

# Capítulo 1

## Módulos

### 1.1. Módulos

**Axiomas de módulo:** Sea  $A$  un anillo (conmutativo y con unidad) y sea  $M$  un conjunto. Diremos que una operación  $M \times M \xrightarrow{+} M$  y una aplicación  $A \times M \xrightarrow{\cdot} M$  definen en  $M$  una estructura de  **$A$ -módulo** cuando

*Axioma 1:*  $(M, +)$  es un grupo conmutativo.

*Axioma 2:*  $a \cdot (m + n) = a \cdot m + a \cdot n$

*Axioma 3:*  $(a + b) \cdot m = a \cdot m + b \cdot m$

*Axioma 4:*  $(ab) \cdot m = a \cdot (b \cdot m)$

*Axioma 5:*  $1 \cdot m = m$

Es decir, dada una aplicación  $A \times M \rightarrow M$ , cada elemento  $a \in A$  define una aplicación  $a \cdot : M \rightarrow M$  y el segundo axioma expresa que  $a \cdot$  es morfismo de grupos. Los tres últimos axiomas expresan que la aplicación  $\phi: A \rightarrow \text{End}(M)$ ,  $\phi(a) = a \cdot$ , es morfismo de anillos. Recíprocamente, si  $M$  es un grupo abeliano, cada morfismo de anillos  $\phi: A \rightarrow \text{End}(M)$  define una estructura de  $A$ -módulo en  $M$  tal que  $a \cdot m = \phi(a)(m)$ . Resumiendo, dar una estructura de  $A$ -módulo en un grupo abeliano  $M$  es dar un morfismo de anillos de  $A$  en el anillo (no conmutativo en general) de los endomorfismos del grupo  $M$ . *Los  $A$ -módulos son las representaciones de  $A$  como anillo de endomorfismos de un grupo abeliano.*

**Definición:** Una aplicación  $f: M \rightarrow N$  entre dos  $A$ -módulos es un **morfismo** de  $A$ -módulos cuando es un morfismo de grupos y conserva el producto por elementos de  $A$ :

$$\begin{aligned}f(m + m') &= f(m) + f(m') \\f(a \cdot m) &= a \cdot f(m)\end{aligned}$$

Diremos que un morfismo de  $A$ -módulos  $f: M \rightarrow N$  es un **isomorfismo** de  $A$ -módulos si existe algún morfismo de  $A$ -módulos  $h: N \rightarrow M$  tal que  $f \circ h = Id_N$  y  $h \circ f = Id_M$ .

La composición de morfismos de  $A$ -módulos también es morfismo de  $A$ -módulos, la identidad siempre es morfismo de  $A$ -módulos, y los isomorfismos de  $A$ -módulos son los morfismos biyectivos.

**Definición:** Sea  $M$  un  $A$ -módulo. Diremos que un subgrupo  $N$  de  $M$  es un **submódulo** si es estable por el producto por elementos de  $A$ ; i.e.,  $a \in A$ ,  $m \in N \Rightarrow am \in N$ .

En tal caso  $N$  hereda una estructura de  $A$ -módulo.

Si  $f: M \rightarrow N$  es un morfismo de  $A$ -módulos, su núcleo  $\text{Ker } f$  es un submódulo de  $M$  y su imagen  $\text{Im } f$  es un submódulo de  $N$ .

$M$  y  $0$  son submódulos de  $M$ . Además, la intersección de cualquier familia de submódulos de  $M$  también es un submódulo de  $M$ . Por tanto, dada una familia  $\{m_i\}_{i \in I}$  de elementos de  $M$ , la intersección de todos los submódulos de  $M$  que la contengan es el menor submódulo de  $M$  que la contiene y recibe el nombre de submódulo **generado** por tal familia. Claramente es el submódulo de  $M$  formado por las combinaciones lineales finitas con coeficientes en  $A$  de elementos de la familia  $\{m_i\}_{i \in I}$  dada, y se denotará  $\sum_{i \in I} Am_i$ .

### Ejemplos:

1. Si  $k$  es un cuerpo, los  $k$ -módulos son los  $k$ -espacios vectoriales, y los morfismos de  $k$ -módulos son las aplicaciones  $k$ -lineales.
2. Cada grupo abeliano  $(M, +)$  admite una única estructura de  $\mathbb{Z}$ -módulo. En efecto, si  $n \in \mathbb{N}$ , basta poner

$$nm := m + \dots + m \quad , \quad (-n)m := (-m) + \dots + (-m)$$

3. Sea  $E$  un espacio vectorial sobre un cuerpo  $k$ . Cada endomorfismo  $k$ -lineal  $T: E \rightarrow E$  define una estructura de  $k[x]$ -módulo en  $E$ :

$$(a_n x^n + \dots + a_1 x + a_0)e := a_n T^n(e) + \dots + a_1 T(e) + a_0 e$$

y los submódulos de  $E$  son los subespacios vectoriales  $V \subseteq E$  invariantes:  $T(V) \subseteq V$ .

4. Cada anillo  $A$  es claramente un  $A$ -módulo, y sus submódulos son precisamente los ideales de  $A$ . Se dice que un ideal  $I$  de  $A$  es **principal** cuando está generado por un elemento:  $I = aA$ . Diremos que un anillo  $A$  es un **dominio de ideales principales** cuando es íntegro y todos los ideales son principales. Por ejemplo,  $\mathbb{Z}$  y  $k[x]$  (al igual que todo anillo euclídeo) lo son.
5. Sea  $M$  un  $A$ -módulo. Cada  $a \in A$  induce un morfismo de  $A$ -módulos  $M \xrightarrow{a} M$ ,  $m \mapsto am$ ; y cada  $m \in M$  induce un morfismo de  $A$ -módulos  $A \xrightarrow{m} M$ ,  $a \mapsto am$ .
6. Sea  $M$  un  $A$ -módulo y  $\mathfrak{a}$  un ideal de  $A$ . El submódulo de  $M$  generado por los productos  $am$ , donde  $a \in \mathfrak{a}$  y  $m \in M$ , se denota  $\mathfrak{a}M$ . Los elementos de  $\mathfrak{a}M$  son las combinaciones lineales finitas  $a_1 m_1 + \dots + a_n m_n$  de elementos de  $M$  con coeficientes en  $\mathfrak{a}$ .
7. 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 subgrupo de  $\prod_{i \in I} M_i$  formado por los elementos  $(m_i)$  que tienen todas sus componentes  $m_i$  nulas salvo un número finito y se llamará **suma directa** de tal familia (nótese que  $\bigoplus_i M_i = \prod_i M_i$  cuando el conjunto de índices es finito). Tanto la suma directa  $\bigoplus_i M_i$  como el producto directo  $\prod_i M_i$  son  $A$ -módulos con el siguiente producto por elementos de  $A$ :

$$a \cdot (m_i)_{i \in I} = (am_i)_{i \in I}$$

Si todos los módulos  $M_i$  son iguales a cierto módulo  $M$ , el producto directo  $\prod_i M_i$  se denota  $M^I = \prod_I M$  y la suma directa  $\bigoplus_i M_i$  se denota  $M^{(I)} = \bigoplus_I M$ . Cuando el conjunto  $I$  es finito y de cardinal  $n$ , ambos módulos coinciden y se denotan  $M^n$ .

## Módulo Cociente

Si  $N$  es un submódulo de un  $A$ -módulo  $M$ , es un subgrupo normal de  $M$ . Es sencillo comprobar que en el grupo cociente  $M/N$  existe una única estructura de  $A$ -módulo tal que la

proyección canónica  $\pi: M \rightarrow M/N$ ,  $\pi(m) = [m]$ , sea morfismo de  $A$ -módulos. Tal estructura viene definida por el producto

$$a \cdot [m] = [am]$$

La demostración de la propiedad universal del  $A$ -módulo cociente  $M/N$ , y la del correspondiente teorema de isomorfía, es similar a la dada para morfismos de grupos y anillos:

**Propiedad universal del módulo cociente:** Sea  $N$  un submódulo de un  $A$ -módulo  $M$  y sea  $\pi: M \rightarrow M/N$  la proyección canónica. Si un morfismo de  $A$ -módulos  $f: M \rightarrow M'$  se anula en  $N$ , entonces existe un único morfismo de  $A$ -módulos  $\varphi: M/N \rightarrow M'$  tal que  $f = \varphi \circ \pi$ ; es decir,  $\varphi([m]) = f(m)$ .

**Teorema de Isomorfía:** Sea  $f: M \rightarrow N$  un morfismo de  $A$ -módulos. Tenemos un isomorfismo de  $A$ -módulos:

$$\phi: M/\text{Ker } f \longrightarrow \text{Im } f \quad , \quad \phi([m]) = f(m)$$

**Teorema 1.1.1** Sea  $M$  un  $A$ -módulo y sea  $\pi: M \rightarrow M/N$  la proyección canónica en el cociente por un submódulo  $N$ . Si  $\bar{P}$  es un submódulo de  $M/N$ , entonces  $\pi^{-1}(\bar{P})$  es un submódulo de  $M$  que contiene a  $N$ . Tenemos así una biyección que conserva inclusiones

$$\left[ \begin{array}{c} \text{Submódulos} \\ \text{de } M/N \end{array} \right] = \left[ \begin{array}{c} \text{Submódulos de } M \\ \text{que contienen a } N \end{array} \right]$$

*Demostración:* Es claro que  $\pi^{-1}(\bar{P})$  es un submódulo de  $M$  que contiene a  $\text{Ker } \pi = N$  y que  $\pi^{-1}(\bar{P}_1) \subseteq \pi^{-1}(\bar{P}_2)$  cuando  $\bar{P}_1 \subseteq \bar{P}_2$ . Por tanto, basta probar que la aplicación así obtenida del conjunto de los submódulos de  $M/N$  en el de los submódulos de  $M$  que contienen a  $N$  es biyectiva. La aplicación inversa asigna a cada submódulo  $P$  de  $M$  que contenga a  $N$  el submódulo  $\pi(P)$  de  $M/N$ . En efecto:

Si un submódulo  $P$  de  $M$  contiene a  $N$ , entonces

$$P \subseteq \pi^{-1}(\pi(P)) \subseteq P + N \subseteq P$$

y  $P = \pi^{-1}(\pi(P))$ . Recíprocamente, si  $\bar{P}$  es un submódulo de  $M/N$ , entonces  $\pi(\pi^{-1}(\bar{P})) \subseteq \bar{P}$  y se da la igualdad porque  $\pi$  es epiyectivo.

**Corolario 1.1.2** Sea  $\mathfrak{a}$  un ideal de un anillo  $A$  y sea  $\bar{A} = A/\mathfrak{a}$ . La proyección canónica  $\pi: A \rightarrow \bar{A}$  establece una correspondencia biyectiva, que conserva inclusiones, entre los ideales de  $\bar{A}$  y los ideales de  $A$  que contienen a  $\mathfrak{a}$ . Además, si  $\bar{\mathfrak{b}}$  es el ideal de  $\bar{A}$  correspondiente a un ideal  $\mathfrak{b} \supseteq \mathfrak{a}$ , entonces

$$A/\mathfrak{b} \simeq \bar{A}/\bar{\mathfrak{b}}$$

En particular, ideales primos se corresponden con ideales primos e ideales maximales con ideales maximales.

*Demostración:* La primera parte es consecuencia del teorema anterior, pues los submódulos del  $A$ -módulo  $A/\mathfrak{a}$  son sus ideales.

En cuanto al isomorfismo  $A/\mathfrak{b} \simeq \bar{A}/\bar{\mathfrak{b}}$ , el morfismo de anillos natural  $A \rightarrow \bar{A}/\bar{\mathfrak{b}}$  es epiyectivo y su núcleo es precisamente el ideal  $\mathfrak{b} = \pi^{-1}(\bar{\mathfrak{b}})$ . Concluimos al aplicar el teorema de isomorfía para morfismos de anillos.

**Teorema 1.1.3** Todo anillo no nulo tiene algún ideal maximal.

*Demostración:* Sea  $A$  un anillo y sea  $X$  el conjunto de sus ideales distintos de  $A$ , ordenado por inclusión. Si  $\{\mathfrak{a}_i\}_{i \in I}$  es una cadena de elementos de  $X$ , entonces  $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$  es claramente un ideal  $\neq A$  que contiene a todos los ideales  $\mathfrak{a}_i$ . Es decir, toda cadena de  $X$  admite una cota superior. Si  $A \neq 0$ , entonces  $X$  no es vacío y el lema de Zorn afirma que  $X$  tiene algún elemento maximal, que es un ideal maximal de  $A$ .

**Teorema 1.1.4** *Sea  $\mathfrak{a}$  un ideal de un anillo  $A$ . Si  $\mathfrak{a} \neq A$ , entonces  $\mathfrak{a}$  está contenido en algún ideal maximal de  $A$ .*

*Demostración:* Si  $\mathfrak{a} \neq A$ , entonces  $A/\mathfrak{a} \neq 0$  y, por 1.1.3, el anillo  $A/\mathfrak{a}$  tiene algún ideal maximal que, según 1.1.2, se corresponde con un ideal maximal de  $A$  que contiene a  $\mathfrak{a}$ .

**Corolario 1.1.5** *La condición necesaria y suficiente para que un elemento de un anillo  $A$  sea invertible es que no pertenezca a ningún ideal maximal de  $A$ .*

*Demostración:* Sea  $f$  un elemento de un anillo  $A$ . Si  $f$  pertenece a un ideal maximal, claramente no puede ser invertible en  $A$ . Recíprocamente, si  $f$  no es invertible en  $A$ , entonces  $fA \neq A$  y, según 1.1.4, el ideal  $fA$  está contenido en algún ideal maximal de  $A$ .

## Módulos Libres

Cada familia  $\{m_i\}_{i \in I}$  de elementos de un  $A$ -módulo  $M$  define un morfismo de  $A$ -módulos  $f: \bigoplus_I A \rightarrow M$

$$\phi((a_i)_{i \in I}) := \sum_{i \in I} a_i m_i$$

y diremos que forman un **sistema de generadores** de  $M$  cuando  $M = \sum_i A m_i$ ; es decir, cuando el correspondiente morfismo  $\phi: A^{(I)} \rightarrow M$  sea epiyectivo. Diremos que forman una **base** de  $M$  cuando  $\phi$  sea un isomorfismo; es decir, cuando cada elemento de  $M$  descomponga, y de modo único, como combinación lineal con coeficientes en  $A$  de los elementos  $\{m_i\}_{i \in I}$ .

Todo módulo admite sistemas de generadores (la familia formada por todos sus elementos, etc.); pero existen módulos que no tienen ninguna base. Por ejemplo, ningún grupo abeliano finito no nulo tiene bases.

**Definición:** Diremos que un  $A$ -módulo es de **tipo finito** si admite algún sistema finito de generadores; es decir, si es isomorfo a un cociente de alguna suma directa finita  $A^n$ .

Diremos que un  $A$ -módulo es **libre** si admite alguna base; es decir, si es isomorfo a alguna suma directa  $A^{(I)}$ . Cuando  $A \neq 0$ , veremos a continuación que todas las bases de un  $A$ -módulo libre  $L$  tienen el mismo cardinal, que se llamará **rango** de  $L$ .

Sea  $I$  un ideal de un anillo  $A$ .

Si  $M$  es un  $A$ -módulo, en  $M/IM$  tenemos una estructura natural de  $(A/I)$ -módulo,  $[a] \cdot [m] := [am]$ , pues es sencillo comprobar que tal producto no depende de los representantes  $a$  y  $m$  elegidos.

Ahora, si  $f: M \rightarrow N$  es un morfismo de  $A$ -módulos, entonces  $f(IM) \subseteq IN$ , de modo que el morfismo  $M \rightarrow N/IN$ ,  $m \mapsto [f(m)]$ , se anula en  $IM$ , y la propiedad universal del módulo cociente afirma la existencia de un único morfismo de  $A$ -módulos  $\bar{f}: M/IM \rightarrow N/IN$  tal que  $\bar{f}([m]) = [f(m)]$ . De hecho  $\bar{f}$  es un morfismo de  $(A/I)$ -módulos.

**Lema 1.1.6** *Sea  $A$  un anillo no nulo. Si existe algún morfismo epiyectivo de  $A$ -módulos  $A^{(I)} \rightarrow A^{(J)}$ , entonces el cardinal de  $I$  es mayor o igual que el cardinal de  $J$ . En particular todas las bases de un  $A$ -módulo libre tienen el mismo cardinal.*

*Demostración:* Sea  $\mathfrak{m}$  un ideal maximal de  $A$  y  $k = A/\mathfrak{m}$  su cuerpo residual. Nótese que  $\mathfrak{m} \cdot A^{(I)} = \mathfrak{m}^{(I)}$  y que  $A^{(I)}/\mathfrak{m}A^{(I)} \simeq (A/\mathfrak{m})^{(I)} = k^{(I)}$ . Si algún morfismo de  $A$ -módulos  $\varphi: A^{(I)} \rightarrow A^{(J)}$  es epiyectivo, también lo será el morfismo

$$\bar{\varphi}: A^{(I)}/\mathfrak{m}A^{(I)} \rightarrow A^{(J)}/\mathfrak{m}A^{(J)} \quad , \quad \bar{\varphi}([m]) = [\varphi(m)] \quad .$$

Como  $\bar{\varphi}$  es  $k$ -lineal, el cardinal de  $J$  no puede superar al cardinal de  $I$ .

## 1.2. Sucesiones Exactas

**Definición:** Diremos que una sucesión  $\dots \rightarrow M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \rightarrow \dots$  de morfismos de  $A$ -módulos es **exacta** cuando  $\text{Im } f_n = \text{Ker } f_{n+1}$  para todo índice  $n$ .

**Teorema 1.2.1** Sea  $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$  una sucesión exacta de morfismos de  $A$ -módulos. Las siguientes condiciones son equivalentes:

1. Existe un morfismo de  $A$ -módulos  $r: M \rightarrow M'$  (llamado **retracto** de  $i$ ) tal que  $r \circ i = \text{Id}_{M'}$ .
2. Existe un morfismo de  $A$ -módulos  $s: M'' \rightarrow M$  (llamado **sección** de  $p$ ) tal que  $p \circ s = \text{Id}_{M''}$ .

Además, en tal caso los morfismos  $r$  y  $s$  pueden tomarse de modo que

$$\text{Id}_M = ir + sp,$$

y por tanto  $M$  es isomorfo a  $M' \oplus M''$ .

*Demostración:* (1  $\Rightarrow$  2) Si se verifica la primera condición, entonces  $p: \text{Ker } r \rightarrow M''$  es un isomorfismo y su inverso define un morfismo  $s: M'' \rightarrow M$  tal que  $ps = \text{Id}_{M''}$ . En efecto, si  $r(m) = 0$  y  $p(m) = 0$ , entonces  $m = i(m')$  para algún  $m' \in M'$ . Luego  $0 = r(i(m')) = m'$  y  $m = i(m') = 0$ . Por otra parte, si  $m'' \in M''$ , tenemos que  $m'' = p(m) = p(m - ir(m))$  para algún  $m \in M$ , y  $m - ir(m) \in \text{Ker } r$ .

(2  $\Rightarrow$  1) Si se verifica la segunda condición, entonces  $\pi i: M' \rightarrow M/\text{Im } s$  es un isomorfismo y su inverso, compuesto con la proyección canónica  $M \rightarrow M/\text{Im } s$ , define un morfismo  $r: M \rightarrow M'$  tal que  $ri = \text{Id}_{M'}$ . En efecto, si  $\pi i(m') = 0$ , entonces  $i(m') = s(m'')$  para algún  $m'' \in M''$ . Luego  $0 = \pi i(m') = ps(m'') = m''$  y  $0 = s(m'') = i(m')$ , de modo que  $m' = 0$ . Además, si  $m \in M$ , tenemos que  $\pi(m) = \pi(m - sp(m)) = \pi i(m')$  para algún  $m' \in M'$ , porque  $m - sp(m) \in \text{Ker } p = \text{Im } i$ .

Además, por definición, para cada  $m \in M$  existe algún  $m'' \in M''$  tal que  $m = ir(m) + s(m'')$ . Aplicando  $p$  se sigue que  $p(m) = 0 + m''$ , y concluimos que  $m = ir(m) + sp(m)$ . Esta igualdad muestra que  $M = \text{Im } i + \text{Im } s$ . Como además  $0 = \text{Im } i \cap \text{Ker } r = \text{Im } i \cap \text{Im } s$ , concluimos que

$$M = \text{Im } i \oplus \text{Im } s \simeq M' \oplus M''.$$

**Definición:** Las sucesiones exactas  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  se llaman sucesiones exactas **cortas**. Diremos que una sucesión exacta corta **escinde** o **rompe** si verifica las condiciones equivalentes del teorema anterior. En tal caso  $M \simeq M' \oplus M''$ .

**Corolario 1.2.2** Toda sucesión exacta  $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} L \rightarrow 0$  de morfismos de  $A$ -módulos, donde  $L$  es  $A$ -módulo libre, escinde. En particular, si  $k$  es un cuerpo, toda sucesión exacta corta de aplicaciones  $k$ -lineales escinde.

*Demostración:* Sea  $\{e_i\}_{i \in I}$  una base de  $L$ . Como  $p$  es epiyectivo, existen elementos  $m_i \in M$  tales que  $p(m_i) = e_i$ . Ahora la aplicación  $s: L \rightarrow M$ ,  $s(\sum_i a_i e_i) = \sum_i a_i m_i$ , es  $A$ -lineal y claramente  $ps = \text{Id}_L$ , de modo que la sucesión escinde.

**Ejemplo:** La sucesión exacta corta  $0 \rightarrow \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$  no escinde.



# Capítulo 2

## Localización

### 2.1. Anillos de Fracciones

**Definición:** Diremos que un subconjunto  $S$  de un anillo  $A$  es un **sistema multiplicativo** cuando  $1 \in S$  y  $a, b \in S \Rightarrow ab \in S$ .

Si  $S$  es un sistema multiplicativo de un anillo  $A$ , vamos a construir el anillo de fracciones con numerador en  $A$  y denominador en  $S$ . Consideramos en  $A \times S$  la relación:

$$(a, s) \equiv (b, t) \Leftrightarrow \text{existen } u, v \in S \text{ tales que } au = bv \text{ y } su = tv$$

que es una relación de equivalencia en  $A \times S$ . Claramente tiene las propiedades simétrica y reflexiva. En cuanto a la transitiva, si  $(a, s) \equiv (b, t)$  y  $(b, t) \equiv (c, r)$ , existen  $u, v, u', v' \in S$  tales que  $au = bv$ ,  $su = tv$  y  $bu' = cv'$ ,  $tu' = rv'$ . Luego

$$auu' = bvu' = cvv' \quad , \quad suu' = tvu' = rrv'$$

Como  $uu', vv' \in S$ , concluimos que  $(a, s) \equiv (c, r)$

El conjunto cociente  $(A \times S)/\equiv$  se denota  $S^{-1}A$  ó  $A_S$ , y la clase de equivalencia de cada pareja  $(a, s)$  en  $A_S$  se denota  $a/s$ .

**Definición:** Sea  $S$  un sistema multiplicativo de un anillo  $A$ . Llamaremos **anillo de fracciones** o **localización** de  $A$  por  $S$  al conjunto  $A_S$  con la estructura de anillo que definen las siguientes operaciones:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \end{aligned}$$

Para ver que estas operaciones no dependen de los representantes elegidos, basta comprobarlo cuando la fracción  $a/s$  se sustituye por  $au/su$ :

$$\begin{aligned} \frac{au}{su} + \frac{b}{t} &= \frac{aut + bsu}{stu} = \frac{(at + bs)u}{stu} = \frac{at + bs}{st} \\ \frac{au}{su} \cdot \frac{b}{t} &= \frac{abu}{stu} = \frac{ab}{st} \end{aligned}$$

Es sencillo comprobar que estas operaciones definen en  $A_S$  una estructura de anillo. El cero es  $0/1$ , la unidad es  $1/1$  y el opuesto de  $a/s$  es  $(-a)/s$ . Además, una fracción  $a/s$  es nula precisamente cuando  $ta = 0$  para algún  $t \in S$ .

