Notas de Álgebra II

Guillermo Cortiñas

10 de agosto de 2020, 17:10

Introducción

Éstas son las notas del curso de Álgebra II dictado en la FCEyN-UBA en el primer cuatrimestre virtual de 2020. La materia es una introducción a las teorías de grupos, anillos y módulos. Como en la mayoría de las cursadas, en este cuatrimestre se dieron los teoremas de Sylow (1.7.18, 1.7.19, 1.7.22) y el teorema de estructura para módulos finitamente generados sobre un dominio principal (4.4.2). También vimos otros resultados clásicos importantes, como por ejemplo, los teoremas de Morita 3.2.1, Baer 3.8.9, Artin-Wedderburn 3.11.1 y Maschke 3.11.6 y el teorema de estructura para módulos inyectivos sobre un dominio principal 4.6.9. Otros temas que figuran en el programa de la materia, como localización o producto tensorial, no fueron incluídos.

Las demostraciones presentadas distan mucho de ser originales; muchas provienen de una mezcla de referencias que son clásicas en la materia (e.g. [2], [3], [5]) y otras del folklore del tema. Los temas tratados son tan clásicos que incluso aquéllas demostraciones para las cuales no se consultaron referencias, seguramente se le ocurrieron antes a otros.

En esta versión de las notas incluímos también las guías de trabajos prácticos que utilizamos en la cursada, que son el fruto no sólo de quienes dictamos la materia en este cuatrimestre sino del trabajo de los muchos docentes que han pasado por ella a lo largo de los años.

Es un placer agradecer a Iván Sadofschi Costa y Guido Arnone, que me acompañaron en las clases prácticas; en particular Iván se encargó de seleccionar los ejercicios de las guías de trabajos prácticos que utilizamos. Gracias también a todos los alumnos que me indicaron correcciones, en particular a Janou Glaeser.

Guillermo Cortiñas
Maschwitz, agosto 2020.

Índice general

Capítulo 1

Grupos

1.1. Semigrupos, monoides y grupos

Este curso es una introducción al estudio de las estructuras algebraicas. Las estructuras que veremos consisten de un conjunto X junto con una o más operaciones binarias. Una *operación binaria* en un conjunto X es una función

$$\cdot : X \times X \to X.$$

Decimos que $\cdot$ es

- *asociativa* si $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para todo $x, y, z \in X$,
- *conmutativa* su $x \cdot y = y \cdot x$ para todo $x, y \in X$.

Un elemento $e \in X$ se llama *neutro* para $\cdot$ si la siguientes identidades se cumplen para todo $x \in X$

$$e \cdot x = x \cdot e = x.$$

Un elemento $x \in X$ es *inversible* para $\cdot$ si existe $y \in X$ tal que

$$x \cdot y = y \cdot x = e.$$

Un tal elemento y, cuando existe, se llama la *inversa* de x.

Ejercicios 1.1.1. Probar

i) Si e y f son elementos neutros para $\cdot$, entonces $e = f$.

ii) Si $\cdot$ es asociativa, entonces x tiene inversa a ambos lados si y sólo si es inversible. En ese caso la inversa de un elemento inversible es única.

Notación 1.1.2. Si S es un monoide cuya operación se denota multiplicativamente, e.g. $\cdot$, usualmente llamaremos 1 al elemento neturo. En caso en que la operación se denote por $+$, utilizaremos 0 para denotar al neutro. Del mismo modo, la inversa de un elemento inversible se denota x^{-1} en notación multiplicativa y $-x$ en notación aditiva. La notación aditiva se utiliza sólo cuando el monoide en cuestión es abeliano; la notación multiplicativa se puede utilizar tanto en el caso abeliano como en el no abeliano. En notación multiplicativa, es frecuente omitir el símbolo $\cdot$; se escribe xy en vez de $x \cdot y$.

Un *semigrupo* es un conjunto con una operación asociativa $\cdot$. Un *monoide* es un semigrupo que tiene elemento neutro. Un *grupo* es un monoide en el cual todo elemento es inversible. Un semigrupo, monoide o grupo se dice *abeliano* si la operación $\cdot$ es conmutativa.

Ejemplos 1.1.3. El conjunto $\mathbb{N}$ de los números naturales es un semigrupo abeliano para la suma y un monoide abeliano para el producto. El conjunto $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ es un monoide abeliano, tanto con respecto a la suma como con respecto al producto. El conjunto $\mathbb{Z}$, equipado con la suma, es un grupo abeliano; equipado con el producto, es un monoide abeliano.

Ejemplos 1.1.4. Sea $n \geq 1$ y sea $M_n\mathbb{C}$ el conjunto de las matrices complejas de $n \times n$. Equipado con la suma, este conjunto es un monoide abeliano. Equipado con el producto, es un monoide no abeliano. El subconjunto $\mathrm{GL}_n(\mathbb{C})$ de las matrices inversibles es un grupo para el producto. En particular, tomando $n = 1$, obtenemos el grupo

$$\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^* := \mathbb{C} \setminus \{0\}.$$

También es un grupo el subconjunto $U_n \subset \mathrm{GL}_n(\mathbb{C})$ formado por todas las matrices A tales que $A^{-1} = \bar{A}^t$, la matriz adjunta. En particular, tomando $n = 1$ obtenemos

$$U_1 = S^1 := \{z \in \mathbb{C} : |z| = 1\}.$$

Ejercicio 1.1.5. Sea $M = (M, \cdot)$ un monoide y sea $\mathrm{inv}(M) \subset M$ el subconjunto de todos los elementos inversibles. Probar que $\mathrm{inv}(M)$ es cerrado por $\cdot$ y que $(\mathrm{inv}(M), \cdot)$ es un grupo.

