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 $A \times M \to M$, cada elemento $a \in A$ define una aplicación $a\cdot\colon M \to M$ y el segundo axioma expresa que $a\cdot$ es morfismo de grupos. Los tres últimos axiomas expresan que la aplicación $\phi\colon A \to \mathrm{End}(M)$, $\phi(a) = a\cdot$, es morfismo de anillos. Recíprocamente, si M es un grupo abeliano, cada morfismo de anillos $\phi\colon A \to \mathrm{End}(M)$ 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 $f\colon M \to N$ entre dos A-módulos es un **morfismo** de A-módulos cuando es un morfismo de grupos y conserva el producto por elementos de A:

$$f(m + m') = f(m) + f(m')$$
$$f(a \cdot m) = a \cdot f(m)$$

Diremos que un morfismo de A-módulos $f\colon M \to N$ es un **isomorfismo** de A-módulos si existe algún morfismo de A-módulos $h\colon N \to M$ 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 $f\colon M \to N$ es un morfismo de A-módulos, su núcleo $\operatorname{Ker} f$ es un submódulo de M y su imagen $\operatorname{Im} f$ 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

$$nm := m+ \overset{n}{\ldots} +m$$
$$(-n)m := (-m)+ \overset{n}{\ldots} +(-m)$$

   de modo que los submódulos de M son precisamente los subgrupos de M, y los morfismos de $\mathbb{Z}$-módulos son los morfismos de grupos.

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

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

   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.

5. Sea M un A-módulo. Cada $a \in A$ induce un morfismo de A-módulos $M \xrightarrow{a\cdot} M$, $m \mapsto am$; y cada $m \in M$ induce un morfismo de A-módulos $A \xrightarrow{\cdot m} M$, $a \mapsto am$.

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 $a_1m_1 + \ldots + a_nm_n$ 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.

8. Fijado un conjunto $\{x_i\}_{i\in I}$, cada elemento x_i define canónicamente un elemento de $A^{(I)}$: aquél cuyas componentes son todas nulas, excepto la i-ésima que es la unidad. Ahora todo elemento de $A^{(I)} = \bigoplus_I A$ descompone, y de modo único, como una suma finita $a_1x_1 + \ldots + a_nx_n$, donde $a_i \in A$. Es decir, $A^{(I)} = \bigoplus_I A$ es el módulo de las combinaciones lineales finitas de elementos de I con coeficientes en el anillo A.

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 $\pi\colon M \to M/N$, $\pi(m) = [m]$, 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 $\pi\colon M \to M/N$ la proyección canónica. Si un morfismo de A-módulos $f\colon M \to M'$ se anula en N, entonces existe un único morfismo de A-módulos $\varphi\colon M/N \to M'$ tal que $f = \varphi \circ \pi$; es decir, $\varphi([m]) = f(m)$.*

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

$$\phi\colon M/\mathrm{Ker}\, f \;\longrightarrow\; \mathrm{Im}\, f \quad , \quad \phi([m]) = f(m)$$

Teorema 1.1.1 *Sea M un A-módulo y sea $\pi\colon M \to M/N$ 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*

$$\begin{bmatrix}\text{Submódulos}\\ \text{de } M/N\end{bmatrix} \;=\; \begin{bmatrix}\text{Submódulos de } M\\ \text{que contienen a } N\end{bmatrix}$$

Demostración: Es claro que $\pi^{-1}(\bar{P})$ es un submódulo de M que contiene a $\mathrm{Ker}\,\pi = N$ 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

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

y $P = \pi^{-1}\big(\pi(P)\big)$. Recíprocamente, si $\bar{P}$ es un submódulo de M/N, entonces $\pi\big(\pi^{-1}(\bar{P})\big) \subseteq \bar{P}$ y se da la igualdad porque π 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 $\pi\colon A \to \bar{A}$ 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 $A \to \bar{A}/\bar{\mathfrak{b}}$ 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 $f\colon \bigoplus_I A \to M$

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

y diremos que forman un **sistema de generadores** de M cuando $M = \sum_i Am_i$; es decir, cuando el correspondiente morfismo $\phi\colon A^{(I)} \to M$ sea epiyectivo. Diremos que forman una **base** de M cuando ϕ 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.

Lema 1.1.6 *Sea A un anillo no nulo. Si existe algún morfismo epiyectivo de A-módulos $A^{(I)} \to A^{(J)}$, 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 igual 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 $\varphi\colon A^{(I)} \to A^{(J)}$ es epiyectivo, también lo será el morfismo $\bar\varphi\colon A^{(I)}/\mathfrak{m}A^{(I)} \to A^{(J)}/\mathfrak{m}A^{(J)}$, $\bar\varphi([m]) = [\varphi(m)]$. Como $\bar\varphi$ es k-lineal, el cardinal de J no puede superar al cardinal de I.

