreducibles.

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

17. Dada una curva plana compleja $p(x, y) = 0$, y un punto de la curva (α, β), diremos que es singular si $\frac{\partial p}{\partial x}(\alpha, \beta) = \frac{\partial p}{\partial y}(\alpha, \beta) = 0$. Demostrar que (α, β) es singular si y sólo si toda recta que pasa por (α, β) corta con multiplicidad mayor que uno a la curva en el punto.

    Si (α, β) es no singular, diremos que la recta $\frac{\partial p}{\partial x}(\alpha, \beta) + \frac{\partial p}{\partial y}(\alpha, \beta) = 0$ es tangente a la curva en (α, β). Demostrar que una recta es tangente en un punto singular (α, β), si y sólo si corta a la curva con multiplicidad mayor que uno en (α, β).

Capítulo 7

Variedades proyectivas

7.1 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 se define el espacio proyectivo asociado a un espacio vectorial como el conjunto de rectas del espacio vectorial (que pasan por el origen). En Geometría Algebraica vamos a definir de modo equivalente a partir de $\mathbb{A}_n = \operatorname{Spec} \mathbb{C}[x_1, \ldots, x_n]$ el espacio proyectivo. Las únicas subvariedades V que queremos considerar en $\mathbb{A}_n$ son las variedades homogéneas, es decir, las que contengan para todo punto cerrado $p \in V$ las rectas que pasan por p y el origen. Así, las subvariedades homogéneas de dimensión menor serán las rectas que pasan por el origen, que se corresponderán con los puntos cerrados del espacio proyectivo que queremos asociarle a $\mathbb{A}_n$.

Si $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ es una función que se anula en la variedad homogénea V, escribamos $p(x_1, \ldots, x_n) = p_s(x_1, \ldots, x_n) + \cdots + p_m(x_1, \ldots, x_n)$ como suma de polinomios homogéneos. Tendremos que

$$p(\lambda x_1, \ldots, \lambda x_n) = \lambda^s p_s(x_1, \ldots, x_n) + \cdots + \lambda^m p_m(x_1, \ldots, x_n) = 0 \text{ en } V \ \forall \ \lambda$$

Por tanto, $p_i(x_1, \ldots, x_n) = 0$ 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 para todo punto cerrado $p = (\alpha_1, \ldots, \alpha_n) \in V$ las rectas que pasan por p y el origen están contenidas en V. En particular, las subvariedades homogéneas $V \subseteq \mathbb{A}_n$ minimales son las rectas que pasan por el origen.

Diremos que el espacio proyectivo $\mathbb{P}_{n-1} = \operatorname{Proj} \mathbb{C}[x_1, \ldots, x_n]$ asociado a $\mathbb{C}[x_1, \ldots, x_n]$ es el subconjunto de $\mathbb{A}_n$ de los ideales primos de $\mathbb{C}[x_1, \ldots, x_n]$ generados por polinomios homogéneos. Si consideramos en $\mathbb{P}_{n-1}$ la topología inducida por $\mathbb{A}_n$, tendremos que los puntos cerrados de $\mathbb{P}_{n-1}$ se

corresponden con las variedades homogéneas de $\mathbb{A}_n$ de dimensión más pequeña, que son justamente las rectas de $\mathbb{A}_n$ que pasan por el origen.

En Geometría Proyectiva se demuestra que $\mathbb{P}_{n-1}$ está recubierto por los subconjuntos $U^h_{x_i} = \{$rectas de $\mathbb{C}^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{C}\}$ 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 $\mathbb{A}_{n-1}$, del modo siguiente: El morfismo

$$\mathbb{A}_n - \{x_i = 0\} \to \mathbb{A}_{n-1}, (\alpha_1, \ldots, \alpha_n) \mapsto (\frac{\alpha_1}{\alpha_i}, \ldots, \frac{\alpha_n}{\alpha_i})$$

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

$$U^h_{x_i} = \{\text{rectas } \lambda(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \neq 0\} \longrightarrow\!\!\!\!\!\!= \mathbb{A}_{n-1}$$

$$\lambda(\alpha_1, \ldots, \alpha_n) \longrightarrow (\tfrac{\alpha_1}{\alpha_i}, \ldots, \tfrac{\alpha_n}{\alpha_i})$$