Ejercicio 1.1.6. Sean M y N monoides y sea $M \times N$ su producto cartesiano.

- Probar que $M \times N$, equipado con la siguiente operación, es un monoide

$$(m_1, n_1) \cdot (m_2, n_2) = (m_1 \cdot m_2, n_1 \cdot n_2).$$

- Probar que $\mathrm{inv}(M \times N) = \mathrm{inv}(M) \times \mathrm{inv}(N)$. Deducir que $M \times N$ es un grupo cuando M y N lo son.

Observación 1.1.7. Cuando los monoides M y N son abelianos, su producto cartesiano suele denotarse con $\oplus$; así $M \oplus N = M \times N$.

Notación 1.1.8. Si S es un semigrupo y $X_1, X_2 \subset S$, escribimos

$$X_1 \cdot X_2 = \{x_1 \cdot x_2 : x_i \in X_i, i = 1, 2\}.$$

Si además S es un grupo y $X \subset S$ ponemos

$$X^{-1} = \{x^{-1} : x \in X\}.$$

Notar que si X tiene más de un elemento, $X \cdot X^{-1} \neq \{e\}$

1.2. Subgrupos

Sean G un grupo, con operación $\cdot$ y elemento neutro 1. Un *subgrupo* de G es un subconjunto $S \subset G$ tal que

i) $1 \in S$.

ii) $S \cdot S \subset S$.

iii) $S^{-1} \subset S$.

Observación 1.2.1. En presencia de las condiciones ii) y iii) de la definición de grupo, la condición i) puede reemplazarse equivalentemente por la condición

i') $S \neq \emptyset$.

En presencia de i), la inclusión de la condición ii) equivale a la igualdad $S \cdot S = S$. Finalmente, en iii), la inclusión equivale a la igualdad $S = S^{-1}$.

Ejemplos 1.2.2. $U_n \subset \mathrm{GL}_n \mathbb{C}$ es un subgrupo, lo mismo que

$$T_n\mathbb{C} = \{A \in M_n\mathbb{C} : (\forall i)\ A_{i,i} = 1, A_{i,j} = 0 \text{ si } i > j\}.$$

Sea G un grupo. Entonces G y $1 := \{1\}$ son ambos sugrupos de G.

Sea $S \subset G$ un subgrupo. Decimos que S es *normal* (en G) si

$$gsg^{-1} \in S \quad \forall g \in G, s \in S.$$

Para enfatizar que S es un subgrupo normal de G, escribimos $S \lhd G$.

Ejemplo 1.2.3. Sea G un grupo. El *centro* de G es

$$Z(G) = \{z \in G : (\forall g \in G) zg = gz\}.$$

Notar que $Z(G) \lhd G$.

Ejercicio 1.2.4. Sean G un grupo y $\{S_i\}_{i\in I}$ una familia de subgrupos de G.

i) Probar que $S = \bigcap_{i\in I} S_i$ es subgrupo de G.

ii) Probar que si además $S_i \lhd G$ para todo $i \in I$, entonces $S \lhd G$.

Sean G un grupo y $X \subset G$ un subconjunto. Entonces X está contenido en al menos un subgrupo de G; el propio G. En general, este no es el subrupo más pequeño que lo contiene. Se sigue del Ejercicio 1.2.4 que el subgrupo de G más pequeño que contiene a X es

$$\langle X \rangle := \bigcap \{S \subset G : S \text{ subgrupo.}\}$$

El subgrupo $\langle X \rangle$ se llama *subgrupo generado* por X. Los elementos de este subgrupo pueden describirse explícitamente, como veremos a continuación. Observemos que si $x_1, \ldots, x_n \in X$ y $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, entonces

$$x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \langle X \rangle. \tag{1.2.5}$$

En otras palabras el subconjunto $S \subset G$ de todos los elementos de la forma (1.2.5) está contenido en $\langle X \rangle$. Por otra parte la inversa de un elemento de la

forma (1.2.5) y el producto de dos de ellos es de nuevo de la misma forma, o sea $S^{-1} \subset S$ y $SS \subset S$. Si además $X \neq \emptyset$, tenemos también $1 \in S$, de modo que en este caso, S es un subgrupo contenido en todos los subgrupos que contienen a G, y por tanto coincide con $\langle X \rangle$. Por otro lado, es claro que

$$\langle \emptyset \rangle = 1.$$

De modo que, adoptando la convención de que el producto de la familia vacía de elementos de un grupo da el elemento neutro, podemos decir que, siempre, los elementos de $\langle X \rangle$ son los productos de familias finitas de elementos de $X \cup X^{-1}$.

Notación 1.2.6. Si $X = \{x_1, \ldots, x_n\} \subset G$, escribimos

$$\langle x_1, \ldots, x_n \rangle := \langle X \rangle$$

Observación 1.2.7. Sean G un grupo y $x, y \in G$. Entonces $S_0 = \{x^i y^j : i, j \in \mathbb{Z}\} \subset \langle x, y \rangle$, pero la inclusión puede ser estricta. Por ejemplo, las potencias $(xy)^n$ con $n \geq 2$ no tienen porqué estar en S_0.

Notación 1.2.8. Si X es un conjunto, denotamos por $|X|$ a su cardinal.

Sean G un grupo y $S \subset G$ un subgrupo. Un *conjunto de generadores* de S es un subconjunto tal que $S = \langle X \rangle$. Decimos que un grupo G es *cíclico* si existe $g \in G$ tal que $G = \langle g \rangle$. El *orden* de un elemento $g \in G$ es $|\langle g \rangle|$ si éste es finito, y es infinito en otro caso. El orden de g se denota $\operatorname{ord}(g)$.