1.2. Sucesiones Exactas

Sean M y N dos A-módulos. El conjunto de los morfismos de A-módulos de M en N se denota $\mathrm{Hom}_A(M,N)$. Si $f, h\colon M \to N$ son dos morfismos de A-módulos, su suma $f+h$, que es la aplicación

$$(f+h)(m) := f(m) + h(m)$$

también es morfismo de A-módulos, y el producto af por cualquier elemento $a \in A$, que es la aplicación

$$(af)(m) := a\big(f(m)\big)$$

también es morfismo de A-módulos.

Con estas operaciones, $\mathrm{Hom}_A(M,N)$ tiene estructura de A-módulo.

Sea $f\colon M' \to M$ un morfismo de A-módulos y N un A-módulo. La composición con f induce aplicaciones

$$\begin{aligned} f_*\colon \mathrm{Hom}_A(N,M') &\longrightarrow \mathrm{Hom}_A(N,M)\ , \quad f_*(h) := f\circ h \\ f^*\colon \mathrm{Hom}_A(M,N) &\longrightarrow \mathrm{Hom}_A(M',N)\ , \quad f^*(h) := h\circ f \end{aligned}$$

que son morfismos de A-módulos. Es claro que f^* y f_* son la identidad cuando f lo es y que se verifica:

$$\begin{aligned} (f\circ h)_* = (f_*)\circ(h_*) \quad &, \quad (af+bh)_* = a(f_*)+b(h_*) \\ (f\circ h)^* = (h^*)\circ(f^*) \quad &, \quad (af+bh)^* = a(f^*)+b(h^*) \end{aligned}$$

Ejemplo: Sea E un espacio vectorial sobre un cuerpo k. Su espacio *dual*, por definición, es $E^* = \mathrm{Hom}_k(E,k)$. Ahora, si $T\colon E \to F$ es una aplicación k-lineal entre dos k-espacios vectoriales, la aplicación k-lineal $T^*\colon F^* \to E^*$, $T^*(\omega) = \omega\circ T$, que acabamos de definir es precisamente la aplicación *traspuesta*; i.e, $(T^*\omega)(e) = \omega(Te)$ para todo $e \in E$, $\omega \in F^*$.

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

Teorema 1.2.1 *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

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

Demostración: Supongamos que $\mathrm{Im}\, i = \mathrm{Ker}\, p$ y que p es epiyectivo. Si $f \in \mathrm{Hom}_A(M'',N)$ y $fp = 0$, entonces f se anula en $\mathrm{Im}\, p = M''$; luego $f = 0$, lo que muestra que p^* es inyectivo. Como $pi = 0$, se sigue que $0 = (pi)^* = i^*p^*$; luego $\mathrm{Im}\, p^* \subseteq \mathrm{Ker}\, i^*$. Por último, si $h \in \mathrm{Ker}\, i^*$, entonces el morfismo $h\colon M \to N$ se anula en $\mathrm{Im}\, i = \mathrm{Ker}\, p$, así que h factoriza a través de la proyección canónica $\pi\colon M \to M/\mathrm{Ker}\, p \simeq M''$ de acuerdo con la propiedad universal del cociente. Es decir, $h \in \mathrm{Im}\, \pi^* = \mathrm{Im}\, p^*$.

Veamos ahora que la condición es suficiente. Como p^* es inyectivo cuando $N = M''/\mathrm{Im}\, p$, se sigue que la proyección canónica $\pi\colon M'' \to N$ es nula; es decir, $\mathrm{Im}\, p = M''$ y p es epiyectivo. Además, la condición $i^*p^* = (pi)^* = 0$ implica que $pi = (pi)^*(Id) = 0$; luego $\mathrm{Im}\, i \subseteq \mathrm{Ker}\, p$. Por último, si $N = M/\mathrm{Im}\, i$ y $\pi\colon M \to N$ es la proyección canónica, tenemos que $i^*(\pi) = 0$. Luego existe algún morfismo $f\colon M'' \to N$ tal que $\pi = p^*(f) = f\circ p$ y concluimos que $\mathrm{Ker}\, p \subseteq \mathrm{Ker}\, \pi = \mathrm{Im}\, i$.