La aplicación  $\gamma: A \rightarrow S^{-1}A$ ,  $\gamma(a) = a/1$ , es morfismo de anillos

$$\begin{aligned}\gamma(a+b) &= (a+b)/1 = a/1 + b/1 = \gamma(a) + \gamma(b) \\ \gamma(ab) &= ab/1 = (a/1)(b/1) = \gamma(a)\gamma(b) \\ \gamma(1) &= 1/1\end{aligned}$$

Nótese que  $\gamma(s) = s$  es invertible en  $S^{-1}A$  para todo  $s \in S$ , pues su inverso es  $1/s$ . Este morfismo de anillos canónico  $\gamma: A \rightarrow S^{-1}A$  se llamará **morfismo de localización**.

**Propiedad Universal de la Localización:** Sea  $\gamma: A \rightarrow S^{-1}A$  el morfismo de localización de un anillo  $A$  por un sistema multiplicativo  $S$ . Si  $f: A \rightarrow B$  es un morfismo de anillos tal que  $f(s)$  es invertible en  $B$  para todo  $s \in S$ , entonces existe un único morfismo de anillos  $\psi: S^{-1}A \rightarrow B$  tal que  $f = \psi \circ \gamma$ :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \gamma \searrow & & \nearrow \psi \\ & S^{-1}A & \end{array}$$

*Demostración:* Si  $f(s)$  es invertible en  $B$  para todo  $s \in S$ , entonces la aplicación

$$\psi: S^{-1}A \rightarrow B, \quad \psi(a/s) = f(a)f(s)^{-1}$$

no depende del representante  $a/s$  elegido, porque

$$\psi(au/su) = f(au)f(su)^{-1} = f(a)f(u)f(s)^{-1}f(u)^{-1} = f(a)f(s)^{-1}$$

Se comprueba fácilmente que esta aplicación  $\psi$  es un morfismo de anillos. Además, si  $a \in A$ , entonces  $(\psi \circ \gamma)(a) = \psi(a/1) = f(a)f(1)^{-1} = f(a)$ .

**Teorema 2.1.1** Sea  $A$  un anillo íntegro.  $S = A - \{0\}$  es un sistema multiplicativo, el anillo de fracciones  $S^{-1}A$  es un cuerpo (llamado **cuerpo de fracciones** de  $A$ ) y el morfismo de localización  $\gamma: A \rightarrow S^{-1}A$  es inyectivo.

*Demostración:* Si  $A$  es íntegro,  $S = A - \{0\}$  es un sistema multiplicativo porque en  $A$  el producto de elementos no nulos nunca es nulo y  $1 \neq 0$ .

Por otra parte, si  $a/1 = 0$ , existe  $s \neq 0$  tal que  $sa = 0$ ; luego  $a = 0$  y se sigue que  $\gamma: A \rightarrow S^{-1}A$  es inyectivo. En particular  $S^{-1}A \neq 0$ . Además, si  $a/s$  no es nulo, entonces  $a \neq 0$ ; luego  $a \in S$  y  $s/a \in S^{-1}A$  verifica que  $(a/s)(s/a) = 1$ , de modo que  $a/s$  es invertible en  $S^{-1}A$  y concluimos que  $S^{-1}A$  es un cuerpo.

## 2.2. Localización de Módulos

**Definición:** Sea  $S$  un sistema multiplicativo de un anillo  $A$ . Si  $M$  es un  $A$ -módulo, denotaremos  $S^{-1}M$  ó  $M_S$  el cociente de  $M \times S$  respecto de la relación de equivalencia

$$(m, s) \equiv (n, t) \Leftrightarrow \text{existen } u, v \in S \text{ tales que } mu = nv \text{ y } su = tv$$

y la imagen de cada pareja  $(m, s)$  en el cociente  $S^{-1}M$  se denotará  $m/s$ .

Las operaciones

$$\begin{aligned}\frac{m}{s} + \frac{n}{t} &= \frac{tm + sn}{st} \\ \frac{a}{s} \cdot \frac{m}{t} &= \frac{am}{st}\end{aligned}$$

no dependen de los representantes elegidos, y definen en  $S^{-1}M$  una estructura de  $S^{-1}A$ -módulo y diremos que es la **localización** de  $M$  por  $S$ . La aplicación canónica

$$\gamma: M \longrightarrow S^{-1}M, \quad \gamma(m) = m/1$$

es morfismo de  $A$ -módulos y diremos que es el **morfismo de localización**. También diremos que  $\gamma(m) = m/1$  es la localización de  $m$  por  $S$ . Por definición, *la condición necesaria y suficiente para que la localización de un elemento  $m \in M$  por  $S$  sea nula es que  $sm = 0$  para algún  $s \in S$ .*

Cada morfismo de  $A$ -módulos  $f: M \rightarrow N$  induce de modo natural una aplicación, llamada **localización** de  $f$  por  $S$ :

$$S^{-1}f: S^{-1}M \longrightarrow S^{-1}N, \quad (S^{-1}f)(m/s) = f(m)/s$$

que es morfismo de  $S^{-1}A$ -módulos.

Es inmediato comprobar que la localización de morfismos conserva composiciones y combinaciones  $A$ -lineales:

$$\begin{aligned} S^{-1}(f \circ g) &= (S^{-1}f) \circ (S^{-1}g) \\ S^{-1}(af + bg) &= a(S^{-1}f) + b(S^{-1}g) \end{aligned}$$

**Propiedad universal de la localización de módulos:** *Sea  $M$  un  $A$ -módulo y sea  $S$  un sistema multiplicativo de  $A$ . Si  $N$  es un  $S^{-1}A$ -módulo y  $f: M \rightarrow N$  es un morfismo de  $A$ -módulos, existe un único morfismo de  $S^{-1}A$ -módulos  $\phi: S^{-1}M \rightarrow N$  tal que  $f = \phi \circ \gamma$ ; es decir,  $\phi(m/1) = f(m)$  para todo  $m \in M$ :*

$$\text{Hom}_A(M, N) = \text{Hom}_{S^{-1}A}(S^{-1}M, N)$$

*Demostración:* La unicidad es evidente, pues tal morfismo  $\phi$  ha de ser  $\phi(m/s) = s^{-1}f(m)$ . En cuanto a la existencia, veamos que tal igualdad define una aplicación de  $S^{-1}M$  en  $N$ :

$$\phi(um/us) = (su)^{-1}f(um) = s^{-1}u^{-1}uf(m) = s^{-1}f(m)$$

Ahora es inmediato comprobar que esta aplicación  $\phi$  es morfismo de  $S^{-1}A$ -módulos.

**Teorema 2.2.1** *Sea  $S$  un sistema multiplicativo de un anillo  $A$  y sea*

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

*una sucesión exacta de  $A$ -módulos. También es exacta la sucesión*

$$M'_S \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} M''_S$$

*Demostración:*  $\text{Im}(S^{-1}f) \subseteq \text{Ker}(S^{-1}g)$  porque

$$(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = 0$$

Recíprocamente, si  $m/s \in \text{Ker}(S^{-1}g)$ , entonces  $g(m)/s = 0$ . Luego  $0 = tg(m) = g(tm)$  para algún  $t \in S$  y, por hipótesis, existe  $m' \in M'$  tal que  $tm = f(m')$ . Por tanto

$$m/s = tm/ts = f(m')/ts = (S^{-1}f)(m'/ts)$$

y  $\text{Ker}(S^{-1}g) \subseteq \text{Im}(S^{-1}f)$ . Concluimos que  $\text{Im}(S^{-1}f) = \text{Ker}(S^{-1}g)$ .

Una consecuencia de este teorema es que la localización transforma submódulos en submódulos. Con precisión, si  $N$  es un submódulo de un módulo  $M$  y consideramos la inclusión natural  $N \rightarrow M$ , su localización  $S^{-1}N \rightarrow S^{-1}M$  es inyectiva, así que induce un isomorfismo de  $S^{-1}N$  con su imagen, que es un submódulo de  $S^{-1}M$  que también denotaremos  $S^{-1}N$ :

$$S^{-1}N = \{m \in S^{-1}M : m = n/s \text{ para algún } n \in N\}$$

**Corolario 2.2.2**

$$\begin{aligned}
S^{-1}(M/N) &= (S^{-1}M)/(S^{-1}N) \\
S^{-1}(N \cap N') &= (S^{-1}N) \cap (S^{-1}N') \\
S^{-1}(M \oplus M') &= (S^{-1}M) \oplus (S^{-1}M') \\
S^{-1}(\text{Ker } f) &= \text{Ker } (S^{-1}f) \\
S^{-1}(\text{Im } f) &= \text{Im } (S^{-1}f) \\
S^{-1}(N + N') &= (S^{-1}N) + (S^{-1}N') \\
S^{-1}(\mathfrak{a}M) &= (S^{-1}\mathfrak{a})(S^{-1}M)
\end{aligned}$$

*Demostración:* La primera afirmación se obtiene localizando la sucesión exacta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

En cuanto a la segunda, si  $n/s = n'/s'$ , donde  $n \in N$ ,  $n' \in N'$ , entonces  $un = u'n'$  para ciertos  $u', u \in S$ ; luego  $un$  está en  $N \cap N'$  y  $n/s = (un)/(us) \in S^{-1}(N \cap N')$ .

Localizando la sucesión exacta escindida  $0 \rightarrow M' \rightarrow M' \oplus M \rightarrow M \rightarrow 0$ , obtenemos una sucesión exacta

$$0 \longrightarrow M'_S \longrightarrow (M' \oplus M)_S \longrightarrow M_S \longrightarrow 0$$

que escinde; luego  $(M' \oplus M)_S = M'_S \oplus M_S$ .

Si  $f: M \rightarrow N$  es un morfismo de  $A$ -módulos, localizando la sucesión exacta

$$0 \longrightarrow \text{Ker } f \longrightarrow M \xrightarrow{f} N$$

obtenemos que  $S^{-1}(\text{Ker } f) = \text{Ker } (S^{-1}f)$ .

Las restantes igualdades se siguen directamente de las definiciones.

### 2.3. Espectro de un Anillo

**Definición :** Llamaremos **espectro primo** de un anillo  $A$  al conjunto de sus ideales primos y lo denotaremos  $\text{Spec } A$ . Llamaremos **funciones** a los elementos del anillo  $A$  y **puntos** a los elementos de su espectro  $\text{Spec } A$ , de modo que cada punto  $x \in \text{Spec } A$  se corresponde con un ideal primo de  $A$  que denotaremos  $\mathfrak{p}_x$ . Diremos que una función  $f \in A$  se **anula** en un punto  $x \in \text{Spec } A$  cuando  $f \in \mathfrak{p}_x$ , de modo que *el ideal primo  $\mathfrak{p}_x$  de un punto  $x$  está formado por todas las funciones que se anulan en  $x$*

$$\mathfrak{p}_x = \{f \in A: f \text{ se anula en } x\}.$$

El hecho de que el ideal de un punto  $x$  sea un ideal primo significa que:

*La función 0 se anula en todos los puntos.*

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

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

*Si un producto de funciones se anula en  $x$ , algún factor se anula en  $x$ .*

El teorema 1.1.3 muestra que *todo anillo no nulo tiene espectro no vacío* y 1.1.5 nos dice que *las funciones invertibles son las que no se anulan en ningún punto del espectro*.

**Definición:** Sea  $A$  un anillo. Si  $f \in A$ , llamaremos **ceros** de la función  $f$  al subconjunto  $(f)_o$  del espectro de  $A$  formado por todos los puntos donde se anule  $f$ . Llamaremos **ceros** de un ideal  $\mathfrak{a}$  de  $A$  al subconjunto de  $\text{Spec } A$  formado por los puntos donde se anulen todas las funciones de  $\mathfrak{a}$  y lo denotaremos  $(\mathfrak{a})_o$ :

$$(\mathfrak{a})_o = \bigcap_{f \in \mathfrak{a}} (f)_o = \{x \in \text{Spec } A: \mathfrak{a} \subseteq \mathfrak{p}_x\} = \left[ \begin{array}{l} \text{Ideales primos de } A \\ \text{que contienen a } \mathfrak{a} \end{array} \right]$$

Ahora 1.1.2 afirma que

$$\text{Spec}(A/\mathfrak{a}) = (\mathfrak{a})_o$$

**Teorema 2.3.1** *Si  $S$  es un sistema multiplicativo de un anillo  $A$ , entonces el espectro de  $A_S$  está formado por los puntos de  $\text{Spec } A$  donde no se anula ninguna función  $f \in S$ :*

$$\text{Spec } A_S = \left[ \begin{array}{l} \text{Ideales primos de } A \\ \text{que no cortan a } S \end{array} \right]$$

donde cada ideal primo  $\mathfrak{q}$  de  $A_S$  se corresponde con  $A \cap \mathfrak{q} := \{a \in A : a/1 \in \mathfrak{q}\}$ , y cada ideal primo  $\mathfrak{p}$  de  $A$  se corresponde con  $\mathfrak{p}A_S = \{a/s \in A_S : a \in \mathfrak{p}\}$ .

*Demostración:* Es fácil comprobar que  $\mathfrak{p} = A \cap \mathfrak{q}$  es un ideal primo de  $A$  y que

$$\mathfrak{q} = \{a/s \in A_S : a \in \mathfrak{p}\} = \mathfrak{p}A_S$$

así que la aplicación considerada es inyectiva. Además  $\mathfrak{p}$  no corta a  $S$  porque, en caso contrario,  $\mathfrak{q} = \mathfrak{p}A_S$  tendría elementos invertibles y  $\mathfrak{q} = A_S$ , contra la hipótesis de que el ideal  $\mathfrak{q}$  es primo. Además, si  $\mathfrak{p}$  es un ideal primo de  $A$  que no corta a  $S$ , entonces  $A \cap (\mathfrak{p}A_S) = \mathfrak{p}$ :

$$\frac{a}{1} = \frac{b}{s}, b \in \mathfrak{p} \Rightarrow au = bv \in \mathfrak{p}, u \in S \Rightarrow a \in \mathfrak{p}$$

Se sigue también que  $\mathfrak{p}A_S$  es un ideal primo de  $A_S$ ,

$$(a_1/s_1)(a_2/s_2) \in \mathfrak{p}A_S \Rightarrow a_1a_2 \in A \cap \mathfrak{p}A_S = \mathfrak{p} \Rightarrow a_i \in \mathfrak{p} \Rightarrow a_i/s_i \in \mathfrak{p}A_S$$

lo que permite concluir que el morfismo de localización  $\gamma: A \rightarrow A_S$  establece una biyección entre los ideales primos de  $A_S$  y los ideales primos de  $A$  que no cortan a  $S$ .

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

**Corolario 2.3.2** *Los ideales primos de  $A_f$  se corresponden con los ideales primos de  $A$  que no contienen a  $f$ :*

$$\text{Spec } A_f = (\text{Spec } A) - (f)_o$$

**Definición:** Llamaremos **radical** de un anillo  $A$  al conjunto de sus elementos nilpotentes:

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

y diremos que un anillo es **reducido** si su radical es nulo; es decir, si carece de elementos nilpotentes no nulos.

**Teorema 2.3.3** *El radical de un anillo  $A$  es la intersección de todos sus ideales primos, y por tanto es un ideal de  $A$ . Es decir, las funciones nilpotentes son las que se anulan en todos los puntos del espectro.*

*Demostración:* Es claro que los elementos nilpotentes de un anillo  $A$  pertenecen a todos sus ideales primos.

Recíprocamente, si un elemento  $f \in A$  pertenece a todos los ideales primos, entonces  $A_f$  carece de ideales primos según 2.3.2. De acuerdo con 1.1.3 tenemos que  $A_f = 0$ ; luego  $1/1 = 0/1$ , de modo que existe una potencia  $f^n$  tal que  $0 = f^n(1 - 0) = f^n$ .

## 2.4. Propiedades Locales

**Notación:** Sea  $x \in \text{Spec } A$  y sea  $\mathfrak{p}$  el correspondiente ideal primo de  $A$ . La localización de un  $A$ -módulo  $M$  por el sistema multiplicativo  $S = A - \mathfrak{p}$  de las funciones que no se anulan en  $x$  se denota  $M_x$  o  $M_{\mathfrak{p}}$ . La imagen de cada elemento  $m \in M$  por el morfismo canónico de localización  $M \rightarrow M_x$  se denota  $m_x$ .

**Lema 2.4.1** *Si  $m_x = 0$  en todo punto  $x \in \text{Spec } A$ , entonces  $m = 0$ .*

*Demostración:* Sea  $I = \{f \in A: fm = 0\}$  el ideal anulador de  $m$ . Si  $m_x = 0$ , entonces  $fm = 0$  para alguna función  $f \in A$  que no se anula en  $x$ ; luego  $x$  no está en  $(I)_o$ .

Ahora bien, si  $(I)_o = \emptyset$ , según 1.1.4 tenemos que  $I = A$  y concluimos que  $0 = 1 \cdot m = m$ .

**Teorema 2.4.2** *Sea  $M$  un  $A$ -módulo. Si  $M_x = 0$  en todo  $x \in \text{Spec } A$ , entonces  $M = 0$ .*

*Demostración:* Si  $M_x = 0$ , entonces todo elemento de  $M$  se anula al localizar en  $x$ , y el lema anterior permite concluir que todo elemento de  $M$  es nulo.

**Teorema 2.4.3** *Una sucesión de morfismos de  $A$ -módulos  $M' \xrightarrow{f} M \xrightarrow{g} M''$  es exacta si y sólo si es exacta su localización  $M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$  en todo punto  $x \in \text{Spec } A$ .*

*Demostración:* Según 2.2.1, la localización de una sucesión es exacta también es exacta.

Recíprocamente, si la sucesión es exacta al localizar en todo punto  $x$ , entonces

$$(\text{Im } gf)_x = \text{Im } (gf)_x = \text{Im } (g_x f_x) = 0$$

y, de acuerdo con 2.4.2, se sigue que  $\text{Im } gf = 0$ ; es decir,  $\text{Im } f \subseteq \text{Ker } g$ .

Localizando ahora  $(\text{Ker } g)/(\text{Im } f)$  obtenemos que

$$(\text{Ker } g/\text{Im } f)_x = (\text{Ker } g)_x/(\text{Im } f)_x = (\text{Ker } g_x)/(\text{Im } f_x) = 0$$

y de nuevo 2.4.2 permite concluir que  $(\text{Ker } g)/(\text{Im } f) = 0$ . Es decir,  $\text{Ker } g = \text{Im } f$ .

**Corolario 2.4.4** *La condición necesaria y suficiente para que un morfismo de  $A$ -módulos sea inyectivo (respectivamente epiyectivo, isomorfismo) es que lo sea al localizar en todos los puntos de  $\text{Spec } A$ .*

**Corolario 2.4.5** *Si un  $A$ -módulo  $M$  está anulado por alguna potencia de cierto ideal maximal  $\mathfrak{m}$ , i.e  $\mathfrak{m}^n M = 0$ , entonces  $M = M_{\mathfrak{m}}$ .*

*Demostración:* El morfismo natural  $M \rightarrow M_{\mathfrak{m}}$  siempre es un isomorfismo al localizar en  $\mathfrak{m}$ . Cuando  $\mathfrak{m}^n M = 0$ , también es isomorfismo al localizar en cualquier otro punto  $x \in \text{Spec } A$ . En efecto, como existe  $f \in \mathfrak{m}^n$  que no se anula en  $x$  y  $fM = 0$ , se tiene que  $M_x = 0$  y  $(M_{\mathfrak{m}})_x = (M_x)_{\mathfrak{m}} = 0$ . q.e.d.

El teorema anterior reduce la mayor parte de las cuestiones sobre un  $A$ -módulo  $M$  a estudiar el correspondiente problema sobre los  $A_x$ -módulos  $M_x$ , donde  $x$  recorre los puntos de  $\text{Spec } A$ . Ahora bien, estos anillos  $A_x$  no son arbitrarios, sino que tienen la particularidad de tener un único ideal maximal  $\mathfrak{p}A_x$ , y vamos a ver que la anulación de  $M_x$  equivale, cuando  $M$  es un  $A$ -módulo de tipo finito, a la del espacio vectorial  $M_x/\mathfrak{p}M_x$  sobre el cuerpo residual  $A_x/\mathfrak{p}A_x$  del punto  $x$ , que es una cuestión de álgebra lineal.

**Proposición 2.4.6** *Sea  $\mathfrak{p}$  el ideal primo de un punto  $x \in \text{Spec } A$ . Los ideales primos de  $A_x$  se corresponden con los ideales primos de  $A$  contenidos en  $\mathfrak{p}$ . En particular,  $A_x$  tiene un único ideal maximal, que es  $\mathfrak{p}A_x$ .*

*Demostración:* Basta aplicar 2.3.1 al sistema multiplicativo  $S = A - \mathfrak{p}$ .

**Definición:** Un anillo es **local** si tiene un único ideal maximal.

**Lema de Nakayama:** Sea  $\mathcal{O}$  un anillo local y  $\mathfrak{m}$  su único ideal maximal. Si  $M$  es un  $\mathcal{O}$ -módulo de tipo finito y  $\mathfrak{m}M = M$ , entonces  $M = 0$ .

*Demostración:* Si  $M \neq 0$ , consideramos un sistema finito  $\{m_1, \dots, m_n\}$  de generadores de  $M$  tales que  $m_2, \dots, m_n$  no generen  $M$ . Por hipótesis  $M = \mathfrak{m}M = \mathfrak{m}(\mathcal{O}m_1 + \dots + \mathcal{O}m_n) = \mathfrak{m}m_1 + \dots + \mathfrak{m}m_n$ , así que  $m_1 = f_1m_1 + f_2m_2 + \dots + f_nm_n$  para ciertas funciones  $f_1, \dots, f_n \in \mathfrak{m}$ . Luego

$$(1 - f_1)m_1 = f_2m_2 + \dots + f_nm_n$$

y  $1 - f_1$  no está en  $\mathfrak{m}$ , que es el único ideal maximal de  $\mathcal{O}$ . En virtud de 1.1.5 concluimos que  $1 - f_1$  es invertible en  $\mathcal{O}$  y, por tanto, que  $m_1$  está en  $\mathcal{O}m_2 + \dots + \mathcal{O}m_n$ . Luego  $m_2, \dots, m_n$  generan  $M$ , lo que implica una contradicción.

**Corolario 2.4.7** Sea  $\mathcal{O}$  un anillo local,  $k = \mathcal{O}/\mathfrak{m}$  el cuerpo residual de su único ideal maximal  $\mathfrak{m}$ , y sea  $M$  un  $\mathcal{O}$ -módulo de tipo finito.

La condición necesaria y suficiente para que  $m_1, \dots, m_n \in M$  generen el  $\mathcal{O}$ -módulo  $M$  es que  $\bar{m}_1, \dots, \bar{m}_n$  generen el  $k$ -espacio vectorial  $M/\mathfrak{m}M$ .

*Demostración:* Sea  $N = \mathcal{O}m_1 + \dots + \mathcal{O}m_n$ . La condición de que  $\bar{m}_1, \dots, \bar{m}_n$  generen el  $k$ -espacio vectorial  $M/\mathfrak{m}M$  significa que  $M = N + \mathfrak{m}M$ . Pasando al cociente por  $N$  obtenemos que  $M/N = \mathfrak{m}(M/N)$ , y el lema de Nakayama permite concluir que  $M/N = 0$ . Es decir,  $N = M$  y  $m_1, \dots, m_n$  generan el  $\mathcal{O}$ -módulo  $M$ .



## Capítulo 3

# Módulos sobre Dominios de Ideales Principales

### 3.1. Dominios de Ideales Principales

**Definición:** Un **dominio de ideales principales** es un anillo íntegro donde cada ideal es principal, es decir, está generado por un elemento. En este capítulo  $A$  denotará un dominio de ideales principales.

Ejemplos de dominios de ideales principales son los anillos euclídeos, en particular  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$  y el anillo de polinomios  $k[x]$  con coeficientes en un cuerpo  $k$ . La localización de un dominio de ideales principales también es un dominio de ideales principales.

**Definición:** 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** cuando carecen de divisores propios comunes.

Nótese que un elemento  $a$  es divisor de otro  $b$  si y sólo si  $bA \subseteq aA$ .