Observación 1.2.9. Sean G un grupo y $g \in G$. Entonces

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}. \tag{1.2.10}$$

Aquí, como venimos haciendo, no suponemos que G sea abeliano, y usamos por tanto notación multiplicativa. Por la convención notacional que adoptamos arriba, $g^0 = 1$. Además si $n > 0$, g^n es el producto de g consigo mismo n-veces; si $n < 0$ es $(g^{-1})^{-n}$. Si G es abeliano y usamos notación aditiva para su operación, escribimos ng en lugar de g^n; así, el subgrupo generado por g es $\{ng : n \in \mathbb{Z}\}$.

Lema 1.2.11. *Sean G un grupo y $g \in G$. Si $g = 1$, $\operatorname{ord}(g) = 1$. Sea $g \in G \setminus \{1\}$. Entonces $\operatorname{ord}(g)$ es finito si y sólo si el conjunto*

$$X = \{n \in \mathbb{N} : g^n = 1\}$$

no es vacío, en cuyo caso $\operatorname{ord}(g) = \min X$.

Demostración. Sea $g \in G \setminus \{1\}$. Supongamos que $\operatorname{ord}(g) < \infty$. En vista de (1.2.10), hay $n \neq m$ tales que $g^n = g^m$. Est igualdad equivale tanto a $g^{m-n} = 1$ como a $g^{n-m} = 1$. En particular, $X \neq \emptyset$. Sea $d = \min X$; entonces $\langle g \rangle = \{1 = g^0, g = g^1, \ldots, g^{d-1}\}$. Además si $0 \leq i \leq j < d$, entonces nuevamente $g^i = g^j$ equivale a $g^{j-i} = 1$, o sea a que $j - i \in X$. Se sigue que $i = j$, por minimalidad de d. Luego $\operatorname{ord}(g) = |\langle g \rangle|$. □

Ejemplo 1.2.12. Sea $z \in \mathbb{C}^*$. Entonces z tiene orden finito si y sólo si existe $n \in \mathbb{N}$ tal que z es raíz n-ésima de la unidad. En ese caso, z tiene orden m si y sólo si es raíz primitiva de ese orden. En términos de la notación de Álgebra I,

$$\{z \in \mathbb{C}^* : \operatorname{ord}(z) < \infty\} = \bigcup_{n \geq 1} G_n = G_\infty.$$

Ejemplo 1.2.13. Como siempre, consideramos a $\mathbb{Z}$ como grupo con respecto a la suma, y adoptamos entonces notación aditiva. Así, si $m \in \mathbb{Z}$, el subgrupo generado por m es

$$\langle m \rangle = m\mathbb{Z}.$$

Sea $S \subset \mathbb{Z}$ un subgrupo. Vamos a probar que S es cíclico. Esto es claro para $S = 0$. Si $S \neq 0$, tiene un elemento no nulo. Más aún, dado que S es cerrado por inversos aditivos, tiene un elemento positivo. Es decir, $S \cap \mathbb{N} \neq \emptyset$. Por el principio de buena ordenación de los naturales, existe $m := \text{mín}(S \cap \mathbb{N})$. Es claro que $m\mathbb{Z} \subset S$. Además si $s \in S$, por algoritmo de división, podemos escribir a $s = mq + r$ como la suma de un elemento de $m\mathbb{Z}$ más un elemento de $\in \mathbb{N}_0 \cap S$ estrictamente menor que m. Dado que $r = s - mq \in S$ y dada la minimalidad de m, tiene que ser $r = 0$. Por tanto $S = m\mathbb{Z}$.

Ejercicio 1.2.14. Sean $X = \{S \subset \mathbb{Z} \text{ subgrupo }\}$ y $f : \mathbb{N}_0 \to X$, $f(n) = n\mathbb{Z}$. Probar

i) f es biyectiva.

ii) $f(m) \subset f(n) \iff n$ divide a m.

Ejemplo 1.2.15. Sea $\theta \in \mathbb{R}$ y sean

$$R = R_\theta := \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Notar que ambas matrices son inversibles; sea $D(\theta) = \langle R, S \rangle \subset \mathrm{GL}_2(\mathbb{R})$. Se tiene

$$S^2 = 1, \quad SRS = R^{-1}.$$

Se sigue que

$$D(\theta) = \{R^j S^i : j \in \mathbb{Z}, i \in \{0, 1\}\}.$$

Observemos que R es la matriz de la rotación de ángulo θ; en términos de la identificación usual $\mathbb{R}^2 = \mathbb{C}$, R corresponde a la multiplicación por $e^{i\theta}$, por la fórmula de De Môivre. En particular $\text{ord}(R) = \text{ord}(e^{i\theta})$ es finito si y sólo si $q := \theta/2\pi$ es racional. En ese caso, si $q = k/n$ con $(k : n) = 1$, tenemos $\text{ord}(g) = n$. Así,

$$n = |\{R^j : j \in \mathbb{Z}\}| = |\{R^j S : j \in \mathbb{Z}\}|.$$

Notemos además que la matriz R tiene determinante 1, lo mismo que cualquiera de sus potencias, mientras que S y todos los elementos de la forma $R^j S$ tienen determinante -1. Concluimos entonces que $|D(\theta)| = 2n$.