En Álgebra Conmutativa, se prueba que $U^h_{x_i} = \{\ x \in \operatorname{Proj} \mathbb{C}[x_1, \ldots, x_n]$ que no yacen en $(x_i)_0\}$ se identifica con $\operatorname{Proj} \mathbb{C}[x_1, \ldots, x_n]_{x_i}$; y la composición de los morfismos morfismo

$$U^h_{x_i} \hookrightarrow \mathbb{A}_n - (x_i)_0 \longrightarrow \mathbb{A}_{n-1}$$

$$(\alpha_1, \ldots, \alpha_n) \longrightarrow (\tfrac{\alpha_1}{\alpha_i}, \ldots, \tfrac{\alpha_n}{\alpha_i})$$

$$\mathbb{C}[x_1, \ldots, x_n]_{x_i} \hookleftarrow \mathbb{C}[\tfrac{x_1}{x_i}, \ldots, \tfrac{x_n}{x_i}]$$

induce un homeomorfismo $U^h_{x_i} = \operatorname{Proj} \mathbb{C}[x_1, \ldots, x_n]_{x_i} \simeq \operatorname{Spec} \mathbb{C}[\frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}]$. Además se prueba que $\mathbb{P}_{n-1} = \bigcup_i U^h_{x_i}$.

7.2 Espectro proyectivo

Procedamos con todo rigor y generalidad.

Definición 7.2.1. Diremos que un anillo $R = \bigoplus_{n \in \mathbb{Z}} R_n$ 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 $r_i \cdot r_j \in R_{i+j}$

Definición 7.2.2. Sea $R = \bigoplus_{n \in \mathbb{Z}} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo si está generado por elementos homogéneos, es decir, $I = (i_j)_{j \in J}$ con $i_j \in R_{n_j}$.

Ejercicio 7.2.3. Probar que un ideal $I \subseteq R$ es homogéneo si cumple que si $f = f_s + f_{s+1} + \cdots + f_n \in I$ (f_i elemento homogéneo de grado i) entonces $f_i \in I$ para todo i.

Llamaremos ideal irrelevante de R al ideal $(\bigoplus_{n \geq 0} R_n)$. .

Definición 7.2.4. Llamaremos espectro proyectivo de R, y lo denotaremos $\operatorname{Proj} R$, al conjunto de ideales primos homogéneos 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 $(f)_0^h = (f_n, \ldots, f_m)_0^h = (f_n)_0^h \cap \cdots \cap (f_m)_0^h$. Por tanto, una base de abiertos de la topología de $\operatorname{Proj} R$ son los abiertos

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

Si $f_m \in R_m$ es un elemento homogéneo, entonces R_{f_m} es una álgebra homogénea, diciendo que el grado de $\frac{g_n}{f_m^r} \in R_{f_m}$ es $n - mr$, para cada $g_n \in R_n$.

Definición 7.2.5. Diremos que un morfismo de álgebras $\phi\colon R \to R'$ graduadas es un morfismo graduado de grado $m \in \mathbb{N}$, si para cada $f_n \in R_n$ entonces $\phi(f_n) \in R'_{nm}$.

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 por ϕ no está contenido en más ideal primo homogéneo que los que contengan al irrelevante, tenemos definido un morfismo

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

Ejemplo 7.2.6. Sea $\phi\colon k[x_0, x_1, x_2] \to k[x_0, x_1, x_2]$, $\phi(x_i) = \sum_j \lambda_{ij} x_j$, de modo que $|\lambda_{ij}| \neq 0$. Se cumple que ϕ es un isomorfismo graduado de grado 1, que induce un ismorfismo $\phi^*\colon \mathbb{P}_2 \to \mathbb{P}_2$. Diremos que ϕ es un cambio de coordenadas homogéneo.