Dados elementos  $a, b \in A$ , consideremos un generador  $d$  del ideal  $aA + bA$ . Como  $a, b \in aA + bA = dA$ , resulta que  $d$  es divisor de  $a$  y  $b$ . Por otra parte, si  $c$  es divisor de  $a$  y  $b$ , entonces  $dA = aA + bA \subseteq cA$ , luego  $c$  es divisor de  $d$ . En conclusión,  $d$  es el máximo común divisor de  $a$  y  $b$  en  $A$ . De la igualdad  $dA = aA + bA$  se deduce directamente la

**Identidad de Bézout:** Sea  $d$  el máximo común divisor de dos elementos  $a, b$ . Existen elementos  $\alpha, \beta \in A$  tales que

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

**Corolario 3.1.1** Si  $a, b$  son primos entre sí, existen  $\alpha, \beta \in A$  tales que  $1 = \alpha a + \beta b$ .

**Lema 3.1.2** Si  $a$  divide a  $bc$  y es primo con  $b$ , entonces divide a  $c$ .

*Demostración:* Sean  $\alpha, \beta \in A$  tales que  $1 = \alpha a + \beta b$ . Multiplicando por  $c$  resulta  $c = \alpha ac + \beta bc$ ; como  $a$  divide a los dos sumandos se concluye que divide también a la suma  $c$ .

**Lema de Euclides:** Si un elemento irreducible divide un producto, divide algún factor.

**Proposición 3.1.3** Toda cadena de ideales de  $A$  estabiliza.

*Demostración:* Dada una cadena de ideales  $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$  consideremos el generador  $c$  del ideal  $\cup_i \mathfrak{a}_i$ . Se cumple  $c \in \mathfrak{a}_n$  para algún  $n$ . Las inclusiones

$$\mathfrak{a}_n \subseteq \mathfrak{a}_{n+j} \subseteq \cup_i \mathfrak{a}_i = cA \subseteq \mathfrak{a}_n$$

prueban que  $\mathfrak{a}_n = \mathfrak{a}_{n+j}$  para todo  $j > 0$ .

**Teorema 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 el orden y factores invertibles.*

*Demostración:* Si algún elemento propio  $a$  no descompone en producto de factores irreducibles, entonces es producto de elementos propios  $a = bc$  y algún factor, digamos  $b$ , tampoco descompone en producto de factores irreducibles. Como la inclusión  $aA \subset bA$  es estricta, porque  $c$  es propio, reiterando el argumento obtenemos una cadena infinita de ideales estrictamente creciente, en contradicción con la proposición anterior.

Veamos ahora la unicidad. Sean  $a = p_1 \cdots p_n = q_1 \cdots q_m$  dos descomposiciones. Por el lema de Euclides,  $q_1$  divide algún factor  $p_i$ , luego coincide con él (salvo un factor invertible) por ser  $p_i$  irreducible. Pongamos  $q_1 = p_1$  (salvo invertibles). Simplificando la identidad original tenemos  $p_2 \cdots p_n = q_2 \cdots q_m$ . Razonando con  $q_2$  como hicimos 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 el orden y factores invertibles).

## 3.2. Teoremas de Descomposición

Sea  $A$  un dominio de ideales principales, y sea  $\Sigma$  el cuerpo de fracciones de  $A$ ; es decir,  $\Sigma$  es la localización de  $A$  por el sistema multiplicativo  $S = A - \{0\}$ .

**Definición:** Se llama **rango** de un  $A$ -módulo  $M$  a la dimensión de  $S^{-1}M$  como espacio vectorial sobre  $\Sigma$ . Nótese que para un  $A$ -módulo libre  $L = A \oplus \dots \oplus A$  el rango es justamente el número  $r$  de sumandos isomorfos a  $A$ .

**Proposición 3.2.1** *Todo submódulo  $M$  de un  $A$ -módulo libre  $L_r$  de rango finito  $r$  es también libre de rango  $\leq r$ .*

*Demostración:* Procedemos por inducción sobre  $r$ ; pues si  $r = 1$ , entonces  $L_r \simeq A$  y en consecuencia  $M$  es isomorfo a un ideal  $aA$  de  $A$ . Como  $aA = 0$  ó  $aA \simeq A$  se concluye.

Si  $r > 1$ , descomponemos  $L_r$  en suma directa de dos libres de rango menor que  $r$ , digamos  $L = L_n \oplus L_{r-n}$ . Llamando  $\pi: L \rightarrow L_{r-n}$  a la proyección natural, tenemos las sucesiones exactas

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_n & \longrightarrow & L_r & \xrightarrow{\pi} & L_{r-n} & \longrightarrow & 0 \\ & & \cup & & \cup & & \cup & & \\ 0 & \longrightarrow & L_n \cap M & \longrightarrow & M & \xrightarrow{\pi} & \pi(M) & \longrightarrow & 0 \end{array}$$

Por hipótesis de inducción,  $L_n \cap M$  es libre de rango  $\leq n$  y  $\pi(M)$  es libre de rango  $\leq r-n$ . Además, por ser  $\pi(M)$  libre, la segunda sucesión exacta rompe; luego  $M \simeq (L_n \cap M) \oplus \pi(M)$  y concluimos que  $M$  es libre de rango  $\leq r$ .

**Corolario 3.2.2** *Todo submódulo  $M'$  de un  $A$ -módulo finito generado  $M$  también es finito generado.*

*Demostración:* Por ser  $M$  finito generado, existe un epimorfismo  $\pi: L \rightarrow M$  siendo  $L$  libre de rango finito. Por la proposición anterior, el submódulo  $L' = \pi^{-1}(M')$  es libre de rango finito; en particular  $L'$  es finito generado. Como  $\pi: L' \rightarrow M'$  es epiyectivo, se concluye que  $M'$  también es finito generado.

**Ejemplo:** Para hallar una base del submódulo  $L$  de  $A^r$  generado por ciertos elementos, realizamos transformaciones elementales con los generadores (intercambiar dos, sumar a uno un múltiplo de otro o multiplicar por un invertible de  $A$ ), obteniendo así otro sistema de generadores de  $L$ , hasta que los generadores no nulos sean linealmente independientes. Por ejemplo, calculemos una base del subgrupo  $L$  de  $\mathbb{Z}^2$  generado por los elementos  $(14,0)$ ,  $(34,6)$  y  $(39,9)$ :

$$\begin{pmatrix} 14 & 34 & 39 \\ 0 & 6 & 9 \end{pmatrix} C_3 - C_2 \quad \begin{pmatrix} 14 & 34 & 5 \\ 0 & 6 & 3 \end{pmatrix} C_2 - 2C_3 \quad \begin{pmatrix} 14 & 24 & 5 \\ 0 & 0 & 3 \end{pmatrix} C_2 - 2C_1$$

$$\begin{pmatrix} 14 & -4 & 5 \\ 0 & 0 & 3 \end{pmatrix} C_1 + 3C_2 \quad \begin{pmatrix} 2 & -4 & 5 \\ 0 & 0 & 3 \end{pmatrix} C_2 + 2C_1 \quad \begin{pmatrix} 2 & 0 & 5 \\ 0 & 0 & 3 \end{pmatrix}$$

así que  $(2,0)$  y  $(5,3)$  forman una base (luego también  $(2,0)$  y  $(1,3)$  forman una base de  $L$ ).

**Definición:** Un elemento  $m$  de un  $A$ -módulo  $M$  se dice de **torsión** si existe un elemento no nulo  $a \in A$  tal que  $am = 0$ ; es decir, cuando el morfismo  $A \xrightarrow{m} M$  no es inyectivo.

Tal condición equivale a que la localización  $m/1$  sea nula, al localizar por el sistema multiplicativo  $S = A - \{0\}$ ; i.e., la torsión de  $M$  coincide con el núcleo del morfismo de localización  $M \rightarrow M_S$ , así que es un submódulo de  $M$ , llamado **submódulo de torsión**, y se denota  $T(M)$ .

Diremos que un  $A$ -módulo  $M$  es *de torsión* si  $M = T(M)$ . Diremos que  $M$  **carece de torsión** si  $T(M) = 0$ .

Las siguientes propiedades son elementales:

1.  $T(M \oplus N) = T(M) \oplus T(N)$
2.  $M/T(M)$  carece de torsión.
3. Todo  $A$ -módulo libre  $L$  carece de torsión:  $T(L) = 0$ .
4.  $M$  es de torsión precisamente cuando  $M_S = 0$ .

**Proposición 3.2.3** *Todo  $A$ -módulo  $M$  finito generado y sin torsión es libre.*

*Demostración:* Bastará probar que  $M$  se inyecta en un  $A$ -módulo libre de rango finito. Como  $M$  carece de torsión, tenemos una inyección  $M \rightarrow M_S$ . Si  $m_1, \dots, m_s$  es un sistema de generadores de  $M$ , entonces  $m_1/1, \dots, m_s/1$  es un sistema de generadores de  $M_S$  como espacio vectorial sobre  $\Sigma$ . De dicho sistema de generadores podemos extraer una base, digamos  $m_1/1, \dots, m_r/1$ . Podemos escribir entonces:

$$\frac{m_i}{1} = \sum_{j=1}^r \frac{a_{ij}}{b_{ij}} \frac{m_j}{1} \quad \text{con } a_{ij}, b_{ij} \in A$$

y reduciendo a común denominador podemos suponer que todos los  $b_{ij}$  son iguales, digamos  $b_{ij} = b$ , así que

$$\frac{m_i}{1} = \sum_{j=1}^r \frac{a_{ij}}{b} \frac{m_j}{1}$$

Se concluye entonces que los generadores de  $M$  se inyectan en el  $A$ -módulo libre  $L = A(m_1/b) \oplus \dots \oplus A(m_r/b)$ , luego  $M \subseteq L$ .

**Primer teorema de descomposición:** *Todo  $A$ -módulo finito generado descompone de modo único (salvo isomorfismos) en suma directa de un  $A$ -módulo libre y un  $A$ -módulo de torsión. En concreto, si  $r$  es el rango de  $M$ , se verifica*

$$M \simeq (A \oplus \dots \oplus A) \oplus T(M)$$

*Demostración:* Consideremos la sucesión exacta

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0$$

Por la proposición anterior  $M/T(M)$  es libre, así que esta sucesión exacta rompe y obtenemos la descomposición buscada:

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

Veamos ahora la unicidad de la descomposición: Sea  $M \simeq L \oplus T$  donde  $L$  es libre y  $T$  es de torsión. Localizando por  $S$  resulta  $M_S \simeq L_S$ , luego  $M$  y  $L$  tienen el mismo rango; es decir,  $L \simeq A \oplus \dots \oplus A$  donde  $r$  es el rango de  $M$ . Finalmente, tomando torsión en la descomposición  $M \simeq L \oplus T$  resulta

$$T(M) \simeq T(L) \oplus T(T) = 0 \oplus T = T.$$

**Lema 3.2.4** *Sea  $M$  un  $A$ -módulo, y para cada  $b \in A$  pongamos  $\ker b = \{m \in M : bm = 0\}$ . Si  $p, q \in A$  son primos entre sí, entonces*

$$\ker pq = \ker p \oplus \ker q$$

*Demostración:* De acuerdo con la Identidad de Bézout existen  $\lambda, \mu \in A$  tales que  $1 = \lambda p + \mu q$ . Luego para cada  $m \in M$  se cumple

$$m = 1 \cdot m = \lambda pm + \mu qm.$$

Ahora, si  $m \in \ker pq$ , entonces  $\lambda pm \in \ker q$  y  $\mu qm \in \ker p$ . Por consiguiente  $\ker pq = \ker p + \ker q$ .

Por otra parte, si  $m \in \ker p \cap \ker q$  entonces  $m = \lambda pm + \mu qm = 0 + 0 = 0$ .

De todo lo anterior se deduce que  $\ker pq = \ker p \oplus \ker q$ .

**Ejemplo:** Para determinar las sucesiones de Fibonacci, que son las sucesiones  $(a_n)_{n \geq 0}$  tales que  $a_{n+2} = a_{n+1} + a_n$  para todo índice  $n$ , introducimos el  $\mathbb{C}$ -espacio vectorial  $E$  de todas las sucesiones  $(a_n)$  de números complejos y el endomorfismo  $\nabla : E \rightarrow E$ ,  $\nabla(a_n) = (a_{n+1})$ , que induce una estructura de  $\mathbb{C}[x]$ -módulo en  $E$ . Ahora las sucesiones de Fibonacci forman el núcleo del endomorfismo  $\nabla^2 - \nabla - \text{Id}$ ; así que el problema es determinar  $\ker(x^2 - x - 1)$ .

Si  $\alpha, \beta \in \mathbb{R}$  son las raíces de  $x^2 - x - 1$ , de modo que  $x^2 - x - 1 = (x - \alpha)(x - \beta)$ , el lema anterior muestra que

$$\ker(x^2 - x - 1) = \ker(x - \alpha) \oplus \ker(x - \beta)$$

Como el núcleo de  $\nabla - \alpha$  está formado claramente por las progresiones geométricas de razón  $\alpha$ , obtenemos que cada sucesión de Fibonacci  $(a_n)$  descompone, y de modo único, en suma de una progresión geométrica de razón  $\alpha$  y otra de razón  $\beta$ :

$$a_n = a\alpha^n + b\beta^n$$

**Ejemplo:** Para resolver la ecuación diferencial  $f''(t) = -f(t)$  introducimos el  $\mathbb{C}$ -espacio vectorial  $E$  formado por las funciones complejas de variable real  $f(t) = x(t) + iy(t)$  de clase  $C^\infty$ , en el sentido de que lo son  $x(t)$  y  $y(t)$ , y el endomorfismo  $D : E \rightarrow E$ ,  $D(f(t)) = f'(t) = x'(t) + iy'(t)$ , que induce una estructura de  $\mathbb{C}[x]$ -módulo en  $E$ . Ahora las soluciones de la ecuación  $f''(t) = -f(t)$  forman el núcleo del endomorfismo  $D^2 + \text{Id}$ ; así que el problema es determinar  $\ker(x^2 + 1)$ .

Como  $x^2 + 1 = (x - i)(x + i)$ , el lema anterior muestra que

$$\ker(x^2 + 1) = \ker(x - i) \oplus \ker(x + i)$$

Ahora bien,  $\ker(x - \alpha)$  está formado por las soluciones de la ecuación  $f'(t) = \alpha f(t)$ , que fácilmente puede verse que son las funciones  $f(t) = \lambda e^{\alpha t}$ ,  $\lambda \in \mathbb{C}$ . Por tanto, toda solución  $f(t)$  de nuestra ecuación descompone, y de modo único, en suma de dos exponenciales

$$f(t) = \lambda e^{it} + \mu e^{-it} = \lambda(\cos t + i \operatorname{sen} t) + \mu(\cos t - i \operatorname{sen} t) \quad , \quad \lambda, \mu \in \mathbb{C}$$

y si buscamos las soluciones reales, basta tomar la parte real de las soluciones complejas:

$$f(t) = a \cos t + b \operatorname{sen} t \quad , \quad a, b \in \mathbb{R}$$

**Definición:** Sea  $M$  un  $A$ -módulo. Diremos que  $\mathfrak{a} = \{a \in A : aM = 0\}$  es el **ideal anulador** de  $M$ , y el generador de  $\mathfrak{a}$  se llamará **anulador** de  $M$ .

Por definición  $\mathfrak{a}M = 0$ , así que el  $A$ -módulo  $M$  admite una estructura natural de  $A/\mathfrak{a}$ -módulo:  $[a] \cdot m := am$ .

Como el generador de un ideal es único salvo un factor invertible, el anulador de un módulo está bien definido salvo un factor invertible. El anulador de  $A/bA$  es  $b$ .

El anulador de un  $A$ -módulo finito-generado de torsión  $M$  nunca es nulo. En efecto, si  $M = Am_1 + \dots + Am_n$  y  $a_i m_i = 0$ , entonces  $a_1 \dots a_n M = 0$ .

**Segundo teorema de descomposición:** Sea  $a = p_1^{n_1} \dots p_s^{n_s}$  la descomposición en factores irreducibles del anulador de un  $A$ -módulo  $M$ . Entonces  $M$  descompone de modo único en suma directa de submódulos  $M_i$  anulados por  $p_i^{n_i}$ . En concreto se cumple

$$M = \ker p_1^{n_1} \oplus \dots \oplus \ker p_s^{n_s}$$

*Demostración:* Para la existencia, basta aplicar el lema anterior sucesivamente:

$$M = \ker a = \ker p_1^{n_1} \oplus \ker (p_2^{n_2} \dots p_s^{n_s}) = \dots = \ker p_1^{n_1} \oplus \dots \oplus \ker p_s^{n_s}.$$

En cuanto a la unicidad, si  $M = M_1 \oplus \dots \oplus M_s$  donde  $p_i^{n_i} M_i = 0$ , entonces  $M_i \subset \ker p_i^{n_i}$ . Ahora tenemos que

$$(\ker p_1^{n_1}/M_1) \oplus \dots \oplus (\ker p_s^{n_s}/M_s) = (\ker p_1^{n_1} \oplus \dots \oplus \ker p_s^{n_s}) / (M_1 \oplus \dots \oplus M_s) = M/M = 0$$

y concluimos que  $\ker p_i^{n_i}/M_i = 0$ ; es decir,  $M_i = \ker p_i^{n_i}$ .

**Tercer teorema de descomposición:** Si  $M$  es un  $A$ -módulo finito-generado de anulador  $p^n$ , donde  $p$  es irreducible, entonces existe una única sucesión decreciente  $n = n_1 \geq \dots \geq n_s$  tal que

$$M \simeq (A/p^{n_1} A) \oplus \dots \oplus (A/p^{n_s} A)$$

*Demostración:* Veamos primero la existencia de tal sucesión  $n = n_1 \geq \dots \geq n_s$ . Como el ideal  $pA$  es maximal, de 2.4.5 se sigue que  $M = M_p$ , que es un  $A_p$ -módulo; así que podemos suponer que todo elemento no nulo de  $A$  es de la forma  $up^r$  para algún invertible  $u \in A$ .

Consideremos ahora una presentación de  $M$ ; i.e., una sucesión exacta

$$L'_n \xrightarrow{f} L_m \longrightarrow M \longrightarrow 0$$

donde  $L'_n$  y  $L_m$  son módulos libres de rango finito. Elegidas bases  $(e'_1, \dots, e'_n)$  y  $(e_1, \dots, e_m)$  de los módulos libres  $L'_n$  y  $L_m$ , el morfismo  $f$  vendrá dado por una matriz  $(a_{ij})$  de  $m$  filas y  $n$  columnas con coeficientes en el anillo  $A$ :

$$f(e'_j) = \sum_i a_{ij} e_i.$$

Las siguientes operaciones con las columnas  $C_j$  de la matriz  $(a_{ij})$ , que corresponden a cambios de base en  $L'_n$ , y con las filas  $F_i$  de  $(a_{ij})$ , que corresponden a cambios de base en  $L_m$ , se llaman **transformaciones elementales** (donde  $i \neq j$  y  $a \in A$ ):

<u>Transformación Elemental</u>	<u>Cambio de Base</u>
Trasponer $C_i$ y $C_j$	Trasponer $e'_i$ y $e'_j$
Trasponer $F_i$ y $F_j$	Trasponer $e_i$ y $e_j$
Sustituir $C_i$ por $C_i + aC_j$	Sustituir $e'_i$ por $e'_i + ae'_j$
Sustituir $F_i$ por $F_i + aF_j$	Sustituir $e_j$ por $e_j - ae_i$
Multiplicar $C_k$ por un invertible $u$	Sustituir $e'_k$ por $ue'_k$
Multiplicar $F_k$ por un invertible $u$	Sustituir $e_k$ por $u^{-1}e_k$

Intercambiando filas y columnas podemos conseguir que el coeficiente  $a_{11}$  sea la menor potencia de  $p$  que aparezca en la matriz, de modo que divide a todos los coeficientes  $a_{ij}$ . Ahora, con más transformaciones elementales, podemos anular los restantes coeficientes de la primera fila y la primera columna, y reiterando el proceso obtenemos bases de  $L'_n$  y  $L_m$  en que la matriz de  $f$  es de la forma

$$\begin{pmatrix} p^{r_1} & & & & 0 & \cdot \\ & p^{r_2} & & & \cdot & \cdot \\ & & \ddots & & \cdot & \cdot \\ & & & p^{r_m} & 0 & \cdot \end{pmatrix}$$

donde  $r_1 \leq r_2 \leq \dots \leq r_m$ . Luego  $M \simeq (A/p^{r_1}A) \oplus \dots \oplus (A/p^{r_m}A)$ .

Además, al ser  $p^n$  el anulador de  $M$ , tendremos que  $n = r_m$ .

Veamos ahora la unicidad de la descomposición. Sea  $k := A/pA$  y observemos que si  $N \simeq A/p^n A$ , entonces  $p^i N/p^{i+1}N$  es un  $k$ -espacio vectorial de dimensión 1 cuando  $i < n$ , y es nulo cuando  $i \geq n$ . Ahora, si  $\nu_j$  denota el número de sumandos isomorfos a  $A/p^j A$  que aparezcan en una descomposición de  $M$ , tenemos

$$\begin{aligned} \dim_k(M/pM) &= \nu_1 + \dots + \nu_n \\ \dim_k(pM/p^2M) &= \nu_2 + \dots + \nu_n \\ &\dots\dots\dots \\ \dim_k(p^{n-1}M/p^nM) &= \nu_n \end{aligned}$$

Estas igualdades permiten despejar los números  $\nu_j$  a partir de las dimensiones de los espacios vectoriales  $p^i M/p^{i+1}M$ ; luego tales números no dependen de la particular descomposición de  $M$  elegida.

**Definición:** Según el primer teorema de descomposición, todo  $A$ -módulo  $M$  finito generado descompone en suma directa de un módulo libre y otro de torsión. Aplicando a la parte de torsión el segundo y tercer teoremas de descomposición, resulta que todo  $A$ -módulo  $M$  finito generado descompone de modo único (salvo isomorfismos) en la forma

$$M \simeq (A \oplus \dots \oplus A) \oplus \left( \bigoplus_{i,j} A/p_i^{n_{ij}} A \right)$$

donde los elementos  $p_i$  son irreducibles en  $A$ ,  $r$  es el rango del módulo  $M$  y consideramos los exponentes ordenados de mayor a menor:  $n_{i1} \geq n_{i2} \geq \dots$  para cada índice  $i$ . A las potencias  $p_i^{n_{ij}}$  se les llama **divisores elementales** del módulo  $M$ . Nótese que están bien definidos salvo factores invertibles.

Como consecuencia directa de la descomposición obtenida para los módulos finito generados resulta el siguiente

**Teorema de clasificación:** *Los módulos de tipo finito sobre un dominio de ideales principales  $A$  están clasificados salvo isomorfismos por el rango y los divisores elementales; i.e., la condición necesaria y suficiente para que dos  $A$ -módulos de tipo finito sean isomorfos es que tengan el mismo rango y los mismos divisores elementales.*

### 3.3. Factores Invariantes

**Teorema Chino de los Restos:** *Sean  $\mathfrak{a}$  y  $\mathfrak{b}$  ideales de un anillo  $A$ . Si  $\mathfrak{a} + \mathfrak{b} = A$ , entonces  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ , y tenemos un isomorfismo de anillos*

$$\phi: A/\mathfrak{a} \cap \mathfrak{b} \longrightarrow (A/\mathfrak{a}) \times (A/\mathfrak{b}) \quad ; \quad \phi([x]_{\mathfrak{a}\mathfrak{b}}) = ([x]_{\mathfrak{a}}, [x]_{\mathfrak{b}})$$

*Demostración:* Por hipótesis existen  $a \in \mathfrak{a}$  y  $b \in \mathfrak{b}$  tales que  $1 = a + b$ . Ahora, si  $c \in \mathfrak{a} \cap \mathfrak{b}$ , tenemos que  $c = c(a + b) = ca + cb \in \mathfrak{a}\mathfrak{b}$ ; así que  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ , pues la inclusión contraria siempre es válida.

Además, el morfismo de anillos  $f: A \rightarrow (A/\mathfrak{a}) \times (A/\mathfrak{b})$ ,  $f(x) = ([x]_{\mathfrak{a}}, [x]_{\mathfrak{b}})$ , es epiyectivo, porque  $([c]_{\mathfrak{a}}, [d]_{\mathfrak{b}})$  proviene de  $x := bc + ad$ :

$$\begin{aligned} c &= (a + b)c \equiv bc \equiv bc + ad && \text{(módulo } \mathfrak{a}) \\ d &= (a + b)d \equiv ad \equiv bc + ad && \text{(módulo } \mathfrak{b}) \end{aligned}$$

Como el núcleo de  $f$  es  $\mathfrak{a} \cap \mathfrak{b}$ , el Teorema de Isomorfía permite concluir.

