Álgebra Conmutativa

Simplificada

Diciembre-2003

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

Módulos

1.1 Anillos. Ideales

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

Definición 1.1.1. 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 1.1.2. 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 1.1.3. 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 $a, a' \in A$.

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

3. $f(1) = 1$.

Ejemplo 1.1.4. 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.

Definición 1.1.5. 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 $i \in I$.

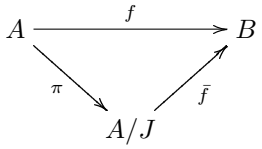
La intersección de ideales es un ideal. Dado un subconjunto $F \subseteq A$, denotaremos por (F) al ideal mínimo de A que contiene a F (que es la intersección de todos los ideales que contienen a F). Explícitamente $(F) = \{a \in A\colon a = \sum_{i=0}^{n} a_i f_i \text{ con } f_i \in F, a_i \in A \text{ y } n \in \mathbb{N} \text{ variables}\}$. 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 antimagen por un morfismo de anillos de un ideal es un ideal. Es inmediata la proposición siguiente.

Proposición 1.1.6. *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 1.1.7. 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 1.1.8. *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 1.1.9. 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 1.1.10. *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 1.1.11. En todo anillo $A \neq 0$ existen ideales primos minimales.

Corolario 1.1.12. *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 1.1.13. *Un ideal* $\mathfrak{m} \subsetneq A$ *es maximal si y sólo si* $A/\mathfrak{m}$ *es un cuerpo. En particular, los ideales maximales son ideales primos, por la proposición* 1.1.8.

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 1.1.14. Se llama espectro primo de un anillo A al conjunto Spec A de sus ideales primos.

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

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,

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

.

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

Teorema 1.1.15. *Existe una correspondencia biunívoca entre los ideales primos de* A_S *y los ideales primos de* A *que no cortan con* S*. Explícitamente, si* $\mathfrak{p}$ *es un ideal primo de* A_S *existe un único ideal primo* $\mathfrak{q}$ *de* A *que no corta con* S*, tal que* $\mathfrak{p} = \mathfrak{q} \cdot A_S$

Demostración. Sea $\mathfrak{p} \subseteq A_S$ un ideal primo. Consideremos el morfismo de localización $A \to A_S$. Sea $\mathfrak{q}$ la antimagen de $\mathfrak{p}$ por el morfismo de localización. Es decir, $\mathfrak{q} := \{a \in A : \frac{a}{1} \in \mathfrak{p}\}$. Es claro que $\mathfrak{p} = \mathfrak{q} \cdot A_S$, pues dado $\frac{a}{s} \in \mathfrak{p}$, $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s}$, y $\frac{a}{1} \in \mathfrak{p}$. Además $\mathfrak{q}$ es un ideal primo de A que no corta con S, porque si $s \in \mathfrak{q} \cap S$ entonces $1 = \frac{s}{s} \in \mathfrak{p}$.

Dado un ideal primo $\mathfrak{q}$ de A que no corta con S, se cumple que $\mathfrak{q} \cdot A_S$ es un ideal primo de A_S: Si $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{q}{s''}$, con $q \in \mathfrak{q}$, entonces existe $t \in S$ de modo que $taa' = tq \in \mathfrak{q}$, luego $a \in \mathfrak{q}$ ó $a' \in \mathfrak{q}$. En conclusión $\frac{a}{s} \in \mathfrak{q} \cdot A_S$ ó $\frac{a'}{s'} \in \mathfrak{q} \cdot A_S$. Además, la antimagen de $\mathfrak{q} \cdot A_S$ por el morfismo de localización es $\mathfrak{q}$: si $\frac{a}{1} = \frac{q}{s}$, con $q \in \mathfrak{q}$, existe $t \in S$ de modo que $ta = tq \in \mathfrak{q}$, luego $a \in \mathfrak{q}$. Obviamente $\frac{a}{1} \in \mathfrak{q} \cdot A_S$, si $a \in \mathfrak{q}$.

Con todo hemos concluido.

□

Notación: Sea A un anillo. Si $f \in A$, denotaremos A_f la localización de A por el sistema multiplicativo $S = \{1, f, f^2, \dots, f^n, \dots\}$. Denotemos por $(f)_0$ el conjunto de los ideales primos de A que contienen a f.

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

Corolario 1.1.16. *El espectro de* A_f *es igual* Spec $A - (f)_0$.