Dejamos que el lector demuestre

Proposición 7.2.7. *1. Se cumple que $R \to R_{f_m}$ es un morfismo de grado uno y*

$$U_{f_m}^h = \operatorname{Proj} R_{f_m}$$

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

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

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

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

Teorema 7.2.8. *Se verifica*

1. $\operatorname{Proj} R = \bigcup_{i=0}^{n} (\operatorname{Proj} R - (\xi_i)_0^h)$.

2. $(\operatorname{Proj} R - (\xi_i)_0^h) \underset{*}{\simeq} \operatorname{Spec} R_0[\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}]$, *donde* $\underset{*}{\simeq}$ *es un homeomorfismo.*

Demostración. 1. $\operatorname{Proj} R = \bigcup_{i=0}^{n} U_{\xi_i}^h$, ya que $\bigcap_{i=0}^{n} (\xi_i)_0^h = (\xi_0, \ldots, \xi_n)_0^h = \emptyset$ (pues $(\xi_0, \ldots, \xi_n)$ es el ideal irrelevante).

2. Hemos sobrentendido que $R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$ es el subanillo obvio de $R_0[\xi_0, \ldots, \xi_n]_{\xi_i} = \underset{n\in\mathbb{Z}}{\oplus} \xi_i^n \cdot R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$.

La composición de los dos morfismos naturales $\operatorname{Proj} R_0[\xi_0, \ldots, \xi_n]_{\xi_i} \hookrightarrow \operatorname{Spec} R_0[\xi_0, \ldots, \xi_n]_{\xi_i} \to \operatorname{Spec} R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$, $\mathfrak{p} \longmapsto (\mathfrak{p} \cap R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i])$, va a ser el homeomorfismo buscado.

Es obvio que todo primo homogéneo $\mathfrak{p}$ de $R_0[\xi_0, \ldots, \xi_n]_{\xi_i}$ está determinado por sus elementos homogéneos de grado cero, es decir, por $\mathfrak{p} \cap R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$. Es fácil comprobar que dado un ideal primo $\mathfrak{q} \subset R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$ entonces $\mathfrak{q} \cdot R_0[\xi_0, \ldots, \xi_n]_{\xi_i} = \oplus \xi_i^n \cdot \mathfrak{q}$ es un ideal primo homogéneo de $R_0[\xi_0, \ldots, \xi_n]_{\xi_i}$. Con lo que obtenemos una biyección

$$\operatorname{Proj} R_0[\xi_0, \ldots, \xi_n]_{\xi_i} \overset{*}{=\!=} \operatorname{Spec} R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$$

$$\mathfrak{p} \longrightarrow \mathfrak{p} \cap R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$$

$$\mathfrak{q} \cdot R_0[\xi_0, \ldots, \xi_n]_{\xi_i} \longleftarrow \mathfrak{q}$$

A través de esta identificación $(f_n)_0^h = (f_n/\xi_i^n)_0^h \overset{*}{=} (f_n/\xi_i^n)_0$ en $\operatorname{Spec} R_0[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$. Es decir, $\overset{*}{=}$ es un homeomorfismo.

□

Diremos que $U_{\xi_i}^h$ es un abierto afín de $\operatorname{Proj} R$.

Ejercicio 7.2.9. 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, $U_{\xi_i}^h \simeq (\xi_i - 1)_0$. Probar que $U_{\xi_i}^h \times (\mathbb{A}_1 - \{0\}) = U_{\xi_i}$. Dar una interpretación geométrica de estos resultados.

Ejercicio 7.2.10. Demostrar que el conjunto de puntos cerrados de $\mathbb{P}_n(\mathbb{C}) = \operatorname{Proj} \mathbb{C}[x_0, \ldots, x_n]$ es biyectivo con el conjunto $\mathbb{C}^{n+1}/\sim$, donde $(\alpha_0, \ldots, \alpha_n) \sim (\alpha_0', \ldots, \alpha_n')$ si $(\alpha_0', \ldots, \alpha_n') = (\lambda \cdot \alpha_0, \ldots, \lambda \cdot \alpha_n)$.

Ejercicio 7.2.11.