**Proposición 3.3.1** *Dado un  $A$ -módulo  $M$  finito generado, existe una única sucesión creciente de ideales  $\phi_1 A \subseteq \phi_2 A \subseteq \dots \subseteq \phi_m A$  tal que*

$$M \simeq A/\phi_1 A \oplus \dots \oplus A/\phi_m A .$$

*Demostración:* Sabemos que

$$M \simeq (A \oplus \dots \oplus A) \oplus \left( \bigoplus_{i,j} A/p_i^{n_{ij}} A \right)$$

siendo los  $p_i^{n_{ij}}$  los divisores elementales de  $M$  y  $r$  el rango. Definamos

$$\phi_1 = \dots = \phi_r = 0, \quad \phi_{r+j} = p_1^{n_{1j}} \dots p_s^{n_{sj}}$$

Agrupando sumandos en la descomposición de  $M$  por medio del teorema chino del resto se obtiene directamente que

$$M \simeq A/\phi_1 A \oplus \dots \oplus A/\phi_m A$$

Para la unicidad se razona a la inversa, descomponiendo cada sumando de la igualdad de arriba por medio del teorema chino del resto.

**Definición:** A los elementos  $\phi_1, \dots, \phi_m$  de la proposición anterior (cada uno múltiplo del siguiente y bien definidos salvo factores invertibles de  $A$ ) se les llama **factores invariantes** del módulo  $M$ .

Nótese que  $\phi_1$  es el anulador del módulo, y que la sucesión de factores invariantes puede considerarse infinita sin más que tomar  $1 = \phi_{m+1} = \phi_{m+2} = \dots$ . Además el rango del módulo coincide con el número de factores invariantes nulos.

En la demostración de la proposición anterior hemos definido los factores invariantes a partir del rango y de los divisores elementales. Recíprocamente, es evidente que los factores invariantes determinan el rango y los divisores elementales del módulo. Luego podemos reenunciar el teorema de clasificación de la siguiente manera:

**Teorema de clasificación:** *La condición necesaria y suficiente para que dos  $A$ -módulos finito generados sean isomorfos es que posean los mismos factores invariantes.*

### 3.4. Clasificación de Grupos Abelianos

Todo grupo conmutativo  $(G, +)$  tiene una estructura natural de  $\mathbb{Z}$ -módulo:

$$\begin{aligned} n \cdot g &= g + \dots + g \\ (-n) \cdot g &= -g - \dots - g \end{aligned}$$

donde  $g \in G$  y  $n \in \mathbb{N}$ . Recíprocamente, todo  $\mathbb{Z}$ -módulo posee por definición una estructura subyacente de grupo abeliano. Además, los morfismos de grupos (abelianos) son justamente los morfismos de  $\mathbb{Z}$ -módulos. Por lo tanto, la clasificación de grupos abelianos equivale a la clasificación de  $\mathbb{Z}$ -módulos. Así pues, todo grupo abeliano finito generado  $G$  viene determinado (salvo isomorfismos) por sus factores invariantes:

$$G \simeq \mathbb{Z}/\phi_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/\phi_m\mathbb{Z}$$

**Teorema de clasificación de grupos abelianos:** *Dos grupos abelianos finito generados son isomorfos si y sólo si poseen los mismos factores invariantes.*

**Corolario 3.4.1** *Todo grupo abeliano finito generado descompone, y de modo único salvo el orden de los sumando, en suma directa de grupos cíclicos infinitos y de grupos cíclicos de órdenes potencias de números primos.*

**Corolario 3.4.2** *Todo grupo abeliano finito  $G$  descompone, y de modo único salvo el orden de los sumandos, en suma directa de grupos cíclicos de órdenes potencias de números primos.*

**Corolario 3.4.3** *Si un número natural  $d$  divide al orden de un grupo abeliano finito  $G$ , entonces  $G$  tiene algún subgrupo de orden  $d$ .*

*Demostración:*  $p^{n-i}\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}/p^i\mathbb{Z}$  es un subgrupo de  $\mathbb{Z}/p^n\mathbb{Z}$  de orden  $p^i$ .

**Corolario 3.4.4** *Si  $G$  es un grupo abeliano finito-generado, las siguientes condiciones son equivalentes:*

1.  $G$  es un grupo finito.
2. El rango de  $G$  es nulo.
3. El primer factor invariante  $\phi_1$  (i.e. el anulador) de  $G$  no es nulo.

en cuyo caso su orden coincide con el producto de los factores invariantes:  $|G| = \phi_1 \dots \phi_m$ .

**Corolario 3.4.5** *La condición necesaria y suficiente para que un grupo abeliano finito-generado  $G$  sea cíclico es que tenga un único factor invariante (i.e.  $\phi_2 = 1$ ).*

### 3.5. Cálculo de los Factores Invariantes

Veamos cómo clasificar un módulo de tipo finito  $M$  sobre un anillo euclídeo  $A$  a partir de una presentación

$$L'_n \xrightarrow{f} L_m \longrightarrow M \longrightarrow 0$$

Elegidas bases  $(e'_1, \dots, e'_n)$  y  $(e_1, \dots, e_m)$  de los módulos libres  $L'_n$  y  $L_m$ , el morfismo  $f$  vendrá dado por una matriz  $A = (a_{ij})$  de  $m$  filas y  $n$  columnas:

$$f(e'_j) = \sum_i a_{ij} e_i.$$

Mediante transformaciones elementales (i.e., cambios de base en  $L'_n$  y  $L_m$ ) podemos conseguir que todos los coeficientes  $a_{ij}$  de la matriz de  $f$  sean múltiplos de  $a_{11}$ , y por

tanto anular los restantes coeficientes de la primera fila y columna. Obtenemos así matrices invertibles  $B$  y  $C$  tales que

$$\bar{A} = C^{-1}AB = \begin{pmatrix} a_1 & & & 0 & \cdot \\ & a_2 & & \cdot & \cdot \\ & & \ddots & \cdot & \cdot \\ & & & a_m & 0 & \cdot \end{pmatrix}$$

es una matriz diagonal donde  $a_{i+1}$  es múltiplo de  $a_i$ . En particular, los factores invariantes del conúcleo  $L_m/\text{Im } f \simeq M$  coinciden con los coeficientes de la diagonal de  $\bar{A}$  (completados con ceros cuando  $n < m$ ); es decir,  $\phi_1 = a_m, \phi_2 = a_{m-1}, \dots$

Esto permite calcular, mediante transformaciones elementales, los factores invariantes de  $M$  a partir de la matriz  $A$  de una presentación. Otro método alternativo lo proporciona el siguiente resultado:

**Proposición 3.5.1** *Si  $c_i$  es el máximo común divisor de los menores de orden  $m - i$  de la matriz  $A$  de una presentación de  $M$  (entendiendo que  $c_i = 0$  cuando  $m - i > n$ , y  $c_i = 1$  cuando  $m - i < 1$ ), se verifica*

$$c_i = \phi_{i+1} \cdots \phi_m$$

$$\phi_i = \begin{cases} c_{i-1}/c_i & \text{cuando } c_i \neq 0 \\ 0 & \text{cuando } c_i = 0 \end{cases}$$

*Demostración:* Si aplicamos una transformación elemental a una matriz  $A$ , se obtiene una matriz  $\bar{A}$  tal que  $(\bar{c}_i) \subseteq (c_i)$ , donde  $\bar{c}_i$  denota el máximo común divisor de los menores de orden  $m - i$  de la matriz  $\bar{A}$ . Como  $A$  también se obtiene de  $\bar{A}$  mediante una transformación elemental, se sigue que  $\bar{c}_i = c_i$ .

Después de aplicar varias transformaciones elementales, podemos suponer que nuestra matriz  $A$  es una matriz diagonal

$$A = \begin{pmatrix} a_1 & & \\ & a_2 & \\ & & \ddots \end{pmatrix}$$

donde  $a_{i+1}$  es múltiplo de  $a_i$ , caso en que el enunciado es inmediato.

**Corolario 3.5.2** *El mínimo número de generadores de  $M$  coincide con el número de factores invariantes.*

*Demostración:* El razonamiento anterior muestra que el número de generadores  $m$  acota al número de factores invariantes; pero, por otra parte, si  $\phi_1, \dots, \phi_m$  son los factores invariantes, entonces  $M \simeq A/\phi_1 A \oplus \dots \oplus A/\phi_m A$  claramente admite un sistema de  $m$  generadores.

**Corolario 3.5.3** *Un sistema de  $m$  ecuaciones diofánticas lineales  $AX = B$  admite solución entera precisamente cuando el rango  $r$  de la matriz  $A$  coincide con el rango de la matriz ampliada  $(A|B)$  y el máximo común divisor  $c_r(A)$  de sus menores de orden  $m - r$  coincide con el máximo común divisor  $c_r(A|B)$  de los menores de orden  $m - r$  de la matriz  $(A|B)$ .*

*Demostración:* Consideremos el morfismo  $\mathbb{Z}$ -lineal

$$f: \mathbb{Z}^n \rightarrow \mathbb{Z}^m, \quad f(X) = AX,$$

y su conúcleo  $M = \mathbb{Z}^m/\text{Im } f$ , de modo que  $\text{rg}(M) = m - \text{rg}(A)$ . Además, según 3.5.1, el orden  $\phi_{r+1} \cdots \phi_m$  del subgrupo de torsión de  $M$  coincide con  $c_r(A)$ .

Si el sistema tiene alguna solución entera, entonces  $B \in \text{Im } f$  y  $M = M/\mathbb{Z}B$ . Ahora 3.5.1 permite concluir que  $c_i(A) = c_i(A|B)$  para todo índice  $i$ . En particular  $c_r(A) = c_r(A|B)$ .

Recíprocamente, si el sistema no tiene solución entera, entonces  $B \neq 0$  en  $M$ . Si  $B$  no es de torsión en  $M$ , entonces  $\text{rg}(M/\mathbb{Z}B) = \text{rg}(M) - 1$  y concluimos que  $\text{rg}(A|B) = \text{rg}(A) + 1$ . Si  $B$  es de torsión en  $M$ , entonces  $\text{rg}(A|B) = \text{rg}(A) = r$ ; pero el orden del subgrupo de torsión de  $M/\mathbb{Z}B$  (que coincide con  $c_r(A|B)$  en virtud de 3.5.1) es estrictamente menor que el orden  $c_r(A)$  del subgrupo de torsión de  $M$ . Luego  $c_r(A) \neq c_r(A|B)$ .

**Ejemplo:** Para estudiar un sistema de ecuaciones diofánticas lineales  $AX = Y$ , mediante transformaciones elementales se reduce  $A$  a una matriz diagonal  $\bar{A}$ , de modo que el sistema dado es equivalente a un sistema  $\bar{A}\bar{X} = \bar{Y}$ , cuyo estudio es inmediato. El vector  $\bar{Y}$  se obtiene aplicando a  $Y$  las transformaciones elementales por filas realizadas (i.e. los cambios de base en  $L$ ), y las soluciones del sistema inicial son  $X = B\bar{X}$ , donde la matriz de cambio de base  $B$  se calcula aplicando a la base inicial de  $L'$  las transformaciones elementales por columnas que se hayan realizado (i.e. los cambios de base en  $L'$ ). Por ejemplo, para hallar las soluciones enteras del sistema

$$\left. \begin{array}{l} 5x_1 - 2x_2 - 11x_3 = 2 \\ 3x_1 + 2x_2 - 5x_3 = -2 \end{array} \right\}$$

reducimos la matriz del sistema mediante transformaciones elementales:

$$\begin{aligned} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 5 & -2 & -11 & \vdots & 2 \\ 3 & 2 & -5 & \vdots & -2 \end{pmatrix} \\ & \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 7 & -2 & -11 & \vdots & 2 \\ 1 & 2 & -5 & \vdots & -2 \end{pmatrix} \\ & \quad \text{,,} \quad \begin{pmatrix} 1 & 2 & -5 & \vdots & -2 \\ 7 & -2 & -11 & \vdots & 2 \end{pmatrix} \\ & \quad \text{,,} \quad \begin{pmatrix} 1 & 2 & -5 & \vdots & -2 \\ 0 & -16 & 24 & \vdots & 16 \end{pmatrix} \\ & \begin{pmatrix} 1 & -2 & 5 \\ -1 & 3 & -5 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & \vdots & -2 \\ 0 & -16 & 24 & \vdots & 16 \end{pmatrix} \\ & B = \begin{pmatrix} 1 & 3 & -4 \\ 1 & -2 & 1 \\ 0 & 1 & -2 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & \vdots & -2 \\ 0 & 8 & 0 & \vdots & 16 \end{pmatrix} \end{aligned}$$

de modo que el sistema inicial es equivalente al sistema  $\bar{A}\bar{X} = \bar{Y}$ :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \end{pmatrix} \begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \end{pmatrix} = \begin{pmatrix} -2 \\ 16 \end{pmatrix}$$

Las soluciones  $\bar{X}$  de este sistema son  $\bar{x}_1 = -2$ ,  $\bar{x}_2 = 2$ ,  $\bar{x}_3 = \lambda \in \mathbb{Z}$ ; luego las soluciones  $X = B\bar{X}$  del sistema inicial son

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & -4 \\ 1 & -2 & 1 \\ 0 & 1 & -2 \end{pmatrix} \begin{pmatrix} -2 \\ 2 \\ \lambda \end{pmatrix}, \quad \begin{cases} x_1 = 4 - 4\lambda \\ x_2 = -2 + \lambda \\ x_3 = 2 - 2\lambda \end{cases}$$

**Nota:** Si sólo se desea estudiar la compatibilidad de un sistema, no es necesario calcular la matriz de cambio de base  $B$ . Así, para estudiar la compatibilidad del sistema

$$\left. \begin{array}{l} 5x_1 - 2x_2 - 11x_3 = a \\ 3x_1 + 2x_2 - 5x_3 = b \end{array} \right\}$$

realizando transformaciones elementales

$$\left( \begin{array}{ccc|c} 5 & -2 & -11 & a \\ 3 & 2 & -5 & b \end{array} \right), \dots, \left( \begin{array}{ccc|c} 1 & 0 & 0 & b \\ 0 & 8 & 0 & a - 7b \end{array} \right)$$

vemos que el sistema dado es equivalente al sistema

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \end{pmatrix} \begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \end{pmatrix} = \begin{pmatrix} b \\ a - 7b \end{pmatrix}$$

que sólo es compatible cuando  $a - 7b$  es múltiplo de 8. El sistema dado es compatible precisamente cuando  $a + b$  sea múltiplo de 8.

**Ejemplo:** Sea  $G$  el grupo abeliano generado por 3 elementos con las relaciones

$$\left. \begin{array}{l} 8a + 10b + 12c = 0 \\ 8a + 4b + 6c = 0 \end{array} \right\}$$

i.e.,  $G$  es el conúcleo del morfismo  $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^3$ ,  $f(x_1, x_2) = x_1(8, 10, 12) + x_2(8, 4, 6)$ . Aplicando transformaciones elementales a la matriz de  $f$ :

$$A = \begin{pmatrix} 8 & 8 \\ 10 & 4 \\ 12 & 6 \end{pmatrix}, \begin{pmatrix} -2 & 4 \\ 10 & 4 \\ 12 & 6 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 10 & 24 \\ 12 & 30 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 0 & 24 \\ 0 & 30 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 0 & 0 \end{pmatrix} = \bar{A}$$

vemos que  $G = \mathbb{Z}^3 / \text{Im } f \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus \mathbb{Z}$ . Los factores invariantes de  $G$  son  $\phi_1 = 0$ ,  $\phi_2 = 6$  y  $\phi_3 = 2$ ; es decir,  $G$  es un grupo abeliano de rango  $r = 1$  y sus divisores elementales son 2, 2, 3. Un método alternativo lo proporciona el cálculo del máximo común divisor  $c_i$  de los menores de orden  $3 - i$  de la matriz  $A$ :

$$\begin{aligned} c_0 &= 0 \\ c_1 &= \text{m.c.d.}(-48, -48, 12) = 12 \\ c_2 &= \text{m.c.d.}(8, 10, 4, 12, 6) = 2 \\ c_3 &= c_4 = \dots = 1 \end{aligned}$$

de modo que  $\phi_1 = c_0/c_1 = 0$ ,  $\phi_2 = c_1/c_2 = 6$ ,  $\phi_3 = c_2/c_3 = 2$ .

En particular,  $G$  es un grupo infinito de rango 1, no es un grupo cíclico (de hecho, no puede ser generado con menos de 3 elementos), su anulador es 0 y su subgrupo de torsión  $T(G) \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z})$  tiene 12 elementos.



## Capítulo 4

# Grupos Finitos

### 4.1. $G$ -conjuntos

**Definición:** Sea  $G$  un grupo y  $X$  un conjunto. Llamaremos **acción** (por la izquierda<sup>1</sup>) de  $G$  en  $X$  a toda aplicación  $G \times X \longrightarrow X$  tal que

1.  $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$  para todo  $g_1, g_2 \in G, x \in X$ .
2.  $1 \cdot x = x$  para todo  $x \in X$ .

Dar una acción de  $G$  en  $X$  es dar un morfismo de grupos  $\rho: G \rightarrow \text{Bij}(X)$ ,  $\rho(g)(x) = g \cdot x$ , en el grupo  $\text{Bij}(X)$  de todas las biyecciones de  $X$ , en cuyo caso diremos que  $X$  es un  **$G$ -conjunto**.

Si  $X$  e  $Y$  son  $G$ -conjuntos, diremos que una aplicación  $f: X \rightarrow Y$  es un **morfismo de  $G$ -conjuntos** cuando  $f(g \cdot x) = g \cdot f(x)$  para todo  $g \in G, x \in X$ . Los isomorfismos de  $G$ -conjuntos son los morfismos biyectivos.

Cada acción de un grupo  $G$  en un conjunto  $X$  define una relación de equivalencia en  $X$  sin más que considerar equivalentes dos elementos  $x, y \in X$  cuando exista algún  $g \in G$  tal que  $y = gx$ . Llamaremos **órbita** de  $x \in X$  a su clase de equivalencia

$$Gx := \{y \in X : y = gx \text{ para algún } g \in G\}$$

y llamaremos **subgrupo de isotropía** de  $x \in X$  al subgrupo

$$I_x := \{h \in G : hx = x\}.$$

Si  $g \in G$ , entonces  $h \in I_{gx} \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hg \in I_x \Leftrightarrow h \in gI_xg^{-1}$ ; luego

$$\boxed{I_{gx} = gI_xg^{-1}}. \tag{4.1}$$

Diremos que una acción es **transitiva** cuando tenga una única órbita, y diremos que  $x \in X$  es un punto fijo o invariante cuando  $Gx = \{x\}$ ; es decir, cuando  $I_x = G$ . El conjunto de puntos fijos se denotará  $X^G$ .

#### Ejemplos:

1.  $G$  actúa en sí mismo por traslaciones:  $g \cdot a = ga$ . Esta acción es transitiva, la isotropía es trivial,  $I_g = 1$ , y no tiene puntos fijos (salvo cuando  $G = 1$ ).

<sup>1</sup>Análogamente puede definirse el concepto de acción por la derecha; pero sólo es necesario estudiar una de estas dos clases de acciones, porque las acciones por la izquierda y por la derecha de  $G$  en  $X$  se corresponden sin más que poner  $g \cdot x = x \cdot g^{-1}$ .

2.  $G$  actúa en sí mismo por conjugación:  $g \cdot a := gag^{-1}$ . El **centro**  $Z(G) := \{a \in G : ab = ba, \forall b \in G\}$  de  $G$ , que es un subgrupo normal de  $G$ , coincide con el conjunto de puntos fijos de esta acción.
3.  $G$  actúa en el conjunto de sus subgrupos por conjugación:  $g \cdot H = gHg^{-1}$ . La órbita de un subgrupo  $H$  está formada por los subgrupos conjugados de  $H$ , y el subgrupo de isotropía es el **normalizador**  $N(H) := \{g \in G : gHg^{-1} = H\}$  de  $H$  en  $G$ , que es el mayor subgrupo de  $G$  tal que  $H \triangleleft N(H)$  (el símbolo  $H_1 \triangleleft H_2$  significa que  $H_1$  es un subgrupo normal de  $H_2$ ).
4. Si  $H$  es un subgrupo de  $G$ , entonces  $G$  actúa en el conjunto cociente  $G/H$  del siguiente modo:  $g \cdot [a] := [ga]$ . Esta acción es transitiva y el subgrupo de isotropía de  $[a]$  es precisamente  $aHa^{-1}$ .
5. Si  $H$  es un subgrupo de  $G$ , todo  $G$ -conjunto hereda una estructura de  $H$ -conjunto sin más que restringir a  $H$  la acción de  $G$ . En particular  $H$  actúa en  $G/H'$  cualquiera que sea el subgrupo  $H'$ .

**Teorema 4.1.1** *Si  $X$  es un  $G$ -conjunto, para todo  $x \in X$  se tiene un isomorfismo de  $G$ -conjuntos*

$$\boxed{G/I_x = Gx} \quad , \quad [g] \mapsto gx .$$

*En particular, si  $G$  es un grupo finito, el cardinal de cualquier órbita es un divisor del orden de  $G$ .*

*Demostración:* La aplicación  $G/I_x \rightarrow Gx, [g] \mapsto gx$ , está bien definida porque  $I_x x = x$ , es claramente morfismo de  $G$ -conjuntos y es epiyectiva por definición de  $Gx$ . Para concluir, veamos que es inyectiva:

$$g_1 x = g_2 x \Rightarrow g_1^{-1} g_2 x = x \Rightarrow g_1^{-1} g_2 \in I_x \Rightarrow [g_1] = [g_2]$$

**Fórmula de Clases:** *Si un grupo finito  $G$  de orden  $n$  actúa en un conjunto finito  $X$ , entonces*

$$|X| = |X^G| + \sum_{x_i} [G : I_{x_i}] = |X^G| + \sum_i d_i \quad , \quad 1 < d_i | n$$

*donde  $\{x_i\}$  tiene un punto en cada órbita de cardinal mayor que 1.*

*Demostración:*  $X$  es la unión disjunta de las órbitas, porque son las clases de equivalencia de una relación de equivalencia,  $|X^G|$  es el número de órbitas con un único punto, y por el teorema anterior los cardinales de las restantes órbitas coinciden con los índices  $d_i = [G : I_{x_i}]$ , que dividen a  $n$  por el teorema de Lagrange.

**Corolario 4.1.2** *Si el orden de un grupo finito  $G$  es potencia de un número primo  $p$ , entonces para todo  $G$ -conjunto finito  $X$  tenemos que*

$$|X| \equiv |X^G| \pmod{p}$$

## 4.2. $p$ -grupos

**Definición:** Sea  $p$  un número primo. Diremos que un grupo finito es un  **$p$ -grupo** si su orden es potencia de  $p$ .

**Teorema 4.2.1** *Si  $G \neq 1$  es un  $p$ -grupo, su centro no es trivial:  $Z(G) \neq 1$ .*

*Demostración:* Si consideramos la acción de  $G$  en sí mismo por conjugación, entonces  $Z(G)$  es el conjunto de puntos invariantes y 4.1.2 permite obtener que el orden del centro es múltiplo de  $p$ . Luego  $|Z(G)| \neq 1$ .

**Teorema 4.2.2** *Si  $G$  es un  $p$ -grupo, existe una sucesión creciente de subgrupos normales*

$$1 = H_0 \subset H_1 \subset \dots \subset H_{n-1} \subset H_n = G$$

*tales que  $H_i$  es de orden  $p^i$ .*

*Demostración:* Por 4.2.1 tenemos que  $Z(G) \neq 1$  y, al ser  $Z(G)$  es abeliano, 3.4.3 asegura la existencia de un subgrupo  $H \subseteq Z(G)$  de orden  $p$ , que es normal en  $G$ . Consideremos la proyección canónica  $\pi: G \rightarrow G/H$ . Procediendo por inducción sobre el orden de  $G$ , podemos suponer la existencia de una sucesión de subgrupos normales de  $G/H$

$$1 = \bar{H}_0 \subset \bar{H}_1 \subset \dots \subset \bar{H}_{n-1} = G/H$$

tal que  $|\bar{H}_i| = p^i$ . Los subgrupos  $H_i = \pi^{-1}(\bar{H}_{i-1})$  son normales en  $G$  y  $H_i/H \simeq \bar{H}_{i-1}$ , de modo que  $|H_i| = p^i$ ,  $1 \leq i \leq n$ .