Ejercicio 1.2.16. Sea

$$\exp : \mathbb{R} \to \mathbb{C}^*, \quad \exp(\theta) = e^{i\theta}.$$

Sean $q, p \in \mathbb{Q}$. Probar que

$$D(2q\pi) = D(2p\pi) \iff \text{ord}(\exp(i2q\pi)) = \text{ord}(\exp(i2p\pi)).$$

1.3. Producto semidirecto

Sean $S, K \subset G$; decimos que S *normaliza* K si $\forall s \in S$, $sKs^{-1} = K$. Por ejemplo, $K \lhd G$ si y sólo si G normaliza K. Veremos que en general, cuando S normaliza K, se tiene que $SK = KS$ es un subgrupo de G. En efecto, si $s \in S$ y $k \in K$ se tiene

$$sk = sks^{-1}s \in KS, \quad ks = s(s^{-1}ks) \in SK.$$

Luego

$$SKSK = SKKS = SKS = SSK = SK.$$

Notemos además que $K \lhd SK$; si $s \in S$ y $k, h \in K$,

$$skh(sk)^{-1} = s(khk^{-1})s^{-1} \in sKs^{-1} = K.$$

Cuando $S \cap K = 1$, el subgrupo SK se llama el *producto semidirecto* de S y K.

Ejemplo 1.3.1. El grupo $D(\theta)$ del Ejemplo 1.2.15 es el producto semidirecto del subgrupo $K = \{R^j : j \in \mathbb{Z}\}$ y el subgrupo $T = \{1, S\}$.

1.4. Morfismos

Sean G_1 y G_2 grupos. Un *morfismo* de G_1 en G_2 es una función $f : G_1 \to G_2$ tal que $f(1) = 1$ y $f(xy) = f(x)f(y)$ $\forall x, y \in G_1$. El *núcleo* de un morfismo f es el conjunto

$$\mathrm{Ker}(f) = f^{-1}(\{1\}).$$

Decimos que f es un *epimorfismo* si es suryectivo, un *monomorfismo* si es inyectivo y un *isomorfismo* si es biyectivo. Un *endomorfismo* de un grupo G es un morfismo $f : G \to G$; un *automorfismo* es un endomorfismo biyectivo.

Ejercicio 1.4.1. Sea $f : G_1 \to G_2$ un morfismo de grupos. Probar que f preserva inversas: si $x \in G_1$ entonces $f(x^{-1}) = f(x)^{-1}$.

Ejemplo 1.4.2. Sea G un grupo. Si $f : \mathbb{Z} \to G$ es un morfismo y $\sigma = f(1)$, entonces

$$f(n) = \sigma^n \quad \forall n \in \mathbb{Z}. \tag{1.4.3}$$

Recíprocamente, si $\sigma \in G$, (1.4.3) define un morfismo $\mathbb{Z} \to G$. En conclusión, dar un morfismo $\mathbb{Z} \to G$, equivale a dar un elemento $\sigma \in G$.

Ejemplo 1.4.4. Sea G un grupo abeliano y sea $F_j : G \to G$, $F_j(x) = x^j$. Tenemos $F_j(1) = 1^j = 1$ y como G es abeliano,

$$F_j(xy) = (xy)^j = x^j y^j = F_j(x)F_j(y).$$

Hemos probado así que F_j es un endomorfismo de G si G es abeliano. Supongamos más aún que G es cíclico. Veremos que entonces los F_j son todos los endomorfismos de G. En efecto, si $G = \langle\sigma\rangle$ y $f : G \to G$ es morfismo, entonces $f(\sigma) = \sigma^j$ para algún j, lo que implica que para todo i,

$$f(\sigma^i) = \sigma^{ij} = F_j(\sigma^i).$$

Notemos además que $F_1 = \mathrm{id}$ y $F_jF_k = F_{jk}$. Luego si G es cíclico infinito, los F_j son todos distintos, y sus únicos autormorfismos son F_1 y F_{-1}. Si en cambio G es cíclico con n elementos, $F_j = F_k \iff j \equiv k \mod (n)$, y F_j es automorfismo si y sólo si $(j : n) = 1$.

Ejemplo 1.4.5. Sean G un grupo y $g \in G$. Sea

$$\mathrm{ad}(g) : G \to G, \quad \mathrm{ad}(g)(x) = gxg^{-1}.$$

Notemos que $\mathrm{ad}(g)$ es un automorfismo con inversa $\mathrm{ad}(g^{-1})$. Un automorfismo f de G se dice *interior* si existe g tal que $f = \mathrm{ad}(g)$. Notar que un subgrupo $S \subset G$ es normal si y sólo si $f(S) = S$ para todo automorfismo interior f de G.

Ejercicio 1.4.6. Sean $f : G_1 \to G_2$ un morfismo de grupos, y $g, x \in G$. Probar que

$$f(\mathrm{ad}(g)(x)) = \mathrm{ad}(f(g))(f(x)).$$

Ejercicio 1.4.7.

i) Sean X_1, X_2, Y_1, Y_2 conjuntos y $\mu_X : X_1 \to X_2$, $\mu_Y : Y_1 \to Y_2$, $\phi_1 : X_1 \to Y_1$ y $\phi_2 : X_2 \to Y_2$ funciones. Probar que si ϕ_1 y ϕ_2 son biyectivas y $\mu_Y\phi_1 = \phi_2\mu_X$, entonces $\phi_2^{-1}\mu_Y = \mu_X\phi_1^{-1}$.

ii) Sea $f : G_1 \to G_2$ un isomorfismo de grupos. Probar que f^{-1} también es morfismo. Sugerencia: aplicar i).

iii) Probar que si $f : G \to H$ y $g : H \to K$ son morfismos de grupos, entonces $g \circ f : G \to K$ también lo es.

Decimos que dos grupos G_1 y G_2 son *isomorfos*, y escribimos $G_1 \cong G_2$, si existe un isomorfismo $G_1 \to G_2$. Notar que, por el Ejercicio 1.4.7, $\cong$ es una relación de equivalencia.

Lema 1.4.8. *Sea G un grupo cíclico.*

i) Si $|G| = \infty$, $G \cong \mathbb{Z}$.

ii) Si $|G| = d < \infty$, $G \cong G_d$.