Corolario 1.2.2 *La condición necesaria y suficiente para que un morfismo de A-módulos $f\colon M \to M''$ sea un isomorfismo es que para todo A-módulo N lo sea el morfismo*

$$f^*\colon \mathrm{Hom}_A(M'',N) \longrightarrow \mathrm{Hom}_A(M,N)$$

Demostración: Un morfismo de A-módulos $g\colon M_1 \to M_2$ es isomorfismo precisamente cuando es exacta la sucesión $0 \to M_1 \xrightarrow{g} M_2 \to 0$.

Teorema 1.2.3 *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

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

Demostración: La necesidad de la condición es inmediata. Para ver que es suficiente basta tomar $N = A$, pues para todo A-módulo M tenemos un isomorfismo natural $M = \mathrm{Hom}_A(A, M)$ y, mediante estos isomorfismos, cada morfismo f se corresponde con f_*.

Corolario 1.2.4 *La condición necesaria y suficiente para que un morfismo de A-módulos $f\colon M' \to M$ sea un isomorfismo es que para todo A-módulo N lo sea el morfismo*

$$f_*\colon \mathrm{Hom}_A(N, M') \to \mathrm{Hom}_A(N, M)$$

Teorema 1.2.5 *Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta de morfismos de A-módulos. Las siguientes condiciones son equivalentes:*

1. *Existe un morfismo de A-módulos $s\colon M'' \to M$ tal que $p \circ s = \mathrm{Id}_{M''}$.*
2. *Existe un morfismo de A-módulos $r\colon M \to M'$ tal que $r \circ i = \mathrm{Id}_{M'}$.*
3. *$p_*\colon \mathrm{Hom}_A(N, M) \longrightarrow \mathrm{Hom}_A(N, M'')$ es epiyectivo para todo A-módulo N.*
4. *$i^*\colon \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M', N)$ es epiyectivo para todo A-módulo N.*

Además, si se verifican estas condiciones, M es isomorfo a $M' \oplus M''$.

Demostración: $(1 \Rightarrow 3)$ Porque $p_* s_* = (ps)_* = \mathrm{Id}$.

$(3 \Rightarrow 1)$ Basta tomar $N = M''$ y considerar la identidad de M''.

$(2 \Rightarrow 4)$ Porque $i^* r^* = (ri)^* = \mathrm{Id}$.

$(4 \Rightarrow 2)$ Basta tomar $N = M'$ y considerar la identidad de M'.

Por último, veamos que las dos primeras condiciones son equivalentes. Si se verifica la primera condición, entonces $\pi i\colon M' \to M/\mathrm{Im}\, s$ es un isomorfismo y su inverso, compuesto con la proyección canónica $M \to M/\mathrm{Im}\, s$, define un morfismo $r\colon M \to M'$ tal que $ri = \mathrm{Id}_{M'}$. En efecto, si $\pi i(m') = 0$, entonces $i(m') = s(m'')$ para algún $m'' \in M''$. Luego $0 = pi(m') = ps(m'') = m''$ 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 $m - sp(m) \in \mathrm{Ker}\, p = \mathrm{Im}\, i$.

Recíprocamente, si se verifica la condición 2, entonces $p\colon \mathrm{Ker}\, r \to M''$ es un isomorfismo y su inverso define un morfismo $s\colon M'' \to M$ tal que $ps = \mathrm{Id}_{M''}$. 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 $m - ir(m) \in \mathrm{Ker}\, r$.

Además, esta última igualdad muestra que $M = \mathrm{Im}\, i + \mathrm{Ker}\, r$. Como es claro que $0 = \mathrm{Im}\, i \cap \mathrm{Ker}\, r$, concluimos que

$$M \;=\; \mathrm{Im}\, i \,\oplus\, \mathrm{Ker}\, r \;\simeq\; M' \oplus M''\ .$$

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

Corolario 1.2.6 *Toda sucesión exacta $0 \to M' \xrightarrow{i} M \xrightarrow{p} L \to 0$ 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 $s\colon L \to M$, $s\big(\sum_i a_i e_i\big) = \sum_i a_i m_i$, es A-lineal y claramente $ps = \mathrm{Id}_L$, de modo que la sucesión 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

$$auu' = bvu' = cvv' \quad , \quad suu' = tvu' = rvv'.$$

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 imagen 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:

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

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

$$\frac{au}{su} + \frac{b}{t} = \frac{(at + bs)u}{stu} = \frac{at + bs}{st}$$
$$\frac{au}{su} \cdot \frac{b}{t} = \frac{abu}{stu} = \frac{ab}{st}$$

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 $\gamma\colon A \to S^{-1}A$, $\gamma(a) = a/1$, 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 $\gamma\colon A \to S^{-1}A$ se llamará **morfismo de localización**.