**Corolario 4.2.3** *Si  $G$  es un  $p$ -grupo y  $p^i$  divide al orden de  $G$ , entonces existe algún subgrupo normal de  $G$  de orden  $p^i$ .*

### 4.3. Subgrupos de Sylow

**Definición:** Sea  $p$  un número primo. Si  $p^n$  es la mayor potencia de  $p$  que divide al orden de un grupo  $G$ , llamaremos  **$p$ -subgrupo de Sylow** de  $G$  a todo subgrupo de orden  $p^n$ .

**Primer teorema de Sylow:** *Si un número primo  $p$  divide al orden de un grupo finito  $G$ , entonces existen  $p$ -subgrupos de Sylow de  $G$ .*

*Demostración:* Procedemos por inducción sobre el orden de  $G$  y usamos la fórmula de clases para la acción de  $G$  en sí mismo por conjugación:

$$p^n m = |G| = |Z(G)| + \sum_i [G : I_{x_i}]$$

Si algún sumando  $[G : I_{x_i}]$  no es múltiplo de  $p$ , entonces  $|I_{x_i}| = p^n m'$  y cualquier  $p$ -subgrupo de Sylow de  $I_{x_i}$ , que existe por hipótesis de inducción, también es un  $p$ -subgrupo de Sylow de  $G$ .

En caso contrario la fórmula de clases muestra que  $p$  divide al orden de  $Z(G)$ . Al ser  $Z(G)$  abeliano, 3.4.3 asegura la existencia de un subgrupo  $H \subseteq Z(G)$  de orden  $p$ , que será normal en  $G$ , y podemos considerar el grupo cociente  $\pi: G \rightarrow G/H$ . Ahora, si  $\bar{P}$  es un  $p$ -subgrupo de Sylow de  $G/H$ , que existe por hipótesis de inducción, entonces  $\pi^{-1}(\bar{P})$  es un  $p$ -subgrupo de Sylow de  $G$ .

**Corolario 4.3.1** *Si una potencia  $p^i$  de un número primo  $p$  divide al orden de un grupo finito  $G$ , entonces  $G$  tiene algún subgrupo de orden  $p^i$ .*

*Demostración:* Se sigue directamente del primer teorema de Sylow y de 4.2.3.

**Teorema de Cauchy:** *Si un número primo  $p$  divide al orden de un grupo finito  $G$ , entonces  $G$  tiene algún elemento de orden  $p$ ; i.e.,  $G$  tiene algún subgrupo de orden  $p$ .*

**Segundo teorema de Sylow:** *Si  $G$  es un grupo finito y  $p$  un número primo, entonces todos los  $p$ -subgrupos de Sylow de  $G$  son conjugados.*

*Demostración:* Sean  $P$  y  $P'$  dos  $p$ -subgrupos de Sylow de  $G$ . Como el cardinal de  $G/P$  no es múltiplo de  $p$  y  $P'$  actúa en  $G/P$ , la fórmula de clases muestra la existencia de algún punto fijo  $[g] \in G/P$ . Como el subgrupo de isotropía de  $[g]$  para la acción de  $G$  sobre  $G/P$  es  $gPg^{-1}$ , se sigue que  $P' \subseteq gPg^{-1}$  y concluimos que  $P' = gPg^{-1}$  al tener ambos subgrupos el mismo orden.

**Tercer teorema de Sylow:** Si  $p$  es un número primo y  $G$  un grupo finito de orden  $p^n m$ , donde  $p \nmid m$ , entonces el número de  $p$ -subgrupos de Sylow de  $G$  divide al índice común  $m$  y es congruente con 1 módulo  $p$ .

*Demostración:* Sea  $X$  el conjunto de  $p$ -subgrupos de Sylow de  $G$  y sea  $P$  un  $p$ -subgrupo de Sylow de  $G$ . La acción de  $G$  en  $X$  por conjugación es transitiva, por el segundo teorema, y el subgrupo de isotropía de  $P$  es su normalizador  $N(P)$ . Por 4.1.1 tenemos que  $|X| = [G : N(P)]$  divide a  $[G : P] = m$ .

Consideremos ahora la acción de  $P$  en  $X$  por conjugación y veamos que el único punto fijo es  $P$ . En efecto, si  $gP'g^{-1} = P$  para todo  $g \in P$ , entonces  $P \subset N(P')$ ; luego  $P$  y  $P'$  son  $p$ -subgrupos de Sylow de  $N(P)$ , y el segundo teorema afirma que  $P' = P$ . Usando 4.1.2 concluimos que  $|X| \equiv |X^P| = 1$  (módulo  $p$ ).

## 4.4. Grupos Resolubles

**Definición:** Diremos que un grupo  $G$  es **simple** si todo subgrupo normal  $N \triangleleft G$  es trivial:  $N = 1$  ó  $N = G$ .

**Ejemplos:**

1. Todo grupo de orden primo es simple en virtud del teorema de Lagrange. De hecho es cíclico e isomorfo a  $\mathbb{Z}/p\mathbb{Z}$ .
2. Por 3.4.3, todo grupo abeliano simple tiene orden primo. *Los grupos abelianos simples son los grupos cíclicos de orden primo.*
3. Sea  $X$  un  $G$ -conjunto finito de cardinal  $n$ . Si la acción no es trivial (i.e.,  $X^G \neq X$ ) y el orden de  $G$  es mayor que  $n!$ , entonces  $G$  no es simple, porque el núcleo de la representación  $G \rightarrow \text{Bij}(X) = S_n$  es un subgrupo normal no trivial. En particular, si  $G$  tiene un subgrupo de índice  $n$  y  $n! < |G|$ , entonces  $G$  no es simple.
4. Usando los teoremas de Sylow, puede comprobarse caso a caso que todo grupo simple de orden menor que 60 es de orden primo, y por tanto abeliano.
5. En 4.5.2 veremos que los grupos alternados  $A_n$  son simples cuando  $n \geq 5$ . Como  $A_5$  tiene orden 60, es el grupo simple no abeliano de menor orden.
6. El grupo alternado  $A_4$  no es simple, porque un subgrupo normal de  $A_4$  es el grupo de Klein

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

Es claro que todo grupo finito  $G$  admite una sucesión de subgrupos

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = G$$

tal que los cocientes sucesivos  $H_i/H_{i-1}$ ,  $1 \leq i \leq n$ , son grupos simples. En este sentido todo grupo finito está compuesto de grupos simples, y los que estén compuestos por grupos simples abelianos se llaman resolubles:

**Definición:** Diremos que un grupo finito  $G$  es **resoluble** si existe alguna sucesión de subgrupos

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = G$$

tal que los cocientes sucesivos  $H_i/H_{i-1}$ ,  $1 \leq i \leq n$ , son grupos cíclicos de orden primo. Tales sucesiones reciben el nombre de resoluciones de  $G$ .

**Teorema 4.4.1** *El grupo simétrico  $S_n$  no es resoluble cuando  $n \geq 5$ .*

*Demostración:* Cuando  $n \geq 5$ , todo 3-ciclo  $(ijk)$  es el conmutador de otros dos 3-ciclos:

$$(ijk) = \sigma\tau\sigma^{-1}\tau^{-1} \quad , \quad \sigma = (ijl) \quad , \quad \tau = (ikm)$$

Si existiera una sucesión de subgrupos  $1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{d-1} \triangleleft H_d = S_n$  cuyos cocientes sucesivos fueran abelianos, entonces  $H_{i-1}$  contiene el conmutador de dos elementos cualesquiera de  $H_i$  para todo  $1 \leq i \leq d$ . Luego  $H_{i-1}$  contiene todos los 3-ciclos cuando  $H_i$  los contiene, y se llega al absurdo de que el subgrupo 1 contiene todos los 3-ciclos.

**Teorema 4.4.2** *Si un grupo finito es resoluble, todos sus subgrupos también son resolubles.*

*Demostración:* Sea  $G$  un grupo finito resoluble y  $1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$  una resolución. Si  $H$  es un subgrupo de  $G$  y ponemos  $H'_i = H_i \cap H$ , entonces  $H'_{i-1}$  es un subgrupo normal de  $H'_i$  y  $H'_i/H'_{i-1}$  es (isomorfo a) un subgrupo de  $H_i/H_{i-1}$  para todo  $1 \leq i \leq n$ . Como el orden de  $H_i/H_{i-1}$  es primo, el teorema de Lagrange afirma que  $H'_i/H'_{i-1} = 1$  ó  $H'_i/H'_{i-1} = H_i/H_{i-1}$ . Eliminando las repeticiones en la cadena  $1 = H'_0 \subseteq H'_1 \subseteq \dots \subseteq H'_n = H$  obtenemos una sucesión cuyos cocientes sucesivos son de orden primo, y concluimos que  $H$  es resoluble.

**Teorema 4.4.3** *Sea  $H$  un subgrupo normal de un grupo finito  $G$ . La condición necesaria y suficiente para que  $G$  sea resoluble es que  $H$  y  $G/H$  sean resolubles.*

*Demostración:* Si  $G$  es resoluble,  $H$  es resoluble por 4.4.2. En cuanto a  $G/H$ , consideremos una resolución  $1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$ , la proyección canónica  $\pi: G \rightarrow G/H$ , y pongamos  $H'_i = \pi(H_i)$ . Entonces  $H'_{i-1}$  es un subgrupo normal de  $H'_i$  y  $H'_i/H'_{i-1}$  es (isomorfo a) un cociente de  $H_i/H_{i-1}$  para todo  $1 \leq i \leq n$ . Como el orden de  $H_i/H_{i-1}$  es primo, el teorema de Lagrange afirma que  $H'_i/H'_{i-1} = 1$  ó  $H'_i/H'_{i-1} = H_i/H_{i-1}$ . Eliminando ahora las posibles repeticiones en la cadena  $1 = H'_0 \subseteq H'_1 \subseteq \dots \subseteq H'_n = G/H$  obtenemos una sucesión cuyos cocientes sucesivos son de orden primo, y concluimos que  $G/H$  es resoluble.

Recíprocamente, si  $H$  y  $G/H$  son resolubles, consideramos la proyección canónica  $\pi: G \rightarrow G/H$  y sendas resoluciones

$$\begin{aligned} 1 &= H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = H \\ 1 &= H'_0 \triangleleft H'_1 \triangleleft \dots \triangleleft H'_{d-1} \triangleleft H'_d = G/H \end{aligned}$$

Es sencillo comprobar que en la sucesión creciente de subgrupos

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = \pi^{-1}(H'_0) \triangleleft \pi^{-1}(H'_1) \triangleleft \dots \triangleleft \pi^{-1}(H'_d) = G$$

los cocientes sucesivos son de orden primo, y concluimos que  $G$  es resoluble.

**Corolario 4.4.4** *Todo grupo finito abeliano es resoluble.*

*Demostración:* Procediendo por inducción sobre el orden, si  $H$  es un subgrupo de orden primo de un grupo abeliano finito  $G$ , entonces  $H \triangleleft G$  y el grupo  $G/H$  es resoluble por hipótesis de inducción, así que 4.4.3 permite concluir.

**Corolario 4.4.5** *Sea  $G$  un grupo finito. Si existe una sucesión de subgrupos*

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$$

*tal que los cocientes sucesivos  $H_i/H_{i-1}$  son grupos abelianos, entonces  $G$  es resoluble.*

## 4.5. Grupos Simétricos

**Lema 4.5.1** Si  $n \geq 3$ , toda permutación par es producto de ciclos de orden 3

*Demostración:* Bastará probar que el producto  $(a_1 a_2)(b_1 b_2)$  de dos trasposiciones siempre es producto de 3-ciclos. Ahora bien, tenemos que

$$\begin{aligned} (a_1 a_2)(b_1 b_2) &= (a_1 a_2 b_1)(a_2 b_1 b_2) && \text{cuando las trasposiciones son disjuntas} \\ (a_1 a_2)(b_1 b_2) &= (a_2 a_1 b_2) && \text{cuando } a_1 = b_1 \end{aligned}$$

**Teorema 4.5.2** El grupo alternado  $A_n$  es simple cuando  $n \neq 4$ .

*Demostración:* Si  $n \leq 3$ , el orden de  $A_n$  es 1 ó 3, así que los únicos subgrupos de  $A_n$  son los triviales.

Si  $n \geq 5$  y  $H \neq 1$  es un subgrupo normal de  $A_n$ , vamos a probar que  $H = A_n$ . Sea  $\alpha$  un elemento de  $H$  que deje fijos el mayor número de elementos, exceptuando la identidad, y consideremos su descomposición en producto de ciclos disjuntos. Volviendo a numerar los elementos si fuera preciso podemos suponer que

$$\alpha = (1, 2, \dots, d_1)(d_1 + 1, \dots, d_1 + d_2)(\dots$$

y que  $d_1, d_2, \dots$  es una sucesión decreciente. Sea  $s \geq 1$  el número de elementos que  $\alpha$  no deja fijos. Es claro que  $s \geq 3$  y vamos a ver que  $s \geq 4$  es imposible:

$s \geq 5$ . Sea  $\beta = (345)$ . Como  $\beta \in A_n$  y  $H$  es un subgrupo normal de  $A_n$ ,  $\beta\alpha\beta^{-1} \in H$  y  $\beta\alpha\beta^{-1}\alpha^{-1} \in H$ . Ahora bien,  $\beta\alpha\beta^{-1}\alpha^{-1}$  deja fijos el 2 y también todos los elementos que  $\alpha$  deje fijos; luego  $\beta\alpha\beta^{-1}\alpha^{-1} = 1$  y  $\alpha\beta = \beta\alpha$ . Se sigue que  $\alpha(2) \neq 3$ , de modo que  $\alpha(2) = 1$  y  $\alpha = (12)(34)(56)\dots \Rightarrow \alpha\beta(3) \neq \beta\alpha(3)$ ; luego  $\alpha\beta \neq \beta\alpha$  y concluimos que este caso es imposible.

$s = 4$ . En este caso  $\alpha = (12)(34)$  porque la permutación  $(1234)$  es impar. Sea  $\beta = (345)$ . De nuevo  $\beta\alpha\beta^{-1}\alpha^{-1} \in H$  y  $\beta\alpha\beta^{-1}\alpha^{-1} = (354)$  deja fijos más elementos que  $\alpha$ , en contradicción con la elección de  $\alpha$ . Este caso también es imposible.

Luego  $\alpha = (123)$  y concluimos que  $H$  contiene un ciclo de orden 3.

De acuerdo con el lema anterior, para concluir que  $H = A_n$  basta probar que  $H$  contiene todos los 3-ciclos. Sea  $\sigma = (ijk)$  un 3-ciclo y consideremos una permutación  $\tau$  que transforme 1,2,3 en  $i, j, k$ :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ i & j & k & l & m & \dots \end{pmatrix}$$

Intercambiando  $l$  y  $m$  si fuera preciso podemos suponer que  $\tau$  es par; luego  $\sigma = (ijk) = \tau(123)\tau^{-1} = \tau\alpha\tau^{-1} \in H$  y todos los 3-ciclos están en  $H$ .

**Corolario 4.5.3** Si  $n \neq 4$ , los únicos subgrupos normales de  $S_n$  son 1,  $A_n$  y  $S_n$ .

*Demostración:* Si  $H \triangleleft S_n$ , entonces  $H \cap A_n \triangleleft A_n$  y pueden darse dos casos:

1.  $H \cap A_n = A_n$ . En este caso  $A_n \subseteq H$  y concluimos que  $H = A_n$  ó  $H = S_n$ , porque el índice de  $A_n$  en  $S_n$  es 2.
2.  $H \cap A_n = 1$ . En este caso todas los elementos de  $H$ , salvo la identidad, son permutaciones impares. Luego  $H$  sólo puede tener un elemento  $\sigma \neq 1$ , así que toda permutación que tenga la misma forma que  $\sigma$  debe coincidir con  $\sigma$ , lo cual es imposible cuando  $n \geq 3$  (el caso  $n = 2$  es inmediato). Concluimos que  $H = 1$ .

## Capítulo 5

# Producto Tensorial

### 5.1. Producto Tensorial de Módulos

Sean  $M$ ,  $N$  y  $P$  tres  $A$ -módulos. Una aplicación  $f: M \times N \rightarrow P$  es  **$A$ -bilineal** cuando

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

El conjunto de todas las aplicaciones  $A$ -bilineales de  $M$  y  $N$  en  $P$  se denota  $\text{Bil}_A(M, N; P)$  y es un  $A$ -módulo con las siguientes operaciones:

$$\begin{aligned} (f + g)(m, n) &= f(m, n) + g(m, n) \\ (a \cdot f)(m, n) &= a \cdot f(m, n) \end{aligned}$$

**Definición:** Consideremos el  $A$ -módulo libre  $L$  de base  $M \times N$ , de modo que los elementos de  $L$  son las combinaciones lineales formales

$$\sum_{i=1}^n a_i \cdot (m_i, n_i) \quad , \quad a_i \in A, m_i \in M, n_i \in N$$

Sea  $R$  el submódulo de  $L$  generado por los elementos de la forma

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

Llamaremos **producto tensorial** de  $M$  y  $N$  sobre el anillo  $A$  al  $A$ -módulo cociente  $L/R$  y lo denotaremos  $M \otimes_A N$ . Para cada elemento  $(m, n)$  de  $M \times N$ , entendido como elemento de  $L$ , su imagen en  $M \otimes_A N$  se denotará  $m \otimes n$ .

Por construcción, tales elementos  $m \otimes n$  generan el producto tensorial  $M \otimes_A N$ . De hecho, todo elemento de  $M \otimes_A N$  descompone (aunque no de modo único) en la forma

$$\sum_{i=1}^n m_i \otimes n_i$$

En particular, si  $\{m_i\}_{i \in I}$  es un sistema de generadores de  $M$  y  $\{n_j\}_{j \in J}$  es un sistema de generadores de  $N$ , entonces  $\{m_i \otimes n_j\}_{i \in I, j \in J}$  es un sistema de generadores de  $M \otimes_A N$ . Además, de acuerdo con la definición de  $R$ , tenemos que

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

Es decir, la aplicación canónica  $M \times N \xrightarrow{\otimes} M \otimes_A N$ ,  $(m, n) \mapsto m \otimes n$ , es  $A$ -bilineal.  
En particular  $0 \otimes n = 0$  y  $m \otimes 0 = 0$ .

**Propiedad Universal del Producto Tensorial:** Sean  $M$  y  $N$  dos módulos sobre un anillo  $A$ . Si  $f: M \times N \rightarrow P$  es una aplicación  $A$ -bilineal, existe un único morfismo de  $A$ -módulos  $\phi: M \otimes_A N \rightarrow P$  tal que  $\phi(m \otimes n) = f(m, n)$ :

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

*Demostración:* La unicidad de tal morfismo se debe a que los elementos  $m \otimes n$  generan  $M \otimes_A N$  como  $A$ -módulo. En cuanto a la existencia, la condición de que  $f$  sea  $A$ -bilineal expresa precisamente que el morfismo de  $A$ -módulos

$$\bar{f}: L \longrightarrow P, \quad \bar{f}\left(\sum_i a_i(m_i, n_i)\right) = \sum_i a_i f(m_i, n_i)$$

se anula sobre los generadores del submódulo  $R$ ; luego sobre  $R$  y, por la propiedad universal del módulo cociente, induce un morfismo de  $A$ -módulos

$$\phi: L/R = M \otimes_A N \longrightarrow P, \quad \phi(m \otimes n) = \bar{f}(m, n) = f(m, n)$$

**Nota:** Una construcción análoga puede hacerse para cualquier familia finita de  $A$ -módulos  $M_1, \dots, M_n$ , obteniéndose un  $A$ -módulo  $M_1 \otimes_A \dots \otimes_A M_n$  con una propiedad universal similar.

Como ejemplo de utilización de tal propiedad universal, veamos el comportamiento del producto tensorial frente a los morfismos. Sean  $f: M \rightarrow M'$  y  $g: N \rightarrow N'$  morfismos de  $A$ -módulos. La aplicación

$$M \times N \longrightarrow M' \otimes_A N', \quad (m, n) \mapsto f(m) \otimes g(n)$$

es claramente  $A$ -bilineal; luego existe un único morfismo de  $A$ -módulos

$$f \otimes g: M \otimes_A N \longrightarrow M' \otimes_A N'$$

tal que  $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ . Este producto tensorial de morfismos es compatible, en un sentido obvio, con la suma, el producto por elementos de  $A$  y la composición de morfismos:

$$\begin{aligned} (af + bf') \otimes g &= a(f \otimes g) + b(f' \otimes g) \\ f \otimes (ag + bg') &= a(f \otimes g) + b(f \otimes g') \\ (f' \circ f) \otimes (g' \circ g) &= (f' \otimes g') \circ (f \otimes g) \end{aligned}$$

**Teorema 5.1.1** *Existen isomorfismos naturales de  $A$ -módulos*

1.  $(M \otimes_A N) \otimes_A P = M \otimes_A N \otimes_A P = M \otimes_A (N \otimes_A P)$   
 $(m \otimes n) \otimes p = m \otimes n \otimes p = m \otimes (n \otimes p)$ .
2.  $M \otimes_A N = N \otimes_A M$ ,  $m \otimes n = n \otimes m$ .
3.  $A \otimes_A M = M$ ,  $a \otimes m = am$ .
4.  $(\bigoplus_i M_i) \otimes_A N = \bigoplus_i (M_i \otimes_A N)$ ,  $(\sum_i m_i) \otimes n = \sum_i (m_i \otimes n)$ .

*Demostración:* En cada caso basta definir los correspondientes morfismos, pues entonces es evidente que sus composiciones son la identidad sobre un sistema de generadores. En cuanto a la definición de tales morfismos, haremos las siguientes observaciones:

- 1) Para cada elemento  $p \in P$ , la aplicación

$$M \times N \longrightarrow M \otimes_A N \otimes_A P, \quad (m, n) \mapsto m \otimes n \otimes p$$

es  $A$ -bilineal, así que define un morfismo de  $A$ -módulos

$$f_p: M \otimes_A N \longrightarrow M \otimes_A N \otimes_A P, \quad f_p(m \otimes n) = m \otimes n \otimes p$$

Ahora la aplicación  $(M \otimes_A N) \times P \rightarrow M \otimes_A N \otimes_A P$ ,  $(x, p) \mapsto f_p(x)$  es bilineal e induce el morfismo de  $A$ -módulos  $(M \otimes_A N) \otimes_A P \rightarrow M \otimes_A N \otimes_A P$  deseado.

3) La aplicación  $M \rightarrow A \otimes_A M$ ,  $m \mapsto 1 \otimes m$ , es un morfismo de  $A$ -módulos. Por otra parte, la aplicación  $A \times M \rightarrow M$ ,  $(a, m) \mapsto am$ , es  $A$ -bilineal e induce el morfismo de  $A$ -módulos  $A \otimes_A M \rightarrow M$  deseado.

4) Sea  $M = \bigoplus_i M_i$ . La aplicación

$$M \times N \rightarrow \bigoplus_i (M_i \otimes_A N), \quad (\sum_i m_i, n) \mapsto \sum_i m_i \otimes n$$

es  $A$ -bilineal e induce el morfismo  $M \otimes_A N \rightarrow \bigoplus_i (M_i \otimes_A N)$  deseado.

Por otra parte, las inclusiones canónicas  $j_i: M_i \rightarrow M$  definen morfismos de  $A$ -módulos  $j_i \otimes 1: M_i \otimes_A N \rightarrow M \otimes_A N$  que inducen el morfismo inverso  $\bigoplus_i (M_i \otimes_A N) \rightarrow M \otimes_A N$ .