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

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

Ejercicio 1.1.17. 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 1.1.18. *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 1.1.19. Los anillos con un único ideal maximal se les denomina anillos locales.

Definición 1.1.20. 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 1.1.21. *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 pertenece a todo ideal primo.

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 $f^n \cdot 1 = f^n \cdot 0 = 0$. Entonces f es nilpotente. En conclusión $\operatorname{rad} A \supseteq \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$ y hemos terminado. □

1.2 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.

Definición 1.2.1. 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 $A \times M \xrightarrow{\cdot} M$, $(a, m) \mapsto a \cdot m$, cada elemento $a \in A$ define una aplicación $a\cdot\colon M \to M$, $m \mapsto a \cdot m$. El segundo punto expresa que $a\cdot$ es morfismo de grupos. Los tres últimos puntos expresan que la aplicación $\phi\colon A \to \mathrm{End}(M)$, $\phi(a) = a\cdot$, 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 1.2.2.

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 1.2.3. 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 1.2.4. 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

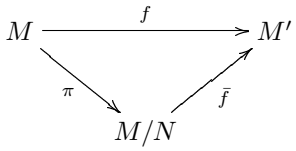
$$M/N = \{\bar{m},\ m \in M \text{ de modo que } \bar{m} = \bar{m'} \iff m - m' \in N\}$$

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 1.2.5. 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 1.2.6. *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 1.2.7 (de isomorfía). *Sea $f\colon M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & M' \\ \Big\downarrow{\scriptstyle \pi} & & \Big\uparrow{\scriptstyle i} \\ M/\operatorname{Ker} f & \xrightarrow{\quad \bar{f} \quad} & \operatorname{Im} f \end{array}$$

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 1.2.8 (de Nakayama). *Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y M un módulo finito generado. Denotemos $\mathfrak{m}M = \{m \in M \colon m = \sum a_i m_i$, 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, $M = \langle m_1, \ldots, m_n \rangle$. □

1.3 Localización de módulos

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

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

Con las operaciones (bien definidas)

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

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

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

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

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

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

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

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

Proposición 1.3.1. *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 1.3.2. 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 1.3.3. *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 1.3.4. 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 1.3.5. 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 $S = A - \mathfrak{p}_x$.

Si $\mathfrak{p}_x$ es un ideal primo maximal diremos que x es un punto cerrado.

Teorema 1.3.6. *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.*

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 $M_S = 0$.

Si $M \neq 0$, entonces existe $m \in M$ no nulo. Sea $I = \text{Anul}\langle m \rangle$ y $\mathfrak{m}_x$ un ideal maximal que contenga a I. Tenemos que $\langle m \rangle_x \neq 0$ por el párrafo anterior. Por tanto, $M_x \neq 0$.

□

Proposición 1.3.7. *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 1.3.8. *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 cerrado $x \in \operatorname{Spec} A$.

Demostración. La implicación $1 \Rightarrow 2$ es un caso particular de 1.3.3.

Veamos que $2 \Rightarrow 1$. 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.

Corolario 1.3.9. *Si $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$, donde $x_1, \ldots, x_n$ son puntos cerrados, entonces*

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

Demostración. El morfismo $A \to A_{x_1} \times \cdots \times A_{x_n}$, $a \mapsto (\frac{a}{1}, \overset{n}{\ldots}, \frac{a}{1})$ es un isomorfismo: Basta verlo al localizar en los x_i. Ahora bien, $(A_{x_i})_{x_j} = 0$ si $x_i \neq x_j$, porque los ideales primos de $(A_{x_i})_{x_j}$ se corresponden con los ideales primos de A que están contenidos en $\mathfrak{m}_{x_i}$ y $\mathfrak{m}_{x_j}$, es decir es vacío, luego $(A_{x_i})_{x_j} = 0$. Por último $(A_{x_i})_{x_i} = A_{x_i}$, porque en el primer término de la igualdad localizamos por invertibles de A_{x_i}. □

1.4 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 1.4.1. 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 1.4.2. 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 1.4.3. 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 1.4.4. *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 1.4.5. *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

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

Definición 1.4.6. Llamaremos soporte de un módulo M al conjunto de ideales primos $\mathfrak{p}_x$ tales que $M_x \neq 0$.

Proposición 1.4.7. *Si* M *es de longitud finita, entonces* $\operatorname{Sop}(M)$ *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 dado $s \in \mathfrak{m}_x \cap (A - \mathfrak{p}_{x'}) \neq 0$, tenemos que $A/mm_x = \frac{s}{s} \cdot A/\mathfrak{m}_x = 0$.