1. En cada uno de los abiertos "afines" de la curva proyectiva compleja plana $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2)$ complementario de los cerrados $(x_i)_0^h$, escribir las ecuaciones de la curva ("deshomogeneizar").

2. 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 $\operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(x_0^2 + x_1^2 + x_2^2) \hookrightarrow \mathbb{P}_2$

3. 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"?

7.3 Dimensión en variedades proyectivas

Definición 7.3.1. Si $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ diremos que es una variedad proyectiva .

Ejemplo 7.3.2. $\mathbb{P}_1$, $\mathbb{P}_2$, $\mathbb{P}_n = \operatorname{Proj} k[x_0, \ldots, x_n]$. En general, $\operatorname{Proj} k[x_0, \ldots, x_n]/I$, donde I es un ideal homogéneo; recordemos que $(I)_0^h = \operatorname{Proj} k[x_0, \ldots, x_n]/I$.

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 $C = (I)_0^h$. Obviamente, el cierre de C en $\operatorname{Spec} R$, es $\bar{C} = (I)_0$ e I, de nuevo, es el ideal de todas las funciones que se anulan en $(I)_0$. Si C es irreducible entonces su cierre en $\operatorname{Spec} R$ es irreducible y sabemos que $I = \mathfrak{p}_x$ es un ideal primo (homogéneo) y que $(I)_0 = \bar{x}$, luego $C = \bar{x}^h$ (denotamos por $\bar{Y}^h$ al cierre de un conjunto $Y \subseteq \operatorname{Proj} R$ 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. Por tanto, $\operatorname{Proj} R$ es unión de un número finito de cerrados irreducibles y $\operatorname{Proj} R = \bar{x}_1^h \cup \cdots \cup \bar{x}_r^h$, donde $\mathfrak{p}_{x_1}, \dots, \mathfrak{p}_{x_r}$ son los ideales primos homogéneos minimales de R.

Definición 7.3.3. Diremos que la dimensión de $\operatorname{Proj} R$ es la máxima longitud de sus cadenas de cerrados irreducibles, que coincide con la máxima longitud de las cadenas de ideales primos homogéneos de R (donde nunca consideraremos el ideal irrelevante). Si además $\dim X = 1$ diremos que X es una curva proyectiva.

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

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

Ejercicio 7.3.4. Probar que la dimensión de $\mathbb{P}_n$ es n. Probar que la dimensión de la esfera ("completa") $\operatorname{Proj} k[x_0, x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 - x_0^2)$ es dos.

Proposición 7.3.5. *Las variedades proyectivas son catenarias.*

Demostración. Dados dos cerrados irreducibles $\bar{x}_1^h \supset \bar{x}_2^h$, sea $U_{\xi_i}^h$ un abierto afín que contenga a x_2. Para ver que toda cadena maximal de cerrados irreducibles entre $\bar{x}_1^h$ y $\bar{x}_2^h$ tiene la misma longitud podemos restringirnos a $U_{\xi_i}^h$, que es una variedad algebraica afín. Concluimos por 6.5.5.

□

7.4 Intersección de curvas planas. Teorema de Bézout

Definición 7.4.1. 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' es $\dim_k k[x_1, \dots, x_n]/(I + I')$.

Ejercicio 7.4.2. Calcular el número de puntos de corte de la recta $x = 0$, con la curva $y^3+xy+x^3+1 = 0$.

Proposición 7.4.3. *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. Basta probar la exactitud de la sucesión

$$0 \to k[x,y]/(p(x,y),q(x,y)) \xrightarrow{\cdot q'(x,y)} k[x,y]/(p(x,y),q(x,y)\cdot q'(x,y)) \longrightarrow k[x,y]/(p(x,y),q'(x,y)) \to 0$$

Veamos sólo que $\cdot q'(x,y)$ es inyectiva. Si $r(x,y)\cdot q'(x,y)=0$ en $k[x,y]/(p(x,y),q(x,y)\cdot q'(x,y))$, entonces $r(x,y)\cdot q'(x,y) = a\cdot p(x,y)+b\cdot q(x,y)\cdot q'(x,y)$ en $k[x,y]$. Como $p(x,y)$ y $q'(x,y)$ son primos entre si, se cumple que $q'(x,y)$ divide a a y $r(x,y)\in(p(x,y),q(x,y))$, es decir, $r(x,y)=0$ en $k[x,y]/(p(x,y),q(x,y))$.