**Corolario 5.1.2** *Si  $L$  es un  $A$ -módulo libre de base  $(e_i)_{i \in I}$  y  $L'$  es un  $A$ -módulo libre de base  $(e'_j)_{j \in J}$ , entonces  $L \otimes_A L'$  es un  $A$ -módulo libre de base  $(e_i \otimes e'_j)_{i \in I, j \in J}$ .*

**Teorema 5.1.3** *Sea  $M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$  una sucesión exacta de morfismos de  $A$ -módulos. Para todo  $A$ -módulo  $N$  tenemos que la siguiente sucesión es exacta:*

$$M' \otimes_A N \xrightarrow{i \otimes 1} M \otimes_A N \xrightarrow{p \otimes 1} M'' \otimes_A N \longrightarrow 0$$

*Demostración:* Es obvio que  $p \otimes 1$  es epiyectiva cuando  $p$  lo es, y que  $(p \otimes 1)(i \otimes 1) = (pi) \otimes 1 = 0$  cuando  $pi = 0$ . Queda por ver que  $\text{Ker } p \otimes 1 \subseteq \text{Im } i \otimes 1$ .

La aplicación  $M'' \times N \rightarrow (M \otimes_A N)/\text{Im } i \otimes 1$ ,  $(m'', n) \mapsto [m \otimes n]$ , donde  $p(m) = m''$ , está bien definida, porque si  $p(\bar{m}) = m''$ , entonces  $\bar{m} = m + i(m')$  para algún  $m' \in M'$  y

$$[m \otimes n] = [(m + i(m')) \otimes n] = [m \otimes n + (i \otimes 1)(m' \otimes n)] = [m \otimes n]$$

y es  $A$ -bilineal. Luego tenemos un morfismo de  $A$ -módulos  $\phi: M'' \otimes_A N \rightarrow (M \otimes_A N)/\text{Im } i \otimes 1$  tal que  $\phi(m'' \otimes n) = [m \otimes n]$ . Como  $\pi := \phi(p \otimes 1): M \otimes_A N \rightarrow (M \otimes_A N)/\text{Im } i \otimes 1$  es claramente la proyección canónica, concluimos que  $\text{Ker } (p \otimes 1) \subseteq \text{Ker } \pi = \text{Im } i \otimes 1$ .

**Corolario 5.1.4**  $(A/\mathfrak{a}) \otimes_A M = M/\mathfrak{a}M$  para todo ideal  $\mathfrak{a}$  de  $A$ .

*Demostración:* La sucesión exacta  $\mathfrak{a} \rightarrow A \rightarrow A/\mathfrak{a} \rightarrow 0$  induce una sucesión exacta

$$\mathfrak{a} \otimes_A M \longrightarrow A \otimes_A M \longrightarrow (A/\mathfrak{a}) \otimes_A M \longrightarrow 0$$

Para concluir basta observar que  $A \otimes_A M = M$  y que el submódulo  $\mathfrak{a}M$  es la imagen del morfismo  $\mathfrak{a} \otimes_A M \rightarrow M$ ,  $a \otimes m \mapsto am$ .

**Nota:** Aunque un morfismo de  $A$ -módulos  $i: M' \rightarrow M$  sea inyectivo, puede ocurrir que el morfismo  $i \otimes 1: M' \otimes_A N \rightarrow M \otimes_A N$  no lo sea. Por ejemplo, si  $A = \mathbb{Q}[t]$ , el morfismo  $t: A \rightarrow A$  es inyectivo mientras que el morfismo  $t \otimes 1: A \otimes_A (A/tA) \rightarrow A \otimes_A (A/tA)$  es nulo y  $A \otimes_A (A/tA) = A/tA \neq 0$ . No obstante, cualquier producto tensorial  $(-)\otimes_A N$  transforma sucesiones exactas escindidas en sucesiones exactas escindidas:

**Corolario 5.1.5** Sea  $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$  una sucesión exacta de morfismos de  $A$ -módulos. Si la sucesión escinde, entonces para todo  $A$ -módulo  $N$  tenemos que la siguiente sucesión es exacta y escinde:

$$0 \longrightarrow M' \otimes_A N \xrightarrow{i \otimes 1} M \otimes_A N \xrightarrow{p \otimes 1} M'' \otimes_A N \longrightarrow 0$$

En particular, si  $0 \rightarrow E' \xrightarrow{i} E \xrightarrow{p} E'' \rightarrow 0$  es una sucesión exacta de  $k$ -espacios vectoriales, entonces para todo  $k$ -espacio vectorial  $F$  tenemos que la siguiente sucesión es exacta:

$$0 \longrightarrow E' \otimes_k F \xrightarrow{i \otimes 1} E \otimes_k F \xrightarrow{p \otimes 1} E'' \otimes_k F \longrightarrow 0$$

*Demostración:* Si la sucesión escinde, de acuerdo con 1.2.1 existe un morfismo de  $A$ -módulos  $r: M \rightarrow M'$  tal que  $r \circ i = Id_{M'}$ , entonces  $(r \otimes 1) \circ (i \otimes 1) = Id_{M' \otimes_A N}$  y concluimos que el morfismo  $i \otimes 1$  es inyectivo y la sucesión escinde.

En cuanto a la última afirmación, baste observar que toda sucesión exacta corta de  $k$ -espacios vectoriales escinde porque todo subespacio vectorial admite un suplementario.

## 5.2. Cambio de Base

Sea  $j: A \rightarrow B$  un morfismo de anillos y consideremos en  $B$  la estructura de  $A$ -módulo inducida:  $a \cdot b = j(a)b$ . Sea  $M$  un  $A$ -módulo. Cada elemento  $b \in B$  define un endomorfismo  $1 \otimes b: M \otimes_A B \rightarrow M \otimes_A B$  y así obtenemos una estructura de  $B$ -módulo en  $M \otimes_A B$ , que viene dada por el siguiente producto:

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

**Definición:** El  $B$ -módulo así definido se denotará  $M_B$  y diremos que se obtiene de  $M$  mediante el **cambio de base**  $j: A \rightarrow B$ . Si  $f: M \rightarrow N$  es un morfismo de  $A$ -módulos, entonces  $f \otimes 1: M_B \rightarrow N_B$ ,  $(f \otimes 1)(m \otimes b) = f(m) \otimes b$ , es un morfismo de  $B$ -módulos y diremos que se obtiene de  $f$  mediante el cambio de base  $j: A \rightarrow B$ .

Tenemos un morfismo canónico de  $A$ -módulos  $M \rightarrow M_B$ ,  $m \mapsto m \otimes 1$ , llamado morfismo de **cambio de base**.

**Proposición 5.2.1** Si  $(e_1, \dots, e_n)$  es una base de un  $A$ -módulo libre  $L$ , entonces  $L_B$  es un  $B$ -módulo libre de base  $(e_1 \otimes 1, \dots, e_n \otimes 1)$ .

*Demostración:* El producto tensorial conmuta con sumas directas.

**Teorema 5.2.2** Sea  $A \rightarrow B$  un morfismo de anillos y sea  $M$  un  $A$ -módulo. Para todo  $B$ -módulo  $N$  se tiene un isomorfismo natural de  $B$ -módulos

$$(M \otimes_A B) \otimes_B N = M \otimes_A N ; \quad (m \otimes b) \otimes n = m \otimes (bn)$$

donde  $M \otimes_A N$  es  $B$ -módulo con la estructura que definen los morfismos

$$1 \otimes b: M \otimes_A N \rightarrow M \otimes_A N$$

*Demostración:* Si  $n \in N$ , la aplicación

$$M \times B \longrightarrow M \otimes_A N, \quad (m, b) \mapsto m \otimes bn$$

es  $A$ -bilineal e induce un morfismo de  $A$ -módulos  $f_n: M_B \rightarrow M \otimes_A N$  que es  $B$ -lineal. Ahora la aplicación

$$M_B \times N \longrightarrow M \otimes_A N, \quad (x, n) \mapsto f_n(x)$$

es  $B$ -bilineal e induce el morfismo de  $B$ -módulos  $(M_B) \otimes_B N \rightarrow M \otimes_A N$  deseado. El morfismo inverso viene inducido por la aplicación  $A$ -bilineal

$$M \times N \longrightarrow (M \otimes_A B) \otimes_B N, \quad (m, n) \mapsto (m \otimes 1) \otimes n$$

$$\begin{aligned}\text{Corolario 5.2.3} \quad (M \otimes_A M')_B &= (M_B) \otimes_B (M'_B) \\ (m \otimes m') \otimes 1 &= (m \otimes 1) \otimes (m' \otimes 1)\end{aligned}$$

*Demostración:*

$$(M \otimes_A B) \otimes_B (M' \otimes_A B) = M \otimes_A (M' \otimes_A B) = (M \otimes_A M') \otimes_A B$$

$$\text{Corolario 5.2.4} \quad (M_B)_C = M_C \quad , \quad (m \otimes b) \otimes c = m \otimes bc.$$

*Demostración:*  $(M \otimes_A B) \otimes_B C = M \otimes_A C$ .

### 5.3. Álgebras

**Definición:** Sea  $k$  un cuerpo. Llamaremos **álgebra** sobre  $k$  a todo anillo  $A$  dotado de un morfismo de anillos  $j: k \rightarrow A$ .

Dada una  $k$ -álgebra  $A$ , el morfismo estructural  $j: k \rightarrow A$  induce en  $A$  una estructura de  $k$ -espacio vectorial:  $\lambda \cdot a = j(\lambda)a$ ,  $\lambda \in k$ ,  $a \in A$ . Por eso, cuando no origine confusión,  $j(\lambda)$  se denotará  $\lambda$  y diremos que es **constante**. Diremos que una  $k$ -álgebra  $A$  es **finita** si lo es la dimensión de  $A$  como  $k$ -espacio vectorial, en cuyo caso recibe el nombre de **grado** de  $A$  sobre  $k$  y se denota  $[A : k]$ .

Llamaremos **extensión** de  $k$  a toda  $k$ -álgebra  $K$  que sea cuerpo.

Dadas dos  $k$ -álgebras  $A$  y  $B$ , diremos que una aplicación  $f: A \rightarrow B$  es un **morfismo** de  $k$ -álgebras si es un morfismo de anillos y  $f(\lambda) = \lambda$  para todo  $\lambda \in k$ . Es decir, cuando  $f$  sea morfismo de anillos y  $k$ -lineal. El conjunto de todos los morfismos de  $k$ -álgebras de  $A$  en  $B$  se denotará  $\text{Hom}_{k\text{-alg}}(A, B)$ . Diremos que un morfismo de  $k$ -álgebras es un **isomorfismo** si admite un morfismo de  $k$ -álgebras inverso.

Es sencillo comprobar que las composiciones de morfismos de  $k$ -álgebras también lo son, que los isomorfismos de  $k$ -álgebras son los morfismos biyectivos, etc.

**Definición:** Diremos que un subanillo  $B$  de una  $k$ -álgebra  $A$  es una **subálgebra** cuando  $\lambda \in B$  para todo  $\lambda \in k$  (i.e.,  $B$  contiene la imagen del morfismo estructural  $k \rightarrow A$ ).

Dada una familia  $\{a_1, \dots, a_n\}$  de elementos de  $A$ , el subanillo

$$k[a_1, \dots, a_n] = \{p(a_1, \dots, a_n); p \in k[x_1, \dots, x_n]\}$$

es la menor subálgebra de  $A$  que contiene a la familia dada y diremos que es la **subálgebra generada** por  $a_1, \dots, a_n$ . Si  $K$  es una extensión de un cuerpo  $k$  y  $\alpha_1, \dots, \alpha_n \in K$ . Entonces

$$k(\alpha_1, \dots, \alpha_n) = \{a/b; a, b \in k[\alpha_1, \dots, \alpha_n], b \neq 0\}$$

es el menor subanillo de  $K$  que es cuerpo y contiene a  $k$  y a  $\alpha_1, \dots, \alpha_n$ . Como contiene a  $k$  y es un cuerpo,  $k(\alpha_1, \dots, \alpha_n)$  es una extensión de  $k$ , y diremos que es la extensión de  $k$  **generada** por  $\alpha_1, \dots, \alpha_n$ . Está formada por todos los elementos de  $K$  que pueden obtenerse a partir de  $\alpha_1, \dots, \alpha_n$  y de elementos de  $k$  con un número finito de sumas, restas, productos y divisiones por elementos no nulos.

## 5.4. Producto Tensorial de Álgebras

Sean  $A$  y  $B$  dos  $k$ -álgebras.

La aplicación  $A \times B \times A \times B \rightarrow A \otimes_k B$ ,  $(a, b, a', b') \mapsto (aa') \otimes (bb')$ , es claramente multilinear; luego induce una aplicación lineal

$$A \otimes_k B \otimes_k A \otimes_k B \rightarrow A \otimes_k B$$

que se corresponde con una aplicación bilineal

$$(A \otimes_k B) \times (A \otimes_k B) \xrightarrow{\cdot} A \otimes_k B$$

Obtenemos así una operación en el espacio vectorial  $A \otimes_k B$ , que denotaremos multiplicativamente. Por definición tenemos que

$$\left(\sum_i a_i \otimes b_i\right) \cdot \left(\sum_j a_j \otimes b_j\right) = \sum_{ij} (a_i a_j) \otimes (b_i b_j)$$

y este producto define en  $A \otimes_k B$  una estructura de anillo. Además, la aplicación  $k \rightarrow A \otimes_k B$ ,  $\lambda \mapsto \lambda \otimes 1 = 1 \otimes \lambda$ , es morfismo de anillos, así que  $A \otimes_k B$  es una  $k$ -álgebra, y tenemos morfismos de  $k$ -álgebras canónicos  $j_1: A \rightarrow A \otimes_k B$ ,  $j_1(a) = a \otimes 1$ , y  $j_2: B \rightarrow A \otimes_k B$ ,  $j_2(b) = 1 \otimes b$ .

Además, si  $f: A \rightarrow A'$  y  $g: B \rightarrow B'$  son morfismos de  $k$ -álgebras, entonces la aplicación  $f \otimes g: A \otimes_k B \rightarrow A' \otimes_k B'$  también es morfismo de  $k$ -álgebras.

**Definición:** Sea  $A$  una  $k$ -álgebra. Si  $L$  es una extensión de  $k$ , el morfismo canónico  $j_2: L \rightarrow A \otimes_k L$  define una estructura de  $L$ -álgebra en  $A \otimes_k L$ . Esta  $L$ -álgebra se denotará  $A_L$  y diremos que se obtiene de la  $k$ -álgebra  $A$  por el **cambio de base**  $k \rightarrow L$ .

Si  $f: A \rightarrow B$  un morfismo de  $k$ -álgebras,  $f \otimes 1: A_L \rightarrow B_L$ ,  $(f \otimes 1)(a \otimes \lambda) = f(a) \otimes \lambda$ , es un morfismo de  $L$ -álgebras, que se denotará  $f_L$  y diremos que se obtiene de  $f$  mediante el cambio de base  $k \rightarrow L$ . Tenemos un morfismo de  $k$ -álgebras canónico  $j: A \rightarrow A_L$ ,  $j(a) = a \otimes 1$ , llamado morfismo de **cambio de base**.

**Propiedad universal del cambio de base:** Sea  $A$  una  $k$ -álgebra y  $L$  una extensión de  $k$ . Si  $B$  es una  $L$ -álgebra y  $f: A \rightarrow B$  es un morfismo de  $k$ -álgebras, entonces existe un único morfismo de  $L$ -álgebras  $\psi: A_L \rightarrow B$  tal que  $\psi(a \otimes 1) = f(a)$ :

$$\text{Hom}_{k\text{-alg}}(A, B) = \text{Hom}_{L\text{-alg}}(A_L, B)$$

*Demostración:* La unicidad se debe a que  $\psi$  ha de ser

$$\psi\left(\sum_i a_i \otimes \lambda_i\right) = \sum_i \psi(\lambda_i \cdot j(a_i)) = \sum_i \lambda_i f(a_i)$$

En cuanto a la existencia, el morfismo  $f: A \rightarrow B$  y el morfismo estructural  $L \rightarrow B$  inducen un morfismo de  $k$ -álgebras  $\psi: A \otimes_k L \rightarrow B$  que, de hecho, es morfismo de  $L$ -álgebras y verifica que  $\psi(a \otimes 1) = f(a)$ .

**Corolario 5.4.1**  $k[x_1, \dots, x_n] \otimes_k L = L[x_1, \dots, x_n]$   
 $q(x_1, \dots, x_n) \otimes \lambda = \lambda q(x_1, \dots, x_n)$

**Corolario 5.4.2**  $(k[x_1, \dots, x_n]/(p_1, \dots, p_r)) \otimes_k L = L[x_1, \dots, x_n]/(p_1, \dots, p_r)$   
 $[q(x_1, \dots, x_n)] \otimes \lambda = [\lambda q(x_1, \dots, x_n)]$

## Capítulo 6

# Álgebras Finitas

En adelante  $k$  denotará un cuerpo (conmutativo) arbitrario.

### 6.1. Raíces

**Definición:** Sea  $p(x) = c_0x^n + \dots + c_n$  un polinomio con coeficientes en un cuerpo  $k$ . Diremos que un elemento  $\alpha$  de una extensión  $L$  de  $k$  es una **raíz** de  $p(x)$  en  $L$  si  $p(\alpha) := c_0\alpha^n + \dots + c_n = 0$ . En tal caso, la regla de Ruffini afirma que  $p(x)$  es múltiplo de  $x - \alpha$  en  $L[x]$  y, si  $p(x)$  no es nulo, llamaremos **multiplicidad** de la raíz  $\alpha$  de  $p(x)$  al mayor número natural  $m$  tal que  $(x - \alpha)^m$  divida a  $p(x)$  en  $L[x]$ .

Las raíces de multiplicidad 1 reciben el nombre de raíces **simples**. Las raíces que no sean simples se denominan **múltiples**.

Sea  $p(x)$  un polinomio no constante con coeficientes en un cuerpo  $k$ . Si  $L$  es una extensión de  $k$  y descomponemos  $p(x)$  en producto de polinomios irreducibles en  $L[x]$ :

$$p(x) = c(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} \cdot q_1(x)^{n_1} \cdots q_s(x)^{n_s}$$

donde  $q_1(x), \dots, q_s(x)$  son polinomios unitarios irreducibles en  $L[x]$  distintos entre sí y de grado mayor que 1 (eventualmente  $r$  o  $s$  puede ser nulo), entonces las raíces de  $p(x)$  en  $L$  son precisamente  $\alpha_1, \dots, \alpha_r$  y sus multiplicidades respectivas son  $m_1, \dots, m_r$ . Tomando grados concluimos que

$$m_1 + \dots + m_r \leq \text{gr } p(x)$$

y diremos que  $p(x)$  tiene **todas sus raíces** en  $L$  cuando se dé la igualdad, lo que equivale a que  $s = 0$ ; es decir, a que en la descomposición de  $p(x)$  en  $L[x]$  no existan factores irreducibles de grado mayor que 1. Resumiendo:

**Teorema 6.1.1** *Sea  $p(x)$  un polinomio no constante con coeficientes en un cuerpo  $k$ . La suma de las multiplicidades de las raíces de  $p(x)$  en cualquier extensión  $L$  de  $k$  no supera al grado de  $p(x)$  y la condición necesaria y suficiente para que coincida con el grado de  $p(x)$  es que  $p(x)$  descomponga en  $L[x]$  en producto de polinomios de grado 1.*

**Corolario 6.1.2** *Sea  $L$  una extensión de un cuerpo  $k$  y sea  $p(x) = c_0x^n + \dots + c_n$  un polinomio de grado  $n \geq 1$  con coeficientes en  $k$  que tenga todas sus raíces en  $L$ . Si  $\alpha_1, \dots, \alpha_n$  son las raíces de  $p(x)$  en  $L$ , cada una repetida tantas veces como indique su multiplicidad, entonces*

$$p(x) = c_0(x - \alpha_1) \cdots (x - \alpha_n)$$

**Corolario 6.1.3** Sea  $p(x) = c_0x^n + \dots + c_n$  un polinomio con coeficientes complejos de grado  $n \geq 1$ . Si  $\alpha_1, \dots, \alpha_n$  son las raíces complejas de  $p(x)$ , cada una repetida tantas veces como indique su multiplicidad, entonces

$$p(x) = c_0(x - \alpha_1) \cdots (x - \alpha_n)$$

*Demostración:* Sólo hay que probar que  $p(x)$  tiene todas sus raíces complejas. Ahora bien, todo polinomio irreducible en  $\mathbb{C}[x]$  es de grado 1, así que todo polinomio con coeficientes complejos no constante descompone en producto de polinomios de grado 1 con coeficientes complejos.

## 6.2. Teorema de Kronecker

**Lema 6.2.1** Si  $p(x)$  es un polinomio no constante de grado  $d$  con coeficientes en  $k$ , entonces  $k[x]/(p(x))$  es una  $k$ -álgebra finita de grado  $d$  y una base es

$$\{[1], [x], \dots, [x]^{d-1}\}$$

*Demostración:* Sea  $V$  el subespacio vectorial de  $k[x]$  de base  $\{1, x, \dots, x^{d-1}\}$ . La aplicación

$$\pi: V \rightarrow k[x]/(p(x)), \quad \pi(q(x)) = [q(x)]$$

es  $k$ -lineal, es inyectiva, porque  $V$  no contiene múltiplos no nulos de  $p(x)$ , y es epiyectiva, porque en  $k[x]/(p(x))$  cada polinomio coincide con el resto de su división por  $p(x)$  y el grado del resto es menor que  $d$ . Por tanto, la dimensión de  $k[x]/(p(x))$  coincide con la de  $V$ , que es  $d$ , y una base de  $k[x]/(p(x))$  es  $\{\pi(1), \pi(x), \dots, \pi(x^{d-1})\}$ .

**Teorema del Grado:** Si  $K$  es una extensión finita de un cuerpo  $k$  y  $L$  es una extensión finita de  $K$ , entonces  $L$  es una extensión finita de  $k$  de grado

$$[L : k] = [L : K] \cdot [K : k]$$

*Demostración:* Sea  $(u_1, \dots, u_n)$  una base de  $K$  sobre  $k$  y  $(v_1, \dots, v_m)$  una base de  $L$  sobre  $K$ . Si  $x \in L$ , entonces  $x = \sum_i \lambda_i v_i$  para ciertos  $\lambda_i \in K$ . A su vez  $\lambda_i = \sum_j a_{ij} u_j$ ,  $a_{ij} \in k$ . Luego  $x = \sum_{ij} a_{ij} v_i u_j$  y concluimos que los elementos  $v_i u_j$  generan  $L$  como  $k$ -espacio vectorial.

Por otra parte, si alguna combinación lineal  $\sum_{ij} a_{ij} v_i u_j$  con coeficientes en  $k$  es nula, entonces

$$\sum_{i=1}^m \left( \sum_{j=1}^n a_{ij} u_j \right) v_i = 0$$

y se sigue que  $a_{i1} u_1 + \dots + a_{in} u_n = 0$  para todo índice  $i$ . Luego los coeficientes  $a_{ij}$  son todos nulos, y los elementos  $v_i u_j$  son linealmente independientes sobre  $k$ . Concluimos que forman una base de  $L$  y, en consecuencia, la dimensión de  $L$  como  $k$ -espacio vectorial es  $nm$ .

**Teorema de Kronecker:** Si  $p(x)$  es un polinomio irreducible con coeficientes en  $k$ , entonces  $k[x]/(p(x))$  es una extensión de  $k$  y una raíz de  $p(x)$  es

$$\bar{x} \in k[x]/(p(x)) .$$

Si  $\alpha$  es otra raíz de  $p(x)$  en una extensión de  $k$ , tenemos un isomorfismo de  $k$ -álgebras

$$k[x]/(p(x)) \simeq k(\alpha) \quad , \quad [q(x)] \mapsto q(\alpha)$$

que transforma  $\bar{x}$  en  $\alpha$ . Por tanto, si  $\beta$  es otra raíz de  $p(x)$  en otra extensión de  $k$ , existe un isomorfismo de  $k$ -álgebras  $k(\alpha) \simeq k(\beta)$  que transforma  $\alpha$  en  $\beta$ .

*Demostración:* Como  $p(x)$  es irreducible, sus múltiplos forman un ideal maximal  $(p(x))$  de  $k[x]$  en virtud del lema de Euclides; luego el anillo cociente  $k[x]/(p(x))$  es un cuerpo y, por tanto, es una extensión de  $k$ . Vamos a probar que  $\bar{x}$  es una raíz de  $p(x)$ .