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

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 $x \in \operatorname{Spec} A$ distinto de los x_i. Luego $M_x = (M_n)_x = \cdots = (M_0)_x = 0$, para todo punto $x \in \operatorname{Spec} A$ distinto de los x_i. En conclusión, el soporte de M es subconjunto de $\{x_i\}$ y hemos terminado.

□

1.5 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 $f^{-1}(m') = m + \operatorname{Ker} f \underset{\text{def}}{=} \{m + n$ con $n \in \operatorname{Ker} f\}$. Sea N un submódulo de M, probar que $f^{-1}(f(N)) = N + \operatorname{Ker} f$.

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

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

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

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 $M = \underset{0 \neq n \in \mathbb{Z}}{\oplus} \mathbb{Z}/n\mathbb{Z}$. 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 $\operatorname{Anul}(M) = \underset{i}{\cap} \operatorname{Anul}(M_i)$. 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 $(\operatorname{Anul}_A(M))_S = \operatorname{Anul}_{A_S}(M_S)$, 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 $x \in \operatorname{Spec} A$, 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 2

Módulos sobre dominios de ideales principales

2.1 Dominios de ideales principales

Definición 2.1.1. 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 2.1.2. 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 2.1.3 (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 2.1.4. 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 2.1.5 (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 2.1.6. *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 2.1.7. *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 2.1.8 (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. Supongamos que a no es producto de factores irreducibles. Si así es, entonces a es producto de dos factores propios y uno de ellos, llamémoslo a_1 no es producto de factores irreducibles. Del mismo modo tenemos que a_1 es producto de dos factores propios y uno de ellos, llamémoslo a_2 no es producto de factores irreducibles. Así sucesivamente, vamos obteniendo una cadena $(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} ldots$ lo que contradice la proposición anterior.

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). □

2.2 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 2.2.1. 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 2.2.2. 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 2.2.3. 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 2.2.4. *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 2.2.5. *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 2.2.4. 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 1.2.5 $M = L' \cap M \oplus \pi(M)$. En conclusión, M es libre. □

Teorema 2.2.6 (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 2.2.7. *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*

$$M = \mathrm{Ker}\, p \oplus \mathrm{Ker}\, q$$

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 $\lambda pm \in \mathrm{Ker}\, q$ y $\mu qm \in \mathrm{Ker}\, p$. Por consiguiente $M = \mathrm{Ker}\, p + \mathrm{Ker}\, q$.

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 2.2.8 (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 2.2.9. *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 2.2.10 (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 2.2.11 (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 2.2.12. A las potencias $p_i^{n_{i,j}}$ del teorema de clasificación se les denomina divisores elementales de M.

Corolario 2.2.13. *Dos módulos finito generados son isomorfos si y sólo si tienen el mismo rango y los mismos divisores elementales.*

Ejercicio 2.2.14. Dos módulos finito generados sobre un dominio de ideales principales son isomorfos si y sólo si son localmente isomorfos.

Ejercicio 2.2.15. Probar que en el caso de que $r = 0$ entonces $\mathrm{Anul}(M) = m.c.m.\{p_i^{n_{i,j}}\}_{i,j}A$.

2.3 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

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

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

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

Teorema 2.3.1 (de clasificación). *Sea G un grupo abeliano finito generado. Existe un isomorfismo de grupos*

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

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

Ejercicio 2.3.3. Probar que $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

2.4 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 $E \overset{x\cdot}{\to} E$, $e \mapsto x \cdot e$. Cuando pensemos E con la estructura de $k[x]$-módulo inducida por el endomorfismo T, lo escribiremos E_T.

Definición 2.4.1. 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 2.4.2. *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 2.4.3. *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 2.4.4. *Dos endomorfismos de un espacio vectorial de dimensión finita son equivalentes si y sólo si poseen los mismos divisores elementales.*

2.4.1 Matrices de Jordan

1. Caso de un cuerpo k algebraicamente cerrado

Lema 2.4.5. *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 $\sum_{i=0}^{n-1} \lambda_i x^i = \dot{p(x)}$. 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 2.4.6. $\{\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)}^{n-1}\}$ *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

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

(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 2.4.7. *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 2.4.8. *Sea E un espacio vectorial sobre $\mathbb{C}$, de base $\{e_1, \dots, e_n\}$. 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 $\{e_1, ie_1, \dots, e_n, ie_n\}$ es*

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

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 2.4.9. *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 $\mathbb{C}$, $\bar{1}, \overline{(x-\alpha)}, \dots, \overline{(x-\alpha)}^{n-1}$ 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

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

2.5 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 2.5.1. 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 2.5.2. 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 2.5.3 (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 2.2.9 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 2.5.4. 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 2.5.5 (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

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

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 2.5.6. *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 $xId - (\lambda_{ij})$.