□

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 $U^h_{x_0}$ 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

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

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 $U^h_{x_0}$ (que contiene a $C\cap C'$) tomado: sea $U^h_{x_1}$ 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 $C\cap C'\cap U^h_{x_0}$, e igualmente $x'=\frac{x_0}{x_1}$ es una función que no se anula en ningún punto de $C\cap C'\cap U^h_{x_1}$, luego

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

Teorema 7.4.4 (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 $(x_0)^h_0$ 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 $(x_0)^h_0\cap C\cap C'=\emptyset$. 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 $p(x_0)=\sum_{i=0}^{s}a_ix_0^i$ y $b=\sum_{i=0}^{r}b_i(x_0,x_1,x_2)$ (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 $B_{x_0}=\bigoplus_{n\in\mathbb{Z}}A\cdot x_0^n$. Denotemos $B^+_{x_0}=\bigoplus_{n\in\mathbb{N}}A\cdot x_0^n$. 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 $B=k[x_0]\oplus\overset{s}{.}\oplus k[x_0]$. 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 $U^h_{\xi_i}=\operatorname{Spec}k[\frac{\xi_1}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$ y podríamos decir que $k[\frac{\xi_1}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$ es el anillo de funciones algebraicas sobre $U^h_{\xi_i}$. 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.

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 6.2.14

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

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

Ejercicio 7.4.5. Calcular la multiplicidad de intersección en el origen de la curva $y^2=x^2+y^3$ con la curva $y^3+x^2=0$.

Proposición 7.4.6. *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,*

$$\dim_k k[x_1,\dots,x_n]/(I+I') = \sum_{x\in C\cap C'} \mu_x(C,C')$$

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.

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 obtenemos 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.

Lema 7.4.7. *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, porque cumple la relación entera

$$\begin{aligned} 0 = \tilde{p}(x,z) = \frac{p(x,y)}{x^r} &= (\frac{y}{x})^r(1+\dot{y}) + \text{ polinomio en } \frac{y}{x} \text{ con coeficientes en } k[x], \text{ de grado } < r \\ &= z^r(1+\dot{y}) + \text{ polinomio en } z \text{ con coeficientes en } k[x], \text{ de grado } < r \end{aligned}$$

donde $1+\dot{y}$ es invertible, porque no se anula en p. 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.

□

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 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.

Proposición 7.4.8. *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*

$$\mu_p(C,C') = \mu_p(C) \cdot \mu_p(C') + \sum_{p_i \in \textit{Fibra excep.}} \mu_{p_i}(\tilde{C}, \tilde{C}')$$

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 7.4.3) 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 lema 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 2. del lema $B/(x) = r$. En conclusión,

$$\mu_p(C,C') = \dim_k A/(q(x,y)) = s \cdot r + \dim_k B/(\tilde{q}(x,z)) = \mu_p(C) \cdot \mu_p(C') + \sum_{p_i \in \text{Fibra excep.}} \mu_{p_i}(\tilde{C}, \tilde{C}')$$

□

Lema 7.4.9. *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

$$\begin{array}{ccc} aA & \hookrightarrow & aB \\ \downarrow & & \downarrow \\ A & \hookrightarrow & B \end{array}$$

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, $\dim_k A/aA = \dim_k B/aB$ □

Ejercicio 7.4.10. 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.

Corolario 7.4.11. *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.*

Corolario 7.4.12. *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. □

Ejercicio 7.4.13. 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.

7.5 Desingularización de curvas planas vía el contacto maximal

Nuestro objetivo es demostrar que dada una curva plana mediante un número finito de explosiones obtenemos una curva sin puntos singulares, i.e., una curva no singular. El número de puntos singulares de una curva plana es finito. Al explotar en un punto singular de multiplicidad μ, la multiplicidad de los puntos de la fibra excepcional es menor que μ, salvo quizás, que sólo aparezca un punto en la fibra excepcional. Tenemos que probar, para demostrar que mediante un número finito de explosiones toda curva plana desingulariza, que después de un número finito de explosiones la multiplicidad baja.