Si  $a \in k$  y  $[r(x)] \in k[x]/(p(x))$ , por definición  $a[r(x)] = [ar(x)]$ ; luego, si  $p(x) = \sum_i a_i x^i$ , tenemos que

$$p(\bar{x}) = \sum_i a_i [\bar{x}]^i = \sum_i a_i [x^i] = \sum_i [a_i x^i] = \left[ \sum_i a_i x^i \right] = [p(x)] = 0 .$$

Ahora, si  $\alpha$  es otra raíz de  $p(x)$  en una extensión  $L$  de  $k$ , consideramos el morfismo de  $k$ -álgebras  $k[x] \rightarrow L$ ,  $q(x) \mapsto q(\alpha)$ . Su imagen es  $k[\alpha]$  y su núcleo contiene al ideal maximal  $(p(x))$ , porque  $\alpha$  es raíz de  $p(x)$ . Luego su núcleo es  $(p(x))$  y el teorema de isomorfía afirma la existencia de un isomorfismo de  $k$ -álgebras  $k[x]/(p(x)) \rightarrow k[\alpha]$ ,  $[q(x)] \mapsto q(\alpha)$ .

Luego  $k[\alpha]$  es cuerpo, porque  $k[x]/(p(x))$  lo es, y concluimos que  $k[\alpha] = k(\alpha)$ .

Por último, si  $\beta$  es otra raíz, entonces  $k(\alpha) \simeq k[x]/(p(x)) \simeq k(\beta)$ .

**Corolario 6.2.2** *Todo polinomio no constante con coeficientes en un cuerpo  $k$  tiene todas sus raíces en alguna extensión finita de  $k$ .*

*Demostración:* Procedemos por inducción sobre el grado del polinomio  $p(x) \in k[x]$ . Si  $p(x)$  es de grado 1, ya tiene todas sus raíces en  $k$ .

Si el grado de  $p(x)$  es mayor que 1, considerando un factor irreducible de  $p(x)$  en  $k[x]$ , vemos que el teorema de Kronecker afirma que  $p(x)$  tiene una raíz  $\alpha$  en alguna extensión finita  $K$  de  $k$ . Según la regla de Ruffini, existe  $q(x) \in K[x]$  tal que  $p(x) = (x - \alpha)q(x)$ ; luego  $\text{gr } q(x) = \text{gr } p(x) - 1$  y, por hipótesis de inducción, existe alguna extensión finita  $L$  de  $K$  en la que  $q(x)$  tiene todas sus raíces. Según 6.1.2,  $q(x)$  descompone en  $L[x]$  en producto de polinomios de grado 1, así que  $p(x) = (x - \alpha)q(x)$  también descompone en  $L[x]$  en producto de polinomios de grado 1 y concluimos que  $p(x)$  tiene todas sus raíces en  $L$ , que es una extensión finita de  $k$  en virtud del teorema del grado.

**Corolario 6.2.3** *Sea  $p(x)$  un polinomio irreducible con coeficientes en un cuerpo  $k$ . Si  $\alpha$  es una raíz de  $p(x)$  en una extensión de  $k$ , entonces  $p(x)$  divide a todos los polinomios con coeficientes en  $k$  que admitan la raíz  $\alpha$ , y  $k(\alpha)$  es una extensión finita de  $k$  de grado  $d$ :*

$$k(\alpha) = k \oplus k\alpha \oplus k\alpha^2 \oplus \dots \oplus k\alpha^{d-1}$$

**Definición:** Sea  $k \rightarrow L$ . Diremos que  $\alpha \in L$  es **algebraico** sobre  $k$  si es raíz de algún polinomio no nulo  $q(x)$  con coeficientes en  $k$ , y por tanto de algún factor irreducible  $p_\alpha(x)$  de  $q(x)$  en  $k[x]$  que, según 6.2.3, divide a todo polinomio con coeficientes en  $k$  que admita la raíz  $\alpha$ . Si  $\alpha \in L$  no es algebraico sobre  $k$ , diremos que es **trascendente** sobre  $k$ .

Tal polinomio  $p_\alpha(x)$  es, salvo factores constantes, el único polinomio irreducible en  $k[x]$  que admite la raíz  $\alpha$  y diremos que es el polinomio irreducible o **mínimo** de  $\alpha$  sobre  $k$ , pues en  $k[x]$  es el polinomio de menor grado que admite la raíz  $\alpha$ . Según 6.2.3:

$$\text{gr } p_\alpha(x) = [k(\alpha) : k]$$

**Corolario 6.2.4** *La condición necesaria y suficiente para que un elemento  $\alpha$  de una extensión de un cuerpo  $k$  sea algebraico sobre  $k$  es que  $k(\alpha)$  sea una extensión finita de  $k$ . En particular todo elemento de una extensión finita de  $k$  es algebraico sobre  $k$ .*

*Demostración:* La necesidad de la condición es consecuencia de 6.2.3.

Recíprocamente, si  $k(\alpha)$  es una extensión finita de  $k$ , entonces las potencias de  $\alpha$  son linealmente dependientes; i.e.,  $\sum_i a_i \alpha^i = 0$  donde los coeficientes  $a_i \in k$  no son todos nulos, y concluimos que  $\alpha$  es raíz de un polinomio no nulo con coeficientes en  $k$ .

**Corolario 6.2.5** *Sumas, restas, productos, cocientes y raíces  $n$ -ésimas de elementos algebraicos sobre un cuerpo  $k$  también son algebraicos sobre  $k$ .*

**Nota:** El teorema de Kronecker permite probar que *todo polinomio no constante  $p(x)$  con coeficientes reales tiene alguna raíz compleja*, y dar así una demostración más algebraica del Teorema de D'Alembert:

Si  $\text{gr } p(x) = n = 2^d m$ , donde  $m$  es impar, procedemos por inducción sobre  $d$ , porque el enunciado es cierto para todos los polinomios de grado impar según el Teorema de Bolzano (y éste es el punto trascendente de la demostración). Sea  $L$  una extensión finita de  $\mathbb{C}$  donde el polinomio tenga todas sus raíces, que existe en virtud de 6.2.2. Dado  $a \in \mathbb{R}$ , formamos el polinomio de raíces  $\alpha_i + \alpha_j + a\alpha_i\alpha_j$ , donde  $\alpha_i$  y  $\alpha_j$  recorren las raíces de  $p(x)$ , que tiene grado  $n(n-1)/2 = 2^{d-1}m(n-1)$ . Sus coeficientes son reales, porque son funciones simétricas de las raíces de  $p(x)$ . Por hipótesis de inducción este polinomio tiene alguna raíz compleja:  $\alpha_i + \alpha_j + a\alpha_i\alpha_j \in \mathbb{C}$  para ciertos índices  $i, j$ . Luego existen índices  $i, j$  tales que

$$\alpha_i + \alpha_j + a\alpha_i\alpha_j, \alpha_i + \alpha_j + b\alpha_i\alpha_j \in \mathbb{C}$$

donde  $a \neq b$ . Se sigue que  $\alpha_i + \alpha_j, \alpha_i\alpha_j \in \mathbb{C}$  y concluimos que  $\alpha_i$  y  $\alpha_j$  son raíces de un polinomio de grado 2 con coeficientes complejos, polinomios que obviamente tienen todas sus raíces complejas:  $\alpha_i, \alpha_j \in \mathbb{C}$ .

Por último, si  $p(x)$  es un polinomio no constante con coeficientes complejos y  $\bar{p}(x)$  denota el polinomio de coeficientes conjugados, entonces  $p(x)\bar{p}(x) \in \mathbb{R}[x]$ ; luego  $p(x)\bar{p}(x)$  tiene alguna raíz compleja  $\alpha$ , que es raíz de  $p(x)$  ó de  $\bar{p}(x)$ , en cuyo caso  $\bar{\alpha}$  es raíz de  $p(x)$ .

### 6.3. Irracionales Cuadráticos

**Definición:** Diremos que un cuerpo  $K \subset \mathbb{C}$  es una extensión de  $\mathbb{Q}$  por **radicales cuadráticos** cuando  $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ , donde  $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$  para todo índice  $1 \leq i \leq n$ .

Diremos que un número complejo  $\alpha$  es un **irracional cuadrático** si pertenece a alguna extensión de  $\mathbb{Q}$  por radicales cuadráticos. Diremos que un polinomio con coeficientes racionales es **resoluble por radicales cuadráticos** si todas sus raíces complejas son irracionales cuadráticos.

#### Ejemplos:

1. Toda ecuación cuadrática  $ax^2 + bx + c = 0$  es resoluble por radicales cuadráticos, porque sus raíces son  $(-b \pm (b^2 - 4ac)^{1/2})/2$ .
2. Toda ecuación bicuadrada  $ax^4 + bx^2 + c = 0$  es resoluble por radicales cuadráticos, pues sus raíces son  $\pm\sqrt{z_1}$  y  $\pm\sqrt{z_2}$ , donde  $z_1$  y  $z_2$  son las raíces de  $az^2 + bz + c$ .
3. Toda cuártica recíproca  $ax^4 + bx^3 + cx^2 + bx + a = 0$  es resoluble por radicales cuadráticos, pues la sustitución  $y = x + x^{-1}$  la reduce a la ecuación  $ay^2 + by + c - 2a = 0$ .
4. Las raíces de la unidad  $e^{\frac{2\pi i}{3}}, e^{\frac{2\pi i}{4}}, e^{\frac{2\pi i}{5}}$  y  $e^{\frac{2\pi i}{6}}$  son irracionales cuadráticos, porque son raíces de los polinomios  $x^2 + x + 1, x^2 + 1, x^4 + x^3 + x^2 + x + 1$  y  $x^2 - x + 1$  respectivamente.

Los polígonos regulares de 3, 4, 5 y 6 lados inscritos en un círculo de radio dado son constructibles con regla y compás.

5. Si  $e^{\frac{2\pi i}{n}}$  es irracional cuadrático, entonces  $e^{\frac{2\pi i}{2n}} = \sqrt{e^{\frac{2\pi i}{n}}}$  también.

Si el polígono regular de  $n$  lados inscritos en un círculo de radio dado es constructible con regla y compás, también lo es el de  $2n$  lados.

**Lema 6.3.1** Si  $a \in k$ , entonces el grado de  $k(\sqrt{a})$  sobre  $k$  es 1 ó 2 (según que  $a$  tenga o no raíz cuadrada en  $k$ ).

*Demostración:* Como  $\sqrt{a}$  es raíz de  $x^2 - a \in k[x]$ , su polinomio irreducible  $p(x)$  sobre  $k$  divide a  $x^2 - a$  y por tanto su grado es 1 ó 2. Concluimos ya que  $[k(\sqrt{a}) : k] = \text{gr } p(x)$  de acuerdo con 6.2.3.

**Teorema 6.3.2** El grado de cualquier extensión  $K$  de  $\mathbb{Q}$  por radicales cuadráticos es potencia de 2.

*Demostración:* Por definición  $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$  donde  $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$  para todo índice  $i$ . Según el lema anterior, el grado de  $\mathbb{Q}(\alpha_1, \dots, \alpha_i)$  sobre  $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$  es 1 ó 2; así que el Teorema del Grado permite concluir que el grado de  $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$  sobre  $\mathbb{Q}$  es potencia de 2.

**Corolario 6.3.3** Si  $\alpha$  es un irracional cuadrático, entonces  $\alpha$  es algebraico sobre  $\mathbb{Q}$  y el grado de su polinomio irreducible  $p_\alpha(x)$  sobre  $\mathbb{Q}$  es potencia de 2.

*Demostración:* Por definición  $\alpha \in K$ , donde  $K$  es una extensión de  $\mathbb{Q}$  por radicales cuadráticos. Luego  $\mathbb{Q}(\alpha) \subseteq K$ ; así que  $\mathbb{Q}(\alpha)$  es una extensión finita de  $\mathbb{Q}$ , de modo que  $\alpha$  es algebraico sobre  $\mathbb{Q}$  por 6.2.4. Además,  $\text{gr } p_\alpha(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$  divide a  $[K : \mathbb{Q}]$  en virtud del Teorema del Grado; luego es potencia de 2 según el teorema anterior.

#### Ejemplos:

1.  $\sqrt[3]{2}$  no es un irracional cuadrático, porque es raíz del polinomio irreducible  $x^3 - 2$ .

*La duplicación del cubo es imposible con regla y compás.*

2. El número complejo  $e^{\frac{2\pi i}{7}}$  no es un irracional cuadrático, porque su polinomio irreducible sobre  $\mathbb{Q}$ , que es  $x^6 + \dots + x + 1$ , tiene grado 6, que no es potencia de 2.

*Es imposible construir con regla y compás el polígono regular de 7 lados.*

3. El número complejo  $e^{\frac{2\pi i}{9}}$  es raíz del polinomio  $p(x) = x^6 + x^3 + 1$  porque  $(e^{\frac{2\pi i}{9}})^3 = e^{\frac{2\pi i}{3}}$  es raíz del polinomio  $x^2 + x + 1$ . La reducción de  $p(x)$  módulo 2 es irreducible porque no tiene raíces en  $\mathbb{F}_2$ , no es múltiplo de  $x^2 + x + 1$ ,  $x^3 + x + 1$  ni  $x^3 + x^2 + 1$ , que son los únicos polinomios irreducibles de grado 2 y 3 con coeficientes en  $\mathbb{F}_2$ .

Luego  $p(x)$  es irreducible en  $\mathbb{Z}[x]$ , y por tanto en  $\mathbb{Q}[x]$ . Como su grado no es potencia de 2, se concluye que  $e^{\frac{2\pi i}{9}}$  no es un irracional cuadrático.

El ángulo de 120 grados es constructible con regla y compás, mientras que el de 40 grados no lo es: *Es imposible realizar la trisección de ángulos con regla y compás.*

## 6.4. Álgebras Finitas

### Propiedades de las álgebras finitas:

1. Subálgebras y cocientes de  $k$ -álgebra finitas son  $k$ -álgebras finitas.
2. Si  $A$  y  $B$  son  $k$ -álgebras finitas, entonces también lo son  $A \oplus B$  y  $A \otimes_k B$  y

$$[A \oplus B : k] = [A : k] + [B : k] \quad , \quad [A \otimes_k B : k] = [A : k] \cdot [B : k]$$

3. Si  $A$  es una  $k$ -álgebra finita y  $L$  es una extensión de  $k$ , entonces  $A_L := A \otimes_k L$  es una  $L$ -álgebra finita y  $[A_L : L] = [A : k]$ .

*Demostración:* Son consecuencias directas de las propiedades de la dimensión de los espacios vectoriales y del producto tensorial.

**Álgebras Reducidas:** Recuérdense que el *radical* de un anillo (i.e., el conjunto de sus elementos nilpotentes) es la intersección de sus ideales primos, y que un anillo es *reducido* cuando su radical es nulo. Los anillos íntegros claramente son reducidos, y el anillo  $A \oplus B$  es reducido si y sólo si  $A$  y  $B$  son reducidos.

**Álgebras Triviales:** Diremos que una extensión  $K$  de  $k$  es **trivial** si su grado es 1; i.e., si el morfismo estructural  $k \rightarrow K$  es un isomorfismo.

Diremos que una  $k$ -álgebra finita  $A$  es *trivial* si es isomorfa a una suma directa  $k \oplus \dots \oplus k$ . Como cualquier ideal  $I$  de  $k \oplus \dots \oplus k$  es de la forma  $I = I_1 \oplus \dots \oplus I_n$ , donde  $I_i = 0, k$ , se sigue que sus ideales maximales se obtienen cuando  $I_i = k$  para todo índice  $i$ , salvo uno. Las álgebras triviales son reducidas, y el número de ideales maximales coincide con el grado del álgebra.

Hemos usado el siguiente resultado elemental:

**Lema 6.4.1** *Si  $A_1$  y  $A_2$  son dos anillos, todo ideal de  $A_1 \oplus A_2$  es de la forma  $\mathfrak{a}_1 \oplus \mathfrak{a}_2$ , donde  $\mathfrak{a}_1$  es un ideal de  $A_1$  y  $\mathfrak{a}_2$  es un ideal de  $A_2$ .*

*Demostración:* Sea  $\mathfrak{a}$  un ideal de  $A_1 \oplus A_2$ . Si ponemos  $\mathfrak{a}_1 := \{a_1 \in A_1 : (a_1, 0) \in \mathfrak{a}\}$  y  $\mathfrak{a}_2 := \{a_2 \in A_2 : (0, a_2) \in \mathfrak{a}\}$ , es claro que  $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \subseteq \mathfrak{a}$ . Ahora bien, si  $(a_1, a_2) \in \mathfrak{a}$ , entonces  $a_1 \in \mathfrak{a}_1$  porque  $(a_1, 0) = (1, 0)(a_1, a_2) \in \mathfrak{a}$  y  $a_2 \in \mathfrak{a}_2$  porque  $(0, a_2) = (0, 1)(a_1, a_2) \in \mathfrak{a}$ .

**Ejemplo:** Sea  $p(x)$  un polinomio no constante con coeficientes en  $k$  y sea  $A = k[x]/(p(x))$ . Si  $p(x) = p_1(x)^{m_1} \dots p_r(x)^{m_r}$  es su descomposición en factores irreducibles, entonces:

1. Los ideales maximales de  $A$  son los ideales  $\mathfrak{m}_1 = (p_1(x)), \dots, \mathfrak{m}_r = (p_r(x))$ , de modo que sus cuerpos residuales son las extensiones  $k[x]/(p_i(x))$ .
2. De acuerdo con el Teorema Chino del Resto, tenemos que

$$A = k[x]/(p_1^{m_1} \dots p_r^{m_r}) \simeq k[x]/(p_1^{m_1}) \oplus \dots \oplus k[x]/(p_r^{m_r})$$

3.  $A$  es un álgebra reducida si y sólo si  $m_1 = \dots = m_r = 1$ .
4.  $A$  es una  $k$ -álgebra trivial si y sólo si  $m_1 = \dots = m_r = 1$  y todos los factores irreducibles  $p_i(x)$  son de grado 1; es decir, cuando  $p(x)$  tiene todas sus raíces en  $k$  y son simples.

## Teorema de Descomposición

**Lema 6.4.2** *Toda  $k$ -álgebra finita íntegra es un cuerpo.*

*Demostración:* Si  $a \in A$  no es nulo, la aplicación lineal  $h_a: A \rightarrow A$ ,  $h_a(x) = ax$ , es inyectiva porque  $A$  es íntegro. Como  $A$  es un  $k$ -espacio vectorial de dimensión finita, se sigue que la dimensión de la imagen de  $h_a$  coincide con la de  $A$ . Luego  $h_a$  es epiyectivo y concluimos que  $1 = h_a(b) = ab$  para algún  $b \in A$ . Es decir,  $a$  es invertible y  $A$  es un cuerpo.

**Lema 6.4.3** *Todo ideal primo de una  $k$ -álgebra finita  $A$  es maximal.*

*Demostración:* Si  $\mathfrak{p}$  es un ideal primo de  $A$ , entonces  $A/\mathfrak{p}$  es una  $k$ -álgebra finita íntegra; luego es un cuerpo y concluimos que  $\mathfrak{p}$  es un ideal maximal.

**Teorema 6.4.4** *El espectro de una  $k$ -álgebra finita  $A$  es un espacio finito y discreto de cardinal acotado por el grado de  $A$  sobre  $k$ , y se da la igualdad precisamente cuando  $A$  es trivial:  $A = k \oplus \dots \oplus k$ .*

*Demostración:* Si  $\mathfrak{m}_1, \dots, \mathfrak{m}_r$  son ideales maximales de una  $k$ -álgebra finita  $A$ , entonces

$$(\mathfrak{m}_1)_o \cap (\mathfrak{m}_2 \cap \dots \cap \mathfrak{m}_r)_o = (\mathfrak{m}_1)_o \cap ((\mathfrak{m}_2)_o \cup \dots \cup (\mathfrak{m}_r)_o) = \emptyset$$

y el Teorema Chino de los Restos nos proporciona un isomorfismo de  $k$ -álgebras natural

$$A/(\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r) = (A/\mathfrak{m}_1) \oplus \dots \oplus (A/\mathfrak{m}_r)$$

Ahora, como  $[A/\mathfrak{m}_i : k] \geq 1$ , tenemos que

$$r \leq [A/\mathfrak{m}_1 : k] + \dots + [A/\mathfrak{m}_r : k] = [A/\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r : k] \leq [A : k]$$

y que si se da la igualdad, entonces  $A = A/\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$  y  $k = A/\mathfrak{m}_1 = \dots = A/\mathfrak{m}_r$ . Luego  $A = k \oplus \dots \oplus k$  es trivial.

Se concluye porque ya sabemos que en las álgebras triviales el número de ideales maximales es igual al grado.

**Teorema 6.4.5** *Toda  $k$ -álgebra finita reducida  $A$  descompone en suma directa de extensiones finitas de  $k$ , que son sus cuerpos residuales.*

*Demostración:* Si  $\mathfrak{m}_1, \dots, \mathfrak{m}_r$  son todos los ideales maximales de un álgebra reducida  $A$ , entonces  $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = 0$ , porque todo ideal primo de  $A$  es maximal, y la intersección de todos los ideales primos de un anillo reducido es nula. Concluimos que

$$A = A/\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = (A/\mathfrak{m}_1) \oplus \dots \oplus (A/\mathfrak{m}_r).$$

**Corolario 6.4.6** *Si una  $k$ -álgebra finita  $A$  es reducida (resp. trivial), todos sus cocientes  $A/I$  son  $k$ -álgebras finitas reducidas (resp. triviales).*

*Demostración:* Todo ideal  $I$  de un álgebra reducida  $A = L_1 \oplus \dots \oplus L_n$  es de la forma  $I = L_1 \oplus \dots \oplus L_r \oplus 0 \oplus \dots \oplus 0$ , después de reordenar las componentes si fuera necesario; luego  $A/I = L_{r+1} \oplus \dots \oplus L_n$  es reducida, y trivial cuando lo sea  $A$ .

**Lema 6.4.7** *Toda subálgebra  $B$  de una  $k$ -álgebra finita trivial  $A$  es trivial.*

*Demostración:* Procedemos por inducción sobre el grado  $n$  de  $A$ , y el enunciado es obvio cuando  $n = 1$ .

Cuando  $n > 1$ , para cada par de índices  $i \neq j$  consideramos la subálgebra  $B_{ij} := \{(\lambda_1, \dots, \lambda_n) \in k^n : \lambda_i = \lambda_j\}$ , que es trivial y de grado  $n - 1$ . Si  $B$  está contenida en alguna subálgebra  $B_{ij}$ , concluimos que  $B$  es trivial por hipótesis de inducción. En caso contrario existen elementos  $b_{ij} \in B$ ,  $b_{ij} \notin B_{ij}$ , y sustituyéndolos por  $\alpha(b_{ij} - \beta)$ ,  $\alpha, \beta \in k$  podemos suponer que su componente  $i$ -ésima es 1 y su componente  $j$ -ésima es 0. Ahora  $(0, \dots, 1, \dots, 0) = \prod_j b_{ij} \in B$  y concluimos que  $B = A$ .

## 6.5. Puntos de un Álgebra

**Definición:** Si  $A$  es una  $k$ -álgebra y  $L$  es una extensión de  $k$ , llamaremos **puntos** de  $A$  con valores en  $L$ , ó  $L$ -puntos de  $A$ , a los morfismos de  $k$ -álgebras  $p: A \rightarrow L$ , y diremos que la imagen por  $p$  de  $f \in A$  es el **valor** de la función  $f$  en el punto  $p$ , y se denotará  $f(p)$ .