Propiedad Universal de la Localización: *Sea $\gamma\colon A \to S^{-1}A$ el morfismo de localización de un anillo A por un sistema multiplicativo S. Si $f\colon A \to B$ 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 $\psi\colon S^{-1}A \to B$ tal que $f = \psi \circ \gamma$:*

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

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

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

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 ψ 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 $\gamma\colon A \to S^{-1}A$ 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 $\gamma\colon A \to S^{-1}A$ 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

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

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

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

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 $f\colon M \to N$ induce de modo natural una aplicación, llamada **localización** de f por S:

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

que es morfismo de $S^{-1}A$-módulos.

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

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

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 $f\colon M \to N$ es un morfismo de A-módulos, existe un único morfismo de $S^{-1}A$-módulos $\phi\colon S^{-1}M \to N$ tal que $f = \phi \circ \gamma$; es decir, $\phi(m/1) = f(m)$ para todo $m \in M$:*

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

Demostración: La unicidad es evidente, pues tal morfismo ϕ 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 ϕ 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: $\mathrm{Im}(S^{-1}f) \subseteq \mathrm{Ker}(S^{-1}g)$ porque

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

Recíprocamente, si $m/s \in \mathrm{Ker}(S^{-1}g)$, 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 $\mathrm{Ker}(S^{-1}g) \subseteq \mathrm{Im}(S^{-1}f)$. Concluimos que $\mathrm{Im}(S^{-1}f) = \mathrm{Ker}(S^{-1}g)$.

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

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 $0 \to M' \to M' \oplus M \to M \to 0$, 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 $f\colon M \to N$ es un morfismo de A-módulos, localizando la sucesión exacta

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

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

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 $\operatorname{Spec} A$. Llamaremos **funciones** a los elementos del anillo A y **puntos** a los elementos de su espectro $\operatorname{Spec} A$, de modo que cada punto $x \in \operatorname{Spec} A$ 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 $x \in \operatorname{Spec} A$ 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*

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

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 $(f)_{\mathrm{o}}$ 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 $\operatorname{Spec} A$ formado por los puntos donde se anulen todas las funciones de $\mathfrak{a}$ y lo denotaremos $(\mathfrak{a})_{\mathrm{o}}$:

$$(\mathfrak{a})_{\mathrm{o}} = \bigcap_{f \in \mathfrak{a}} (f)_{\mathrm{o}} = \{x \in \operatorname{Spec} A\colon\ \mathfrak{a} \subseteq \mathfrak{p}_x\} = \begin{bmatrix}\text{Ideales primos de } A\\ \text{que contienen a } \mathfrak{a}\end{bmatrix}$$

Las siguientes igualdades son de comprobación directa:

$$\begin{aligned}(0)_{\mathrm{o}} &= \operatorname{Spec} A \quad ; \quad (A)_{\mathrm{o}} = \emptyset \\ \Big(\sum_{i\in I} \mathfrak{a}_i\Big)_{\mathrm{o}} &= \bigcap_{i\in I} (\mathfrak{a}_i)_{\mathrm{o}} \\ \Big(\bigcap_{i=1}^{n} \mathfrak{a}_i\Big)_{\mathrm{o}} &= \bigcup_{i=1}^{n} (\mathfrak{a}_i)_{\mathrm{o}}\end{aligned}$$

excepto la última, que basta probar cuando $i = 2$, y se debe a que si en un punto $x \in \operatorname{Spec} A$ no se anula una función $f_1 \in \mathfrak{a}_1$ y no se anula una función $f_2 \in \mathfrak{a}_2$, entonces $f_1 f_2 \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ y no se anula en x.

Estas igualdades muestran que los ceros de los ideales de A son los cerrados de una topología sobre $\operatorname{Spec} A$, llamada **topología de Zariski**. De ahora en adelante consideraremos siempre el espectro de un anillo como un espacio topológico. Por definición, si un punto $x \in \operatorname{Spec} A$ no está en un cerrado $C = (\mathfrak{a})_{\mathrm{o}}$, alguna función $f \in \mathfrak{a}$ no se anula en x (y se anula obviamente en C): *Las funciones de A separan puntos de cerrados en* $\operatorname{Spec} A$.