En este apartado vamos a demostrar, dada una curva plana, la existencia de curvas de "contacto maximal". Es decir, dada una curva y un punto p de ella, existe una curva no singular en p, con multiplicidad de corte con la curva dada en p máxima. Esta curva, verificará que pasa por el punto y los puntos de las sucesivas fibras excepcionales (explotando), 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.

Las técnicas e ideas aquí desarrolladas para la desingularización de curvas planas son básicamente las que se utilizan para la desingularización de superficies.

En este apartado supondremos que k es un cuerpo algebraicamente cerrado de característica cero.

Definición 7.5.1. Diremos que la aplicación

$$D\colon k[x,y] \to k[x,y], D(p(x,y)) = a(x,y)p(x,y) + (b(x,y)\frac{\partial}{\partial x} + c(x,y)\frac{\partial}{\partial y})(p(x,y))$$

es un operador diferencial de orden 1.

Lema 7.5.2. *Sea $p(x,y) = 0$ una curva de multiplicidad m en un punto $p \in \mathbb{A}_2$ de la curva y sea $D\colon k[x,y] \to k[x,y]$ un un operador diferencial de orden 1. Entonces la curva $Dp(x,y) = 0$ tiene multiplicidad mayor o igual que $m-1$ en p.*

Demostración. Denotemos $C \equiv p(x,y) = 0$ y $D = a(x,y) + D'$ con $D' = b(x,y)\frac{\partial}{\partial x} + c(x,y)\frac{\partial}{\partial y}$. Se cumple que $\mu_p(C) = m$ 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, $Dp(x,y) = a(x,y)p(x,y) + \sum f_{i_1} \cdots D' f_{i_j} \cdots f_{i_m} \in \mathfrak{m}_p^{m-1}$. Con lo que concluimos. □

Lema 7.5.3. *Con las notaciones anteriores, existe un operador diferencial D de orden 1, 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 $\sum_{r=0}^{m}(m-r)\lambda_r x^r y^{m-r-1} \neq 0$, concluimos que $Dp(x,y)=0$ tiene multiplicidad $m-1$. □

Lema 7.5.4 (fundamental). *Sea $D\colon k[x,y]\to k[x,y]$ un operador diferencial de orden 1. Consideremos el morfismo inyectivo y birracional $k[x,y]\hookrightarrow k[x,z]$, $x\mapsto x, y\mapsto xz$. Existe un operador diferencial de orden 1 $\bar{D}\colon k[x,z]\to k[x,z]$ tal que para todo $P\in k[x,y]$ (de multiplicidad m en el origen) se verifica*

$$\frac{DP}{x^{m-1}} = \bar{D}(\frac{P}{x^m})$$

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 $\bar{D}=x\cdot h$ se cumple la igualdad requerida.
2. Sea D una derivación, es decir $D=b(x,y)\frac{\partial}{\partial x}+c(x,y)\frac{\partial}{\partial y}$. Tenemos que

$$\frac{DP}{x^{m-1}} = (xD)(\frac{P}{x^m}) + (mDx)(\frac{P}{x^m}) = \bar{D}(\frac{P}{x^m})$$

donde $\bar{D}=m\cdot Dx+xD$. Observemos que $\bar{D}$ es un operador diferencial de orden 1 porque $m\cdot Dx$ es una homotecia y xD es una derivación de $k[x,y]_x$ que deja estable a $k[x,z]$, pues $\bar{D}z=\bar{D}(\frac{y}{x})=Dy-\frac{y}{x}Dx=Dy-zDx$.

□

Definición 7.5.5. Sea $p\in C$ y $C_r\to .\overset{\pi}{.}.\to C$ una sucesión de transformaciones cuadráticas. Los puntos de $\pi^{-1}(p)$ se les llamará "puntos de la curva C infinitamente próximos" a p.