Demostración. Sea $\sigma \in G$ un generador; por definición, $\mathrm{ord}(\sigma) = |G|$. Notemos que si $n, m \in \mathbb{Z}$,

$$\sigma^n = \sigma^m \iff \sigma^{n-m} = 1. \tag{1.4.9}$$

Si $\mathrm{ord}(\sigma) = \infty$, (1.4.9) se da $\iff n = m$. En otras palabras, si $|G| = \infty$ el morfismo $f : \mathbb{Z} \to G$, $f(n) = \sigma^n$ es un isomorfismo. Si en cambio $\mathrm{ord}(\sigma) = d < \infty$, (1.4.9) equivale a que d divide a $n - m$. Esto sucede para todo grupo cíclico de d elementos y todo generador. En particular, se aplica al grupo G_d y a cualquier raíz primitiva d-ésima ζ de la unidad. Por tanto la aplicación $G \to G_d$, $\sigma^n \mapsto \zeta^n$ está bien definida y es biyectiva. Es claro además que es un morfismo; luego $G \cong G_d$, como queríamos probar.

□

Lema 1.4.10. *Sean $f : G \to H$ un morfismo, $K = \mathrm{Ker}(f)$ y $g \in G$. Entonces $f^{-1}(f(g)) = gK$. En particular, f es monomorfismo $\iff K = 1$.*

Demostración. Sea $x \in G$. Entonces $x \in f^{-1}(f(g)) \iff f(x) = f(g) \iff f(g^{-1}x) = 1 \iff g^{-1}x \in K \iff x \in gK$. □

Ejemplo 1.4.11. Sean G un grupo, S, K subgrupos de G. Supongamos que $sk = ks\ \forall s \in S, k \in K$. Entonces $k_1s_1k_2s_2 = k_1k_2s_1s_2\ \forall k_1, k_2 \in K, s_1, s_2 \in S$. En otras palabras, la función

$$f : K \times S \to KS,$$

es morfismo de grupos. Claramente, f es suryectiva. Además,

$$f(k, s) = 1 \iff ks = 1 \iff k = s^{-1}.$$

Luego $\mathrm{Ker}(f) = \{(x, x^{-1}) : x \in K \cap S\}$. Esto prueba que f es un isomorfismo si y sólo si $K \cap S = 1$.

Ejemplo 1.4.12. Sea $n, m \geq 1$ coprimos, y sea $C = \langle \sigma \rangle$ un grupo cíclico de orden nm. Veremos que C es isomorfo a un producto $C_1 \times C_2$ con C_1 cíclico de orden n y C_2 cíclico de orden m. Sean $C_1 = \langle \sigma^m \rangle$ y $C_2 = \langle \sigma^n \rangle$. Claramente C_1 y C_2 son cíclicos, de orden n y m respectivamente. Sean $s, t \in \mathbb{Z}$ tales que $1 = sm + tn$. Entonces

$$\sigma = \sigma^{mt}\sigma^{ns} \in C_1C_2.$$

Se sigue que

$$C = \langle \sigma \rangle \subset C_1C_2 \subset C$$

y por tanto $C = C_1C_2$. Además si $x \in C_1 \cap C_2$, entonces existen $i, j \in \mathbb{Z}$ tales que $x = \sigma^{mi} = \sigma^{nj}$. Luego $mi \equiv nj \mod (nm)$, lo que como $(m : n) = 1$, implica que $i \in n\mathbb{Z}$ y que $j \in m\mathbb{Z}$ y por tanto $x = 1$. Luego $C \cong C_1 \times C_2$ por el Ejemplo 1.4.11.

Proposición 1.4.13. *Sea $f : G_1 \to G_2$ morfismo de grupos y $S_1 \subset G_1$, $S_2 \subset G_2$ subgrupos.*

i) $T_2 = f^{-1}(S_2) \subset G_1$ es un subgrupo. Más aún si $S_2 \lhd G_2$, entonces $T_2 \lhd G_1$.

ii) $T_1 = f(S_1) \subset G_2$ es subgrupo. Si además $S_1 \lhd G_1$ y f es suryectivo, entonces $T_1 \lhd G_2$.

Demostración. Para la parte i), notemos que como $f(1) = 1$ y $1 \in S_2$, resulta que $1 \in T_1$. Análogamente, usando que $S_2^{-1} = S_2$ y el Ejercicio (1.4.1), obtenemos que T_1 es cerrado por inversas. Si $f(x), f(y) \in S_2$, entonces $S_2 \ni f(x)f(y) = f(xy)$, lo que prueba que $T_2 \cdot T_2 \subset T_2$. Probamos así que T_2 es subgrupo de G_1. Si además $S_2 \lhd G_2$, entonces se sigue del Ejercicio (1.4.6) que $T_2 \lhd G_1$. Esto termina la demostración de la parte i). Veamos ahora la parte ii). Como $f(1) = 1$ y $1 \in S_1$, se sigue que $1 \in T_1$. Usando el Ejercicio 1.4.6, tenemos $f(S_1)^{-1} \subset f(S_1^{-1})$. Usando la definición de morfismo, resulta $f(S_1)f(S_1) \subset f(S_1S_1) \subset f(S_1)$. Además, del Ejercicio 1.4.6, se tiene que si $g \in G_1$, entonces $\mathrm{ad}(f(g))f(S_1) \subset f(\mathrm{ad}(g)(S_1))$. Se sigue que si $S_1 \lhd G_1$ y f es sobre, entonces $T_1 \lhd G_2$. □

Corolario 1.4.14. *Tanto* $\mathrm{Ker}(f) \subset G_1$ *como* $\mathrm{Im}(f) \subset G_2$ *son subgrupos. Siempre* $\mathrm{Ker}(f) \lhd G_1$*; si f es sobre, también* $\mathrm{Im}(f) \lhd G_2$.