Ahora 1.1.4 afirma que $(\mathfrak{a})_o = \emptyset$ si y sólo si $\mathfrak{a} = A$, y 1.1.2 afirma que

$$\boxed{\operatorname{Spec}(A/\mathfrak{a}) \;=\; (\mathfrak{a})_{\mathrm{o}}}$$

Proposición 2.3.1 *El cierre de cada punto x del espectro de un anillo A está formado por los ceros de su ideal primo:*

$$\overline{\{x\}} \;=\; (\mathfrak{p}_x)_{\mathrm{o}} \ .$$

Luego $\operatorname{Spec} A$ *es un espacio topológico T_0 (puntos distintos tienen cierres distintos) y los puntos cerrados de* $\operatorname{Spec} A$ *se corresponden con los ideales maximales de A.*

Demostración: La condición de que un cerrado $(\mathfrak{a})_{\mathrm{o}}$ de $\operatorname{Spec} A$ pase por x significa que $\mathfrak{a} \subseteq \mathfrak{p}_x$, en cuyo caso $(\mathfrak{p}_x)_{\mathrm{o}} \subseteq (\mathfrak{a})_{\mathrm{o}}$. Luego $(\mathfrak{p}_x)_{\mathrm{o}}$ es el menor cerrado de $\operatorname{Spec} A$ que contiene a x; es decir, $(\mathfrak{p}_x)_{\mathrm{o}}$ es el cierre de x en $\operatorname{Spec} A$.

Ejemplos: El espectro de un cuerpo tiene un único punto.

De acuerdo con el Lema de Euclides, el espectro de $\mathbb{Z}$ tiene un punto cerrado por cada número primo p (su ideal primo es $p\mathbb{Z}$), y un punto denso (llamado *punto genérico* de $\operatorname{Spec}\mathbb{Z}$) que se corresponde con el ideal primo 0.

Los cerrados no triviales de $\operatorname{Spec}\mathbb{Z}$ son las familias finitas de números primos.

Además, si $n \geq 2$, entonces $\operatorname{Spec}\mathbb{Z}/n\mathbb{Z} \;=\; (n\mathbb{Z})_{\mathrm{o}}$ es el espacio formado por los divisores primos de n, con la topòlogía discreta.

El espectro de $\mathbb{C}[x]$ tiene un punto cerrado por cada número complejo α (su ideal primo $(x-\alpha)$ está formado por todos los polinomios que admiten la raíz $x = \alpha$), y un punto denso (llamado *punto genérico* de $\operatorname{Spec}\mathbb{C}[x]$) que se corresponde con el ideal primo 0.

Los cerrados no triviales de $\operatorname{Spec}\mathbb{C}[x]$ son las familias finitas de números complejos.

Además, $\operatorname{Spec}\mathbb{C}[x]/\big(p(x)\big) = \big(p(x)\big)_{\mathrm{o}}$ es el espacio formado por las raíces complejas de $p(x)$, con la topología discreta.

Si k es un cuerpo, el espectro de $k[x]$ tiene un punto cerrado por cada polinomio unitario irreducible $q(x)$ con coeficientes en k, cuyo ideal primo es $\big(q(x)\big)$, y un punto denso (llamado *punto genérico* de $\operatorname{Spec} k[x]$) que se corresponde con el ideal primo 0.

Los cerrados no triviales de $\operatorname{Spec} k[x]$ son las familias finitas de puntos cerrados.

Además, $\operatorname{Spec} k[x]/\big(p(x)\big) = \big(p(x)\big)_{\mathrm{o}}$ es el espacio formado por los factores irreducibles de $p(x)$, con la topología discreta.

Teorema 2.3.2 *Si S es un sistema multiplicativo de un anillo A, entonces el espectro de A_S está formado por los puntos de* $\operatorname{Spec} A$ *donde no se anula ninguna función $f \in S$:*

$$\operatorname{Spec} A_S = \begin{bmatrix}\text{Ideales primos de } A \\ \text{que no cortan a } S\end{bmatrix}$$

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

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

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

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 $\gamma\colon A \to A_S$ 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 $\{1, f, f^2, \ldots, f^n, \ldots\}$.

Corolario 2.3.3 *Los ideales primos de A_f se corresponden con los ideales primos de A que no contienen a f:*

$$\operatorname{Spec} A_f \;=\; (\operatorname{Spec} A) - (f)_{\mathrm{o}}$$

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

$$\mathrm{r}\,(A) \;=\; \{a \in A\colon\ a^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{N}\}$$

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

Teorema 2.3.4 *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 2.3.3. 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 $x \in \operatorname{Spec} A$ 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 $M \to M_x$ se denota m_x.

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

Demostración: Sea $I = \{f \in A\colon fm = 0\}$ 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 $x \in \operatorname{Spec} A$, 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 $x \in \operatorname{Spec} A$.*

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

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

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

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

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

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

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* $\operatorname{Spec} A$.