2.6 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

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

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

(b) Pruébese este resultado como caso particular de 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 3

Producto tensorial. Módulos proyectivos e inyectivos

3.1 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 3.1.1. 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 3.1.2. 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 3.1.3. 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 3.1.4. *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

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

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 3.1.5. 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 3.1.6. *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 3.1.7. *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 $\operatorname{Ker} p = p^{-1}(0) \subseteq (f \circ p)^{-1}(0) = \pi^{-1}(0) = \operatorname{Im} i$. □

3.2 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 3.2.1. 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 3.2.2. 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 3.2.3 (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 3.2.4. 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

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

3.3 Propiedades del producto tensorial

Teorema 3.3.1. *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 (3.1.4), $(\underset{i\in I}{\oplus} M_i)\otimes_A N = \underset{i\in I}{\oplus}(M_i\otimes N)$.

□

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 3.3.2. *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 3.3.3. *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 3.1.7

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

es una sucesión exacta para todo A-módulo P. De nuevo 3.1.7 nos permite concluir que la sucesión $M^{\cdot}\otimes_A N$ es exacta. □

3.4 Producto exterior

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

Definición 3.4.1. Si $A \to B$ es un morfismo de anillos se dice que B es una A-álgebra.

Definición 3.4.2. 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 3.4.3. 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 3.4.4. *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 3.4.5. 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 3.4.6. *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 3.4.7. 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".

3.5 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 3.5.1. 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 3.5.2. *Sean B, C y D A-álgebras. Se cumple el isomorfismo*

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

Proposición 3.5.3. *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 3.5.4. 1. Con las notaciones obvias, pruébese que

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

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

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 3.4.4, 3.4.6, o de 1.

3.6 Módulos planos y proyectivos

Definición 3.6.1. 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 3.3.3, 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 3.6.2. *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 3.6.3. *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 $(N^{\cdot} \otimes_A P)_x = N_x^{\cdot} \otimes_{A_x} P_x$ es exacta $\iff$ P_x es un A_x-módulo plano para todo punto cerrado $x \in \operatorname{Spec} A$ □

Lema 3.6.4. *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 3.6.5 (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 3.6.6. *Un A-módulo finito generado es plano si y sólo si es localmente libre.*

Demostración. Es consecuencia inmediata de 3.6.3 y 3.6.4. □

Definición 3.6.7. 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 3.1.6), 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 3.6.8. *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 1.2.5, $A^{(I)} = \operatorname{Ker}\pi \oplus P$.

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

Proposición 3.6.9. *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 3.6.10. 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 3.6.11. *Sea M un A-módulo de presentación finita y $S \subset A$ un sistema multiplicativo. Entonces para todo A-módulo N se cumple que*

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

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

Por hipótesis tenemos una sucesión exacta $A^m \to A^n \to M \to 0$. 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

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

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 $\operatorname{Ker} = \mathrm{Hom}_{A_S}(M_S, N_S)$ y terminamos.

□

Teorema 3.6.12. *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 $x \in \operatorname{Spec} A$ 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 $x \in \operatorname{Spec} A$ $\iff$ 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 3.6.13. *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 3.6.6.

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

Si M es proyectivo por 3.6.9 es plano. □

3.7 Módulos inyectivos. Criterio del ideal para módulos inyectivos

Definición 3.7.1. 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 3.7.2 (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 3.7.3. 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 3.7.4. *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.

3.7.1 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

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

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

Si consideramos una sucesión exacta

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

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

Lema 3.7.5. *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 $\text{Hom}_{\mathbb{R}}(-,\mathbb{R})$ 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 $\text{Hom}_k(A,k)$ es inyectivo.

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

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

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

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

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

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

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

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

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

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

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

3.8 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 $M_1, \ldots, M_n$ son A-módulos libres finito generados probar que $M_1^* \otimes_A \cdots \otimes_A M_n^* = Multil_A(M_1, \ldots, M_n; A)$.

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.

Índice de Materias