Ejemplo 1.4.15. Sea $\mathbb{R}$ el conjunto de los números reales. Consideremos a $\mathbb{R}$ como grupo con la suma. Entonces $\mathrm{Im}(\exp) = S^1$, $\mathrm{Ker}(\exp) = 2\pi\mathbb{Z}$, y $\exp^{-1}(G_\infty) = \mathbb{Q}$.

Ejemplo 1.4.16. Sea X un conjunto y sea

$$S(X) = \{f : X \to X \text{ biyectiva } \}.$$

Notemos que $S(X)$ es un grupo con respecto a la composición de funciones. Si Y es otro conjunto y $\phi : X \to Y$ es una biyección, entonces

$$c_\phi : S(X) \to S(Y), \quad f \mapsto \phi \circ f \circ \phi^{-1}$$

es un isomorfismo con inversa $c_{\phi^{-1}}$. En particular, si $|X| = n \geq 1$, $S(X)$ es isomorfo al *grupo simétrico*

$$\mathbb{S}_n = S(\{1, \dots, n\}).$$

Ejemplo 1.4.17. Sea $f : G_1 \to G_2$ un morfismo de grupos. Si f es mono, entonces $g : G_1 \to \mathrm{Im}(f)$, $g(x) = f(x)$ es un isomorfismo.

Proposición 1.4.18. *(Cayley) Sea G un grupo; entonces la función*

$$L : G \to S(G), \quad L_g(h) = gh$$

es un monomorfismo.

Demostración. Por definición de elemento neutro, tenemos $L_1 = \mathrm{id}$. Además si $g_1, g_2, h \in G$,

$$L_{g_1 g_2}(h) = (g_1 g_2)h = g_1(g_2 h) = (L_{g_1} \circ L_{g_2})(h). \tag{1.4.19}$$

Se sigue que L_g es biyectiva con inversa $L_{g^{-1}}$. En particular $L_g \in S(G)$ y (1.4.19) nos dice que es morfismo. Si $g \in \mathrm{Ker}(L)$, es decir si $L_g = \mathrm{id}$, entonces $1 = L_g(1) = g$. Por tanto L es un monomorfismo. □

Corolario 1.4.20. *Si $|G| = n$ entonces G es isomorfo a un subgrupo de S_n.*

Demostración. Se sigue de la Proposición 1.4.18 usando el Ejemplo 1.4.17. □

Sea G un grupo y sea

$$\mathrm{Aut}(G) = \{f : G \to G \text{ isomorfismo } \}.$$

Observemos que la composición de funciones hace de $\mathrm{Aut}(G)$ un subgrupo de $S(G)$.

Ejemplo 1.4.21. Sea $C = \langle \sigma \rangle$ un grupo cíclico. Si $|C| = \infty$, entonces C tiene exactamente 2 automorfismos, por el Ejemplo 1.4.4, luego $\mathrm{Aut}(C) \cong \mathbb{Z}/2\mathbb{Z}$. Si $|C| = n$, C tiene $\phi(n)$ elementos, que son los endomorfismos F_j del citado ejemplo con $0 < j < n$ coprimo con n.

Ejemplo 1.4.22. Si $g \in G$, la aplicación $L_g : G \to G$ de la Proposición 1.4.18 pertenece a $\mathrm{Aut}(G)$ si y sólo si $g = 1$. Por otro lado $\mathrm{ad}(g) \in \mathrm{Aut}(G)$ para todo $g \in G$.

Proposición 1.4.23. *Sea G un grupo. La función*

$$\mathrm{ad} : G \to \mathrm{Aut}(G), \quad g \mapsto \mathrm{ad}(g)$$

es morfismo de grupos. Su imagen es el subgrupo normal $\mathrm{Inn}(G)$ de automorfismos interiores. Su núcleo es el centro de G.

Demostración. Tenemos que $\mathrm{ad}(1) = \mathrm{id}$ y además

$$\begin{aligned}\mathrm{ad}(g_1g_2)(h) =& g_1(g_2hg_2^{-1})g_1^{-1}\\ =& (\mathrm{ad}(g_1)\circ\mathrm{ad}(g_2))(h).\end{aligned}$$

Por tanto ad es morfismo de grupos. Que su imagen es $\mathrm{Inn}(G)$ es inmediato de la definición de automorfismo interior; que $\mathrm{Inn}(G)$ es un subgrupo se sigue del Corolario 1.4.14. Que $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ es consecuencia de la fórmula del Ejercicio 1.4.6. Veamos que $\mathrm{Ker}(\mathrm{ad}) = Z(G)$. Sea $z \in G$; entonces

$$\begin{aligned}z \in \mathrm{Ker}(\mathrm{ad}) &\iff (\forall g \in G) zgz^{-1} = g\\ &\iff (\forall g \in G) zg = gz\\ &\iff z \in Z(G).\end{aligned}$$

□

Proposición 1.4.24. *Sea $f : G_1 \to G_2$ un morfismo de grupos y sean $K = \mathrm{Ker}(f)$, $I = \mathrm{Im}(f)$. Las siguientes funciones son biyecciones inversas que preservan la normalidad*

$$f : \{K \subset S \subset G_1 : \text{ subgrupo }\} \leftrightarrows \{T \subset I : \text{ subgrupo }\} : f^{-1}.$$