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 $M \to M_{\mathfrak{m}}$ siempre es un isomorfismo al localizar en $\mathfrak{m}$. Cuando $\mathfrak{m}^n M = 0$, también es isomorfismo al localizar en cualquier otro punto $x \in \operatorname{Spec} A$. 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 $\operatorname{Spec} A$. 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 $x \in \operatorname{Spec} A$. 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 2.3.2 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 $\{m_1, \ldots, m_n\}$ de generadores de M tales que $m_2, \ldots, m_n$ no generen M. Por hipótesis $M = \mathfrak{m}M = \mathfrak{m}(\mathcal{O}m_1 + \ldots + \mathcal{O}m_n) = \mathfrak{m}m_1 + \ldots + \mathfrak{m}m_n$, así que $m_1 = f_1m_1 + f_2m_2 + \ldots + f_nm_n$ para ciertas funciones $f_1, \ldots, f_n \in \mathfrak{m}$. Luego

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

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 $\mathcal{O}m_2 + \ldots + \mathcal{O}m_n$. Luego $m_2, \ldots, m_n$ 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 $m_1, \ldots, m_n \in M$ generen el $\mathcal{O}$-módulo M es que $\bar{m}_1, \ldots, \bar{m}_n$ generen el k-espacio vectorial $M/\mathfrak{m}M$.

Demostración: Sea $N = \mathcal{O}m_1 + \ldots + \mathcal{O}m_n$. La condición de que $\bar{m}_1, \ldots, \bar{m}_n$ 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 $m_1, \ldots, m_n$ 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** si 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 Σ el cuerpo de fracciones de A; es decir, Σ 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 Σ. Nótese que para un A-módulo libre $L = A \oplus \overset{r}{\dots} \oplus A$ 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 $\pi\colon L \to L_{r-n}$ a la proyección natural, tenemos las sucesiones exactas

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

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 $\pi\colon L \to M$ 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 $\pi\colon L' \to M'$ 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):

$$\begin{pmatrix} 14 & 34 & 39 \\ 0 & 6 & 9 \end{pmatrix} \qquad \begin{pmatrix} 14 & 34 & 5 \\ 0 & 6 & 3 \end{pmatrix} \qquad \begin{pmatrix} 14 & 24 & 5 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 14 & -4 & 5 \\ 0 & 0 & 3 \end{pmatrix} \qquad \begin{pmatrix} 2 & -4 & 5 \\ 0 & 0 & 3 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 & 5 \\ 0 & 0 & 3 \end{pmatrix}$$

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 $A \xrightarrow{\cdot m} M$ 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 $M \to M_S$, 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 $M \to M_S$. Si $m_1, \ldots, m_s$ es un sistema de generadores de M, entonces $m_1/1, \ldots, m_s/1$ es un sistema de generadores de M_S como espacio vectorial sobre Σ. De dicho sistema de generadores podemos extraer una base, digamos $m_1/1, \ldots, m_r/1$. Podemos escribir entonces:

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

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 $L = A(m_1/b) \oplus \ldots \oplus A(m_r/b)$, 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*

$$M \simeq (A \oplus \overset{r}{\ldots} \oplus A) \oplus T(M)$$

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:

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

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, $L \simeq A \oplus \overset{r}{\ldots} \oplus A$ 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 $\nabla\colon E \to E$, $\nabla(a_n) = (a_{n+1})$, que induce una estructura de $\mathbb{C}[x]$-módulo en E. Ahora las sucesiones de Fibonacci forman el núcleo del endomorfismo $\nabla^2 - \nabla - \mathrm{Id}$; 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 α, obtenemos que cada sucesión de Fibonacci (a_n) descompone, y de modo único, en suma de una progresión geométrica de razón α y otra de razón β:

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

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 $\mathcal{C}^\infty$, en el sentido de que lo son $x(t)$ e $y(t)$, y el endomorfismo $D\colon E \to E$, $D(f(t)) = f'(t) = x'(t) + iy'(t)$, 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 $D^2 + \mathrm{Id}$; 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

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

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

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

Definición: Sea M un A-módulo. Diremos que $\mathfrak{a}=\{a\in A\colon\ aM=0\}$ 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 $M=Am_1+\ldots+Am_n$ y $a_im_i=0$, entonces $a_1\ldots a_nM=0$.