**Ejemplos:**

1. Cada morfismo de  $k$ -álgebras  $k[x_1, \dots, x_n] \rightarrow L$  está totalmente determinado por las imágenes  $\alpha_i$  de las indeterminadas  $x_i$ :

$$\text{Hom}_{k\text{-alg}}(k[x_1, \dots, x_n], L) = L^n$$

2. Si  $A = k[x_1, \dots, x_n]/(p_1, \dots, p_r)$ , los morfismos de  $k$ -álgebras  $A \rightarrow L$ , de acuerdo con la propiedad universal del cociente, se corresponden con los morfismos de  $k$ -álgebras  $k[x_1, \dots, x_n] \rightarrow L$  que se anulen en  $(p_1, \dots, p_r)$ . Es decir, con las sucesiones  $(\alpha_1, \dots, \alpha_n) \in L^n$  tales que

$$p_1(\alpha_1, \dots, \alpha_n) = \dots = p_r(\alpha_1, \dots, \alpha_n) = 0.$$

$$\text{Hom}_{k\text{-alg}}(A, L) = \left[ \begin{array}{l} \text{Soluciones en } L \text{ del sistema de} \\ \text{ecuaciones } p_1 = \dots = p_r = 0 \end{array} \right]$$

En particular, cuando  $A = k[x]/(p(x))$ , obtenemos que los puntos de  $A$  con valores en  $L$  son las raíces de  $p(x)$  en  $L$ . *El concepto de raíz de un polinomio es un caso particular del concepto de punto:*

$$\text{Hom}_{k\text{-alg}}(k[x]/(p(x)), L) = \left[ \begin{array}{l} \text{Raíces en } L \text{ del} \\ \text{polinomio } p(x) \end{array} \right]$$

3. Si  $L$  es una extensión finita de un cuerpo  $k$ , todo morfismo de  $k$ -álgebras  $L \rightarrow L$  es un automorfismo porque necesariamente es inyectivo, al ser  $L$  un cuerpo, y  $L$  es un  $k$ -espacio vectorial de dimensión finita. Luego los puntos de  $L$  con valores en  $L$  son precisamente los automorfismos de  $L$  que son la identidad sobre  $k$ . *El concepto de automorfismo de una extensión finita es un caso particular del concepto de punto:*

$$\text{Hom}_{k\text{-alg}}(L, L) = \text{Aut}(L/k)$$

4. Sea  $L$  una extensión finita de un cuerpo  $k$ . Si  $L = k(\alpha)$ , en virtud del Teorema de Kronecker tenemos que  $L \simeq k[x]/(p_\alpha(x))$ , donde  $p_\alpha(x)$  denota el polinomio irreducible de  $\alpha$  sobre  $k$ . Luego

$$\text{Aut}(L/k) = \text{Hom}_{k\text{-alg}}(k[x]/(p_\alpha(x)), L) = \{\text{raíces de } p_\alpha(x) \text{ en } L\}$$

donde cada automorfismo  $\tau$  de  $L$  se corresponde con la raíz  $\tau(\alpha)$  de  $p_\alpha(x)$  en  $L$ .

Cualquier morfismo de  $k$ -álgebras  $p: A \rightarrow k$  necesariamente es epiyectivo, por lo que su núcleo es un ideal maximal  $\mathfrak{m}$  de  $A$  y  $k = A/\mathfrak{m}$ . Veamos que tal correspondencia entre  $k$ -puntos de  $A$  y puntos de  $\text{Spec } A$  de cuerpo residual  $k$  es biyectiva:

**Lema 6.5.1** *Si  $A$  es una  $k$ -álgebra, tenemos una correspondencia biyectiva natural:*

$$\text{Hom}_{k\text{-alg}}(A, k) = \left[ \begin{array}{l} \text{Ideales maximales de } A \\ \text{de cuerpo residual } k \end{array} \right]$$

*Demostración:* Cada ideal maximal  $\mathfrak{m}$  de  $A$  de cuerpo residual  $k$  es el núcleo de la proyección canónica  $\pi: A \rightarrow A/\mathfrak{m} = k$ , que es un  $k$ -punto de  $A$ ; luego tal correspondencia es epiyectiva.

Por otra parte, si dos morfismos de  $k$ -álgebras  $p, p': A \rightarrow k$  tiene igual núcleo y  $a \in A$ , entonces  $p(a) = \lambda \in k$  y  $p(a - \lambda) = 0$ ; luego  $p'(a - \lambda) = 0$  y  $p'(a) = \lambda$ , de modo que  $p' = p$  y concluimos que tal correspondencia es inyectiva.

**Fórmula de los Puntos:** Si  $A$  es una  $k$ -álgebra, para toda extensión  $L$  de  $k$  tenemos una correspondencia biyectiva natural:

$$\mathrm{Hom}_{k\text{-alg}}(A, L) = \left[ \begin{array}{l} \text{Ideales maximales de } A_L \\ \text{de cuerpo residual } L \end{array} \right]$$

*Demostración:* Por la propiedad universal del cambio de base de álgebras, tenemos

$$\mathrm{Hom}_{k\text{-alg}}(A, L) = \mathrm{Hom}_{L\text{-alg}}(A_L, L)$$

y se concluye al aplicar el lema anterior a la  $L$ -álgebra  $A_L$ .

**Corolario 6.5.2** Si  $A$  es una  $k$ -álgebra finita  $A$  y  $L$  es una extensión de  $k$ , el número de morfismos de  $k$ -álgebras  $A \rightarrow L$  está acotado por el grado  $[A : k]$ , y coincide con él precisamente cuando la  $L$ -álgebra  $A_L$  es trivial:  $A \otimes_k L = L \oplus \dots \oplus L$ .

*Demostración:* El número de  $L$ -puntos de la  $L$ -álgebra finita  $A_L$  está acotado por  $[A_L : L] = [A : k]$  (porque lo está el número de puntos del espectro de  $A_L$ ), y se da la coincidencia si y sólo si  $A_L$  es  $L$ -álgebra trivial, en virtud de 6.4.4.

**Corolario 6.5.3** El número de automorfismos de una extensión finita  $L$  de un cuerpo  $k$  está acotado por el grado  $[L : k]$ , y se da la coincidencia si y sólo si  $L \otimes_k L$  es  $L$ -álgebra trivial:  $L \otimes_k L = L \oplus \dots \oplus L$ .

**Ejemplo:** Consideremos las 4 raíces complejas  $\alpha_1 = \sqrt[4]{2}$ ,  $\alpha_2 = i\sqrt[4]{2}$ ,  $\alpha_3 = -\sqrt[4]{2}$ ,  $\alpha_4 = -i\sqrt[4]{2}$  del polinomio  $x^4 - 2$  y la correspondiente extensión  $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\sqrt[4]{2}, i)$ .

El grado de  $\mathbb{Q}(\sqrt[4]{2})$  sobre  $\mathbb{Q}$  es 4 porque  $x^4 - 2$  es irreducible en  $\mathbb{Q}[x]$ , y el grado de  $L$  sobre  $\mathbb{Q}(\sqrt[4]{2})$  es 2 porque  $x^2 + 1$  no tiene raíces en  $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ . Luego  $[L : \mathbb{Q}] = 8$ . Además  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt[4]{2})$  y  $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2})$  son triviales sobre  $L$ :

$$\begin{aligned} \mathbb{Q}(i)_L &= (\mathbb{Q}[x]/(x^2 + 1))_L = L[x]/(x^2 + 1) = L \oplus L \\ \mathbb{Q}(\sqrt[4]{2})_L &= (\mathbb{Q}[x]/(x^4 - 2))_L = L[x]/(x^4 - 2) = L \oplus L \oplus L \oplus L \\ (\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}))_L &= \mathbb{Q}(i)_L \otimes_L \mathbb{Q}(\sqrt[4]{2})_L = (L \oplus L) \otimes_L (L \oplus \dots \oplus L) = \oplus L \end{aligned}$$

Como  $\mathbb{Q}(i, \sqrt[4]{2})$  es un cociente de  $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2})$ , se sigue que  $\mathbb{Q}(i, \sqrt[4]{2})$  también es trivial sobre  $L$ . Es decir,  $L \otimes_{\mathbb{Q}} L = \oplus L$  y la fórmula de los puntos afirma que el grupo  $G = \mathrm{Aut}(L/\mathbb{Q})$  es de orden 8.

Si  $\tau \in G$ , entonces  $\tau(\sqrt[4]{2}) = \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$  y  $\tau(i) = \pm i$ ; luego éstas 8 posibilidades son todos los elementos de  $G$ . Los 8 automorfismos  $\tau_i$ ,  $1 \leq i \leq 8$ , de  $L$  son

$$\begin{array}{c} \sqrt[4]{2} \\ i \\ id \end{array} \left| \begin{array}{cccccccc} \tau_1 & \tau_2 & \tau_3 & \tau_4 & \tau_5 & \tau_6 & \tau_7 & \tau_8 \\ \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} & \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ i & i & i & i & -i & -i & -i & -i \\ id & (1234) & (13)(24) & (1432) & (24) & (12)(34) & (13) & (14)(23) \end{array} \right.$$

Las raíces complejas de  $x^4 - 2$  son los vértices de un cuadrado, y el grupo  $G$  es el grupo de Galois es el grupo de simetrías de este cuadrado:  $\gamma = \tau_2$  es el giro de ángulo recto y  $\sigma = \tau_5$  es la simetría respecto del eje horizontal:

$$G = \{id, \gamma, \gamma^2, \gamma^3, \sigma, \sigma\gamma, \sigma\gamma^2, \sigma\gamma^3\} \quad , \quad \gamma^4 = \sigma^2 = id, \quad \gamma\sigma = \sigma\gamma^3$$

## 6.6. Raíces Múltiples

**Definición:** Sea  $p(x) = \sum_i a_i x^i$  un polinomio con coeficientes en un cuerpo  $k$ . Llamaremos **derivada** de  $p(x)$  al siguiente polinomio con coeficientes en  $k$ :

$$p'(x) = \sum_{i \geq 1} i a_i x^{i-1}$$

donde  $i a_i := a_i + \dots + a_i$  denota la suma  $i$  veces de  $a_i$  en  $k$ . Es fácil comprobar que la derivada es una aplicación  $k$ -lineal:

$$\begin{aligned} (p(x) + q(x))' &= p'(x) + q'(x) \\ (a \cdot p(x))' &= a \cdot p'(x), \quad a \in k \end{aligned}$$

**Teorema 6.6.1**  $(p(x) \cdot q(x))' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$ .

*Demostración:* Cuando  $p(x) = x^i$  y  $q(x) = x^j$  la igualdad se comprueba directamente. En el caso general  $p(x) = \sum_i a_i x^i$ ,  $q(x) = \sum_j b_j x^j$  tenemos:

$$\begin{aligned} (pq)' &= \sum_{ij} a_i b_j (x^i x^j)' = \sum_{ij} i a_i b_j x^{i-1} x^j + \sum_{ij} j a_i b_j x^i x^{j-1} = \\ &= \left( \sum_i i a_i x^{i-1} \right) \left( \sum_j b_j x^j \right) + \left( \sum_i a_i x^i \right) \left( \sum_j j b_j x^{j-1} \right) = p' \cdot q + p \cdot q' \end{aligned}$$

**Teorema 6.6.2** *Sea  $p(x)$  un polinomio no constante con coeficientes en un cuerpo  $k$ . La condición necesaria y suficiente para que una raíz de  $p(x)$  sea múltiple es que sea raíz de la derivada  $p'(x)$ .*

*Demostración:* Sea  $\alpha$  una raíz de  $p(x)$  en alguna extensión  $K$  de  $k$  y sea  $m$  su multiplicidad, de modo que en  $K[x]$  tenemos

$$p(x) = (x - \alpha)^m q(x), \quad q(\alpha) \neq 0$$

Si  $m = 1$ , entonces

$$p'(x) = q(x) + (x - \alpha)q'(x), \quad p'(\alpha) = q(\alpha) \neq 0$$

de modo que  $\alpha$  no es raíz de  $p'(x)$ . Si  $m \geq 2$ , entonces

$$p'(x) = m(x - \alpha)^{m-1} + (x - \alpha)^m q'(x), \quad p'(\alpha) = 0$$

y  $\alpha$  es raíz de  $p'(x)$ .

**Corolario 6.6.3** *Sea  $p(x)$  un polinomio no constante con coeficientes en un cuerpo  $k$ . Las raíces múltiples de  $p(x)$  son las raíces del máximo común divisor de  $p(x)$  y su derivada  $p'(x)$ .*

*Demostración:* Sea  $d(x) = \text{m.c.d.}(p(x), p'(x))$ . Si  $\alpha$  es una raíz de  $d(x)$  en una extensión de  $k$ , entonces  $\alpha$  es raíz de  $p(x)$  y de  $p'(x)$  porque ambos polinomios son múltiplos de  $d(x)$ , así que el teorema anterior permite concluir que  $\alpha$  es una raíz múltiple de  $p(x)$ .

Recíprocamente, si  $\alpha$  es una raíz múltiple de  $p(x)$ , el teorema anterior afirma que también es raíz de  $p'(x)$ . Concluimos que  $\alpha$  es raíz de  $d(x)$  porque, según la Identidad de Bézout, existen  $a(x), b(x) \in k[x]$  tales que

$$d(x) = a(x)p(x) + b(x)p'(x)$$

**Corolario 6.6.4** *Sea  $p(x)$  un polinomio con coeficientes en un cuerpo  $k$ . Si  $p(x)$  es irreducible en  $k[x]$ , entonces todas las raíces de  $p(x)$  son simples o su derivada  $p'(x)$  es nula.*

*Demostración:* Salvo constantes no nulas, los únicos divisores de  $p(x)$  en  $k[x]$  son 1 y  $p(x)$ , así que el máximo común divisor de  $p(x)$  y  $p'(x)$  es 1 ó  $p(x)$ . Si es 1, en virtud del corolario anterior  $p(x)$  no tiene raíces múltiples. Si es  $p(x)$ , como divide a  $p'(x)$  y el grado de  $p'(x)$  no puede ser mayor o igual que el grado de  $p(x)$ , concluimos que  $p'(x) = 0$ .

### Característica de un Anillo

Si  $\text{gr } p(x) \geq 1$ , por definición de la derivada es evidente que  $\text{gr } p'(x) \leq \text{gr } p(x) - 1$ ; pero el grado de  $p'(x)$  puede ser menor que  $\text{gr } p(x) - 1$  e incluso puede ocurrir que  $p'(x) = 0$ . Esto se debe a que un coeficiente  $ia_i$  puede ser nulo aunque  $a_i$  no lo sea, porque en  $k$  la suma iterada  $i$  veces de la unidad  $i \cdot 1 := 1 + \dots + 1$  puede ser nula, suma iterada que denotaremos  $i$  cuando no origine confusión con el número natural  $i$ . Por ejemplo, si  $k = \mathbb{F}_p$ , la derivada del polinomio  $x^p + 1$  es nula, al igual que la de cualquier polinomio  $p(x) = \sum_i a_i x^{pi}$ , pues tenemos que  $p = 0$  en el cuerpo finito  $\mathbb{F}_p$ .

**Definición:** Si  $A$  es un anillo, existe un único morfismo de anillos  $\mathbb{Z} \rightarrow A$ , que transforma cada número natural  $n$  en  $1 + \dots + 1$  y  $-n$  en su opuesto. Su núcleo es un ideal de  $\mathbb{Z}$ ; luego es  $d\mathbb{Z}$  para cierto número natural  $d$ , que recibe el nombre de **característica** de  $A$ .

Por definición, la característica de  $A$  es nula cuando  $n = 1 + \dots + 1 \neq 0$  en  $A$  para todo número natural no nulo  $n$ . Por el contrario, la característica de  $A$  es positiva cuando existe algún número natural positivo  $n$  tal que  $1 + \dots + 1 = 0$  en  $A$  y, en tal caso, la característica de  $A$  es el menor de tales números.

#### Ejemplos:

1. Los anillos  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  y  $\mathbb{C}$  tienen característica nula.
2. Si  $n \in \mathbb{N}$ , la característica del anillo  $\mathbb{Z}/n\mathbb{Z}$  es  $n$ .
3. La característica de un anillo  $A$  coincide con la de cualquier subanillo  $B$ . En particular, la característica de cualquier extensión de un cuerpo  $k$  coincide con la de  $k$ .
4. Sea  $ax^2 + bx + c = 0$  una ecuación cuadrática con coeficientes en un cuerpo  $k$ . La fórmula usual

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

para sus raíces sólo es válida cuando  $\text{car } k \neq 2$ , pues exige dividir por  $2a$ .

5. Todos los anillos finitos tienen característica positiva:
6. Sea  $b$  un elemento no nulo de un cuerpo  $k$  y  $m \in \mathbb{Z}$ . Entonces  $mb$  es nulo si y sólo si  $m = 0$  en  $k$ , lo que equivale a que  $m$  sea múltiplo de la característica de  $k$ . Por tanto, si la característica de  $k$  es nula,  $\text{gr } p'(x) = \text{gr } p(x) - 1$  para todo polinomio no constante  $p(x) \in k[x]$  y, en particular, la derivada  $p'(x)$  no es nula.

Si la característica de  $k$  es positiva, la igualdad  $\text{gr } p'(x) = \text{gr } p(x) - 1$  sólo es válida cuando el grado de  $p(x)$  no sea múltiplo de la característica de  $k$ .

**Teorema 6.6.5** *Sea  $q(x)$  un polinomio con coeficientes en un cuerpo  $k$  de característica nula. Si  $q(x)$  es irreducible en  $k[x]$ , entonces todas las raíces de  $q(x)$  son simples.*

*Demostración:* El grado de  $q'(x)$  es  $\text{gr } q(x) - 1$  porque la característica de  $k$  es nula, así que  $q'(x) \neq 0$  y 6.6.4 permite concluir que todas las raíces de  $q(x)$  son simples.

**Teorema 6.6.6** *La característica de todo anillo íntegro es nula o es un número primo.*

*Demostración:* Sea  $A$  un anillo íntegro de característica positiva  $d$ . Si  $d$  no fuera un número primo, entonces  $d = nm$  donde  $n$  y  $m$  son números naturales menores que  $d$ . Luego  $0 = d = nm$  en  $A$  y, por ser  $A$  íntegro, se sigue que  $n = 0$  ó  $m = 0$  en  $A$ , en contra de que  $d$  es el menor número positivo tal que  $d = 0$  en  $A$ . Concluimos que  $d$  es un número primo.

**Lema 6.6.7** Si la característica de un anillo  $A$  es un número primo  $p$ , entonces para todo  $a, b \in A$  tenemos que:

$$(a + b)^p = a^p + b^p$$

*Demostración:* Sea  $i$  un número natural entre 1 y  $p - 1$ . Como  $i!$  no es múltiplo de  $p$  y  $p(p - 1) \cdots (p - i + 1)$  es múltiplo de  $p$ , del Lema de Euclides se sigue que

$$\binom{p}{i} = \frac{p(p - 1) \cdots (p - i + 1)}{i!}$$

es múltiplo de  $p$  y, por tanto, es nulo en  $A$ . Luego

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

**Teorema 6.6.8** Sea  $q(x)$  un polinomio con coeficientes en un cuerpo finito  $k$ . Si  $q(x)$  es irreducible en  $k[x]$ , entonces todas las raíces de  $q(x)$  son simples.

*Demostración:* De acuerdo con 6.6.4 basta ver que  $q'(x) \neq 0$ . Si  $q(x) = \sum_i a_i x^i \in k[x]$  tiene derivada nula, entonces

$$q(x) = \sum_i a_{ip} x^{ip}$$

Por otra parte, la característica de  $k$  es un número primo  $p$ , y el morfismo de grupos  $F: k^* \rightarrow k^*$ ,  $F(b) = b^p$ , es inyectivo, porque  $x^p - 1 = (x - 1)^p$ ; luego es epiyectivo, al ser  $k^*$  finito, y se sigue la existencia de elementos  $b_i \in k$  tales que  $a_{ip} = b_i^p$ . Concluimos que

$$q(x) = \sum_i b_i^p x^{ip} = \left( \sum_i b_i x^i \right)^p$$

no es irreducible, en contra de la hipótesis de que sí lo es.

## 6.7. Álgebras Separables

**Definición:** Diremos que una  $k$ -álgebra finita reducida  $A$  es **separable** si  $A_L = A \otimes_k L$  es reducida para toda extensión  $k \rightarrow L$ ; en particular las  $k$ -álgebras triviales son separables.

Diremos que un polinomio no nulo  $p(x)$  con coeficientes en  $k$  es **separable** cuando lo sea la  $k$ -álgebra  $k[x]/(p(x))$ ; es decir, cuando su descomposición en factores irreducibles en  $L[x]$  carezca de factores repetidos, para toda extensión  $k \rightarrow L$ . Tal condición equivale a decir que todas las raíces de  $p(x)$  son simples:  $\text{m.c.d.}(p(x), p'(x)) = 1$ .

### Propiedades de las álgebras separables:

1. Subálgebras, cocientes y sumas directas de  $k$ -álgebras finitas separables son  $k$ -álgebras finitas separables.
2. Si  $A$  y  $B$  son  $k$ -álgebras finitas separables, entonces  $A \otimes_k B$  es una  $k$ -álgebra finita separable.
3. El concepto de álgebra finita separable es estable por cambios del cuerpo base (si  $A$  es una  $k$ -álgebra finita separable y  $L$  es una extensión de  $k$ , entonces  $A_L$  es una  $L$ -álgebra finita separable).

*Demostración:* El primer apartado es inmediato. En cuanto al segundo, al ser  $B$  separable sobre  $k$ , para toda extensión  $k \rightarrow L$  tenemos que  $B_L = K_1 \oplus \dots \oplus K_n$  para ciertas extensiones  $K_i$  de  $L$ . Luego

$$(A \otimes_k B) \otimes_k L = A \otimes_k (K_1 \oplus \dots \oplus K_n) = (A \otimes_k K_1) \oplus \dots \oplus (A \otimes_k K_n)$$

es reducida y concluimos que también  $A \otimes_k B$  es separable sobre  $k$ .

Por último, si  $A$  es una  $k$ -álgebra finita separable, para toda extensión  $L \rightarrow E$  tenemos que  $(A_L)_E = A_E$  es reducida; luego la  $L$ -álgebra finita  $A_L$  es separable.

**Teorema 6.7.1** *Si  $A$  es una  $k$ -álgebra finita y existe una extensión  $k \rightarrow L$  tal que  $A_L$  es una  $L$ -álgebra separable (en particular si  $A_L$  es  $L$ -álgebra trivial), entonces  $A$  es una  $k$ -álgebra separable.*

*Demostración:* Para cada extensión  $k \rightarrow E$  consideramos una extensión común  $F$  de  $E$  y  $L$ , por ejemplo un cuerpo residual de  $E \otimes_k L$ . Por hipótesis  $(A_L)_F = A_F$  es reducida; luego también lo es la subálgebra  $A_E$ , y concluimos que  $A$  es separable sobre  $k$ .

**Definición:** Si  $L$  es una extensión finita de un cuerpo  $k$ , diremos que un elemento  $\alpha \in L$  es separable sobre  $k$  cuando lo sea su polinomio irreducible  $p_\alpha(x)$ ; es decir, cuando lo sea la extensión  $k(\alpha) \simeq k[x]/(p_\alpha(x))$ .

**Lema 6.7.2** *Una extensión finita  $k \rightarrow k(\alpha_1, \dots, \alpha_n)$  es separable si y sólo si los elementos  $\alpha_1, \dots, \alpha_n$  son separables sobre  $k$ .*

*Demostración:* Si  $k(\alpha_1, \dots, \alpha_n)$  es una extensión separable de  $k$ , también lo es  $k(\alpha_i)$  para todo índice  $i$ , de modo que  $\alpha_i$  es separable sobre  $k$ .

Recíprocamente, si las extensiones  $k(\alpha_i) \simeq k[x]/(p_{\alpha_i}(x))$  son separables, también lo es  $k(\alpha_1, \dots, \alpha_n)$ , porque es un cociente de  $k(\alpha_1) \otimes_k \dots \otimes_k k(\alpha_n)$ .

**Teorema 6.7.3** *Si  $k$  es un cuerpo de característica nula o un cuerpo finito, todas las extensiones finitas de  $k$  son separables.*

*Demostración:* De acuerdo con 6.6.5 y 6.6.8 todos los elementos de las extensiones finitas de  $k$  son separables.

**Ejemplo:** Sea  $k = \mathbb{F}_2(t)$  el cuerpo de las fracciones racionales en una indeterminada con coeficientes en  $\mathbb{F}_2$ . El polinomio  $p(x) = x^2 - t$  es irreducible en  $k[x]$ , porque es de grado 2 y no tiene raíces en  $k$  (pruébese). No obstante, todas sus raíces son múltiples, porque  $p'(x) = 0$ . De hecho, si  $\alpha$  es una raíz de  $p(x)$ , entonces  $\alpha^2 = t$  y  $x^2 - t = (x - \alpha)^2$ . Esto muestra que la extensión finita  $k(\sqrt{t}) = k[x]/(x^2 - t)$  de  $k$  no es separable.