Demostración. Vimos en la Proposición 1.4.13 que las aplicaciones $S \mapsto f(S)$ y $T \mapsto f^{-1}(T)$ mandan subgrupos en subgrupos. También vimos que $f^{-1}(T)$ es normal si T lo es, y que $f(S)$ es normal en G_2 si S lo es y f es suryectivo. Reemplazando f for su correstricción a I, tenemos que $f(S) \lhd I$ toda vez que $S \lhd G_1$. Por otra parte, sabemos que f^{-1} preserva la inclusión de conjuntos; dado que todo subgrupo de G_2 contiene al 1, se sigue que si $T \subset G_2$ es subgrupo, entonces $f^{-1}(G_2) \supset f^{-1}(\{1\}) = \mathrm{Ker}(f)$. Hemos visto entonces que ambas funciones del enunciado están bien definidas y preservan la normalidad. Resta ver que son biyecciones inversas. Es conocido de Álgebra I que $f(f^{-1}(T)) = T$ para todo subconjunto $T \subset I$ y en particular para todo subgrupo. Veamos ahora que si $G \supset S \supset K$ es un subgrupo, entonces $f^{-1}(f(S)) = S$. Es claro que $f^{-1}(f(S)) \supset S$. Para ver la otra inclusión, sea $x \in f^{-1}(f(S))$. Por definición, $f(x) \in f(S)$, luego existe $s \in S$ tal que $f(x) = f(s)$. Usando el Lema 1.4.10 en la igualdad, y la hipótesis de que $S \supset K$ en la segunda inclusión, tenemos

$$x \in f^{-1}(\{s\}) = sK \subset SK \subset S.$$

□

Ejemplo 1.4.25. Vamos a describir todos los subgrupos de $G_n = \{z \in \mathbb{C}^* : z^n = 1\}$. Sea exp el morfismo del Ejercicio 1.2.16. Notemos que $G_n \subset S^1 = \mathrm{Im}(\exp)$ y que

$$\exp^{-1}(G_n) = \{2k\pi/n : k \in \mathbb{Z}\} = \mathbb{Z}(2\pi/n).$$

Sea

$$f : \mathbb{Z} \to G_n, \quad f(k) = \exp(2k\pi/n).$$

Vemos que f es un morfismo suryectivo, con núcleo $n\mathbb{Z}$. Por el Ejemplo 1.2.13 y el Ejercicio 1.2.14, los subgrupos de $\mathbb{Z}$ que contienen a $n\mathbb{Z}$ son exactamente los de la forma $d\mathbb{Z}$ con $d \geq 0$ divisor de n. Usando la Proposición 1.4.24, concluimos que los subgrupos de G_n son exactamente los de la forma $\exp(2d\mathbb{Z}\pi/n)$.

Ejercicio 1.4.26. Probar que todo subgrupo de un grupo cíclico es cíclico.

1.5. Coclases, teorema de Lagrange

Sean G un grupo, $H \subset G$ un subgrupo y $s \in G$. El subconjunto $sH \subset G$ se llama la *coclase a izquierda* de s. Notemos que cada elemento de G está en al menos una coclase; $s \in sH$. Además si $s, t \in G$

$$sH \cap tH = \{x : s^{-1}x, t^{-1}x \in H\}$$

Si $x \in sH \cap tH$, entonces $s^{-1}t = (s^{-1}x)(t^{-1}x)^{-1} \in H$, y por tanto $sH = tH$. Recíprocamente,

$$sH = tH \iff s^{-1}tH = H \iff s^{-1}t \in H. \tag{1.5.1}$$

En conclusión, cada elemento de G está en exactamente una coclase. Por tanto

$$s \sim t \iff sH = tH$$

es una relación de equivalencia, y por (1.5.1), $s \sim t \iff s^{-1}t \in H$. En términos de esta relación, $sH = \{t \in G : s \sim t\}$ es la clase de equivalencia del elemento s. Llamamos *conjunto cociente* G/H al conjunto de todas las coclases a izquierda

$$G/H = \{sH : s \in G\}.$$

La *proyección al cociente módulo* H es la función $\pi : G \to G/H$, $\pi(s) = sH$.

Notación 1.5.2. $|G : H| = |G/H|$

Teorema 1.5.3. *(Lagrange) Sean G un grupo y $H \subset G$ un subgrupo. Entonces existe una biyección $G \to G/H \times H$. En otras palabras, se tiene la identidad*

$$|G| = |G : H||H|.$$

Demostración. Para cada elemento $\xi \in G/H$, elijamos un $s(\xi) \in G$ tal que $\xi = sH$. Por (1.5.1), tenemos $s(gH)^{-1}g \in H$ ($\forall g \in G$). Sean $\phi : G \to G/H \times H$, $\phi(g) = (gH, s(gH)^{-1}g)$ y $\psi : G/H \times H \to G$, $\psi(\xi, h) = s(\xi)h$. Tenemos

$$\phi(\psi(\xi, x)) = \phi(s(\xi)h) = (s(\xi)hH, h) = (\xi, h)$$
$$\psi(\phi(g)) = \psi(gH, s(gH)^{-1}g) = s(gH)s(gH)^{-1}g = g.$$

□

Corolario 1.5.4. *Si $|G| = n < \infty$ entonces el orden de cualquier subgrupo de G divide a n.*

Corolario 1.5.5. *Si $|G| = n$ y $x \in G$, entonces $x^n = 1$.*

Demostración. Por el Corolario anterior, $d = \text{ord}(x) = |\langle x \rangle|$ divide a n. Luego $n = dq$ para algún $q \in Z$, y por tanto $x^n = (x^d)^q = 1$. □

Corolario 1.5.6. *Si $|G| = p$ es primo, entonces $G \cong G_p$.*

Demostración. Si $\sigma \in G \setminus \{1\}$, entonces $|\langle \sigma \rangle| = \text{ord}(\sigma) > 1$ divide a p, y por tanto es igual a p. Luego $G \cong G_p$, por Lema 1.4.8. □

Observación 1.5.7. También pueden considerarse *coclases a derecha* de un grupo G con respecto a un subgrupo H; son los subconjuntos de la forma Hs con $s \in G$. Éstas son las clases de equivalencia de la relación $s \sim' t \iff st^{-1} \in H$. El conjunto de coclases a derecha suele denotarse $H\backslash G$. Notemos que $sH = (sHs^{-1}s)$; por tanto si $H \lhd G$, $sH = Hs$ y $G/H = H\backslash G$.