Segundo teorema de descomposición: *Sea $a=p_1^{n_1}\cdots p_s^{n_s}$ 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*

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

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

$$M \;=\; \ker a \;=\; \ker p_1^{n_1}\oplus\ker\left(p_2^{n_2}\cdots p_s^{n_s}\right) \;=\; \ldots \;=\; \ker p_1^{n_1}\oplus\ldots\oplus\ker p_s^{n_s}.$$

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

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

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 $n=n_1\geq\cdots\geq n_s$ tal que*

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

Demostración: 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 A-módulos libres de rango finito. Elegidas bases $(e'_1,\ldots,e'_n)$ y $(e_1,\ldots,e_m)$ 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:

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

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**:

Transformación Elemental	Cambio de Base
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_j por un invertible u	Sustituir e'_j por ue'_j
Multiplicar F_i por un invertible u	Sustituir e_i por $u^{-1}e_i$

donde $i \neq j$ y $a \in A$.

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

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

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

Estas igualdades permiten despejar los números ν_j a partir de las dimensiones de los espacios vectoriales $p^iM/p^{i+1}M$; 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

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

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: $n_{i1} \geq n_{i2} \geq \cdots$ 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 $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$, y tenemos un isomorfismo de anillos*

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

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 $c=c(a+b)=ca+cb\in\mathfrak{ab}$; así que $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$, pues la inclusión contraria siempre es válida.

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

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

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 $\phi_1A\subseteq\phi_2A\subseteq\ldots\subseteq\phi_mA$ tal que*

$$M\simeq A/\phi_1A\oplus\ldots\oplus A/\phi_mA\ .$$

Demostración: Sabemos que

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

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

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

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

$$M\simeq A/\phi_1A\oplus\ldots\oplus A/\phi_mA$$

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 $\phi_1,\cdots,\phi_m$ 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 ϕ_1 es el anulador del módulo, y que la sucesión de factores invariantes puede considerarse infinita sin más que tomar $1=\phi_{m+1}=\phi_{m+2}=\cdots$. 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:

$$n \cdot g = g + \overset{n}{\ldots} + g$$
$$(-n) \cdot g = -g - \overset{n}{\ldots} - g$$

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:

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

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 ϕ_1 (i.e. el anulador) de G no es nulo.*

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

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 $(e'_1, \ldots, e'_n)$ y $(e_1, \ldots, e_m)$ 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:

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

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 $L_m/\mathrm{Im}\, f \simeq M$ coinciden con los coeficientes de la diagonal de $\bar{A}$ (completados con ceros cuando $n < m$); es decir, $\phi_1 = a_m$, $\phi_2 = a_{m-1}$,...

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*

$$c_i = \phi_{i+1} \cdots \phi_m$$
$$\phi_i = c_{i-1}/c_i$$

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 $\phi_1, \ldots, \phi_m$ son los factores invariantes, entonces $M \simeq A/\phi_1 A \oplus \ldots \oplus A/\phi_m A$ 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

$$f\colon \mathbb{Z}^n \to \mathbb{Z}^m \qquad , \qquad f(X) = AX,$$

y su conúcleo $M = \mathbb{Z}^m/\mathrm{Im}\, f$, de modo que $\mathrm{rg}(M) = m - \mathrm{rg}(A)$. 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 $B \in \mathrm{Im}\, f$ 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 $\mathrm{rg}(M/\mathbb{Z}B) = \mathrm{rg}(M) - 1$ y concluimos que $\mathrm{rg}(A|B) = \mathrm{rg}(A) + 1$. Si B es de torsión en M, entonces $\mathrm{rg}(A|B) = \mathrm{rg}(A) = r$; 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

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

reducimos la matriz del sistema mediante transformaciones elementales:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \left(\begin{array}{ccc:c} 5 & -2 & -11 & 2 \\ 3 & 2 & -5 & -2 \end{array}\right)$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \left(\begin{array}{ccc:c} 7 & -2 & -11 & 2 \\ 1 & 2 & -5 & -2 \end{array}\right)$$

$$\text{„} \qquad \left(\begin{array}{ccc:c} 1 & 2 & -5 & -2 \\ 7 & -2 & -11 & 2 \end{array}\right)$$

$$\text{„} \qquad \left(\begin{array}{ccc:c} 1 & 2 & -5 & -2 \\ 0 & -16 & 24 & 16 \end{array}\right)$$

$$\begin{pmatrix} 1 & -2 & 5 \\ -1 & 3 & -5 \\ 0 & 0 & 1 \end{pmatrix} \quad \left(\begin{array}{ccc:c} 1 & 0 & 0 & -2 \\ 0 & -16 & 24 & 16 \end{array}\right)$$

$$B = \begin{pmatrix} 1 & 3 & -4 \\ 1 & -2 & 1 \\ 0 & 1 & -2 \end{pmatrix} \quad \left(\begin{array}{ccc:c} 1 & 0 & 0 & -2 \\ 0 & 8 & 0 & 16 \end{array}\right)$$