Teorema 7.5.6 (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 explosiones) 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. Por el lema fundamental 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 $P/x^m=0$, la explosión de $\tilde{C}\equiv DP=0$ en p tiene de ecuaciones $DP/x^{m-1}=\bar{D}(P/x^m)=0$ (podemos suponer que $x=0$ no es tangente ni a $P=0$ ni a $DP=0$). 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 $P/x^m=0$ y $DP/x^{m-1}=\bar{D}(P/x^m)=0$ concluimos.

Por hipótesis de inducción, existe una curva C' regular en p que pasa (sus explosiones) por todos los puntos infinitamente próximos a $p\in\tilde{C}\equiv DP=0$ de multiplicidad $m-1$. Por tanto, C' (y sus explosiones) pasa por todos los puntos de C infinitesimalmente próximos a p de multiplicidad m.

□

Definición 7.5.7. Diremos que una curva plana $p(x,y)=0$ es reducida si $p(x,y)=p_1(x,y)\cdots p_r(x,y)$, siendo los $p_i(x,y)$ irreducibles y primos entre si.

Proposición 7.5.8. *Toda curva plana reducida tiene un número finito de puntos cerrados singulares.*

Demostración. Los puntos singulares de $p(x,y)=0$, son las soluciones del sistema $p(x,y)=0$, $\frac{\partial p(x,y)}{\partial x}=0$, $\frac{\partial p(x,y)}{\partial y}=0$. Ahora bien, como $p(x,y)=0$ es reducida es fácil ver que $p(x,y)$, $\frac{\partial p(x,y)}{\partial x}$ son primos entre si. Por tanto, el sistema anterior tiene un número finito de soluciones. □

Corolario 7.5.9. *Toda curva plana reducida desingulariza mediante un número finito de transformaciones cuadráticas.*

Demostración. El número de puntos singulares es finito. Sea m la máxima multiplicidad de los puntos de la curva. Sea p un punto de multiplicidad m.

Consideremos una curva $P'=0$, regular en p, que pase por todos los puntos infinitesimalmente próximos a p, de multiplicidad m. Como la multiplicidad de intersección de éstas dos curvas es finita, por 7.4.8, tenemos que después de un número finito de explosiones la multiplicidad de C ha de bajar estrictamente. Fácilmente concluimos por inducción sobre m y el número de puntos de multiplicidad m.

□

7.6 Problemas

1. 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.

2. 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.

3. 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.

4. Probar que el conjunto de curvas de grado n de $\mathbb{P}_2$ se corresponden con los puntos racionales de un espacio proyectivo.

5. 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.

6. 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.

7. Sea $q(x,y)=0$ una cónica y $p=(0,\alpha)$ un punto del plano afín que no yace en la cónica. Demostrar que la proyección de la cónica en la recta $y=0$, que asigna a cada punto q de la cónica el punto de la recta $y=0$ obtenido como el corte de la recta que pasa por p y q con la recta $y=0$, está bien definido si y sólo si la recta $y=\alpha$ es una asíntota horizontal de la cónica.

8. Consideremos el morfismo $\phi\colon k[x_{ijk}]_{i+j+k=2}\to k[x_0,x_1,x_2]$, $\phi(x_{ijk})=x_0^i x_1^j x_2^k$. Probar que induce un morfismo $\phi^*\colon \operatorname{Proj} k[x_0,x_1,x_2]\to \operatorname{Proj} k[x_{ijk}]$. Demostrar que la antimagen de un hiperplano por ϕ^* es una cónica.

9. Demostrar que la circunferencia proyectiva es isomorfa a la recta proyectiva.

10. 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

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

11. Sea $f \in k[\xi_0, \ldots, \xi_n]$ una función homogénea que se anula en algún punto de $X = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$. Demostrar que

$$\dim(f)_0^h \geq \dim X - 1$$

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

13. Probar que si una cúbica plana tiene dos puntos singulares entonces no es irreducible.

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

15. 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).

16. 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.

17. Poner un ejemplo de dos cúbicas planas afines irreducibles, cuyos puntos de corte estén alineados.

Índice de Materias