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

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & -4 \\ 1 & -2 & 1 \\ 0 & 1 & -2 \end{pmatrix} \begin{pmatrix} -2 \\ 2 \\ \lambda \end{pmatrix} \quad , \quad \left\{\begin{array}{l} x_1 = 4 - 4\lambda \\ x_2 = -2 + \lambda \\ x_3 = 2 - 2\lambda \end{array}\right.$$

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

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

realizando transformaciones elementales

$$\left(\begin{array}{cccc:c} 5 & -2 & -11 & \vdots & a \\ 3 & 2 & -5 & \vdots & b \end{array}\right) \quad , \quad \cdots\cdots \quad , \quad \left(\begin{array}{ccc:c} 1 & 0 & 0 & \vdots & b \\ 0 & 8 & 0 & \vdots & a-7b \end{array}\right)$$

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

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

i.e., G es el conúcleo del morfismo $f\colon \mathbb{Z}^2 \to \mathbb{Z}^3$, $f(x_1, x_2) = x_1(8, 10, 12) + x_2(8, 4, 6)$. 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 $G = \mathbb{Z}^3/\operatorname{Im} f \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus \mathbb{Z}$. 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:

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

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[1]) de G en X a toda aplicación $G \times X \dashrightarrow X$ 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 $\rho\colon G \to \mathrm{Biy}(X)$, $\rho(g)(x) = g \cdot x$, en el grupo $\mathrm{Biy}(X)$ 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 $f\colon X \to Y$ 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

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

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

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

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

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

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 $G = 1$).

[1] 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** $Z(G) := \{a \in G\colon\ ab = ba,\ \forall b \in G\}$ 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** $N(H) := \{g \in G\colon\ gHg^{-1} = H\}$ de H en G, que es el mayor subgrupo de G tal que $H \lhd N(H)$ (el símbolo $H_1 \lhd H_2$ 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*

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

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

Demostración: La aplicación $G/I_x \to Gx$, $[g] \mapsto gx$, 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*

$$|X| \equiv |X^G| \quad (\text{módulo } p)$$

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*

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

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 $\pi\colon G \to G/H$. Procediendo por inducción sobre el orden de G, podemos suponer la existencia de una sucesión de subgrupos normales de G/H

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

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 $\pi\colon G \to G/H$. 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 $N \lhd G$ 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 $G \to \mathrm{Biy}(X) = S_n$ 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

$$1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{n-1} \lhd H_n = G$$

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

$$1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{n-1} \lhd H_n = G$$

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:

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

Si existiera una sucesión de subgrupos $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{d-1} \lhd H_d = S_n$ 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 $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ 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 $1 = H'_0 \subseteq H'_1 \subseteq \ldots \subseteq H'_n = H$ 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 $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$, la proyección canónica $\pi\colon G \to G/H$, 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 $1 = H'_0 \subseteq H'_1 \subseteq \ldots \subseteq H'_n = H$ 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 $\pi\colon G \to G/H$ y sendas resoluciones

$$1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{n-1} \lhd H_n = H$$
$$1 = H'_0 \lhd H'_1 \lhd \ldots \lhd H'_{d-1} \lhd H'_d = G/H$$

Es sencillo comprobar que en la sucesión creciente de subgrupos

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

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 $H \lhd G$ 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 $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ 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 $(a_1a_2)(b_1b_2)$ de dos trasposiciones siempre es producto de 3-ciclos. Ahora bien, tenemos que

$$\begin{array}{ll} (a_1a_2)(b_1b_2) = (a_1a_2b_1)(a_2b_1b_2) & \text{cuando las trasposiciones son disjuntas} \\ (a_1a_2)(b_1b_2) = (a_2a_1b_2) & \text{cuando } a_1 = b_1 \end{array}$$

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 α 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

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

y que $d_1, d_2, \ldots$ es una sucesión decreciente. Sea $s \geq 1$ el número de elementos que α 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 α 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 $\alpha = (12)(34)(56)\ldots \Rightarrow \alpha\beta(3) \neq \beta\alpha(3)$; 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 α, en contradicción con la elección de α. 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 3 y consideremos una permutación τ que transforme 1,2,3 en i, j, k:

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

Intercambiando l y m si fuera preciso podemos suponer que τ 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 $H \lhd S_n$, entonces $H \cap A_n \lhd A_n$ 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 σ debe coincidir con σ, lo cual es imposible cuando $n \geq 3$ (el caso $n = 2$ es inmediato). Concluimos que $H = 1$.