Ejercicio 1.5.8. Sean $H \subset G$ un subgrupo y $s, t \in G$. Probar que $sH = Ht$ si, y sólo si se satisfacen las siguientes tres condiciones: $s^{-1}Hs = H$, $tHt^{-1} = H$ y $sH = tH$.

Ejercicio 1.5.9. Sea G un grupo y sea G^{op} el cojunto G equipado con la siguiente operación

$$x \cdot_{\text{op}} y = yx.$$

i) Probar que G^{op} es un grupo y que $G \to G^{\text{op}}$, $g \mapsto g^{-1}$ es un isomorfismo.

ii) Sea $H \subset G$ un subgrupo. Probar que hay una biyección $G \xrightarrow{\sim} H \times H\backslash G$. (Sug.: aplicar el teorema de Lagrange para G^{op}).

1.6. Cocientes

Sean X un conjunto y $\sim$ una relación de equivalencia en X. Recordemos que la *clase de equivalencia* de un elemento $x \in x$ es $C_x = \{y \in X : y \sim x\}$. Sea $X/\sim$ el conjunto formado por todas las clases de equivalencia con respecto a $\sim$. La *proyección al cociente* es la función

$$\pi : X \to X/\sim, \quad \pi(x) = C_x. \tag{1.6.1}$$

Proposición 1.6.2. *Sean X un conjunto, $\sim$ una relación de equivalencia en X y $f : X \to Y$ una función. Supongamos que f satisface*

$$x_1 \sim x_2 \Rightarrow f(x_1) = f(x_2). \tag{1.6.3}$$

Entonces existe una única función $\bar{f} : X/\sim \to Y$ tal que $\bar{f} \circ \pi = f$. Se tiene $\text{Im}(\bar{f}) = \text{Im}(f)$. Si además f satisface

$$f(x_1) = f(x_2) \Rightarrow x_1 \sim x_2 \tag{1.6.4}$$

entonces $\bar{f}$ es inyectiva. En particular si f es suryectiva y satisface (1.6.4), $\bar{f}$ es biyectiva.

Demostración. La condición $\bar{f} \circ \pi = f$ equivale a que, para cada $x \in X$,

$$\bar{f}(C_x) = f(x). \tag{1.6.5}$$

Hay que ver (1.6.5) define una función, es decir que $C_x = C_y$ implica $f(x) = f(y)$. Pero esta es precisamente nuestra hipótesis (1.6.3). Notemos además que (1.6.5) nos dice que $\text{Im}(\bar{f}) = \text{Im}(f)$. Si f satisface (1.6.4), entonces $f(x) = f(y) \Rightarrow C_x = C_y$, por tanto $\bar{f}$ es inyectiva. □

Observación 1.6.6. Se sigue de la Proposición 1.6.7 que si $f : X \to Y$ es suryectiva y satisface simultáneamente (1.6.3) y (1.6.4), entonces hay una única biyección $\bar{f} : X/\sim \xrightarrow{\sim} Y$ tal que $f = \bar{f} \circ \pi$. Dado que esta biyección está completamente determinada por las propiedades anteriores, decimos que es *canónica*. Por esta razón diremos que f tiene la *propiedad universal del cociente de X por $\sim$* e identificaremos a Y con $X/\sim$ y a f con π.

En la sección anterior, definimos el cociente de un grupo G por un subgrupo H como el conjunto de clases de equivalencia de la relación $s \sim t \iff s^{-1}t \in H$, y definimos $\pi : G \to G/H$ como la proyección al cociente por esa relación. Aplicando la proposición anterior en este caso se obtiene lo siguiente.

Corolario 1.6.7. *Sean G un grupo, $H \subset G$ un subgrupo y $f : G \to Y$ una función. Supongamos que f satisface*

$$x_1^{-1}x_2 \in H \Rightarrow f(x_1) = f(x_2).$$

Entonces existe una única función $\bar{f} : G/H \to Y$ tal que $\bar{f} \circ \pi = f$. Se tiene $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. Si f satisface

$$f(x_1) = f(x_2) \Rightarrow x_1^{-1}x_2 \in H,$$

entonces $\bar{f}$ es inyectiva.

Ejemplo 1.6.8. Sean $n \geq 2$; consideremos el *grupo ortogonal*

$$O_n = \{A \in \mathrm{GL}_n \mathbb{R} : A^t A = I\}$$

y el subgrupo

$$H = \{A \in O_n : A_{i,n} = A_{n,i} = \delta_{i,n}\}.$$

Aquí $\delta_{i,j}$ es 1 si $i = j$ y 0 en otro caso. Sea

$$S^{n-1} = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} x_i^2 = 1\}.$$

Una matriz $A \in M_n\mathbb{R}$ pertenece a O_n si y sólo si sus columnas forman una base ortonormal de $\mathbb{R}^n$. En particular, si $A \in O_n$ cada columna de A está en S^{n-1}. Definimos

$$p : O_n \to S^{n-1}, p(A) = (A_{1,n}, \ldots, A_{n,n}).$$

Veamos que p es suryectiva. Sea $v \in S^{n-1}$; por Gram-Schmidt existen $v_2, \ldots, v_n \in S^{n-1}$ tales que $\mathcal{B} = \{v, v_2 \ldots, v_n\}$ es base ortonormal. La matriz de cambio de base $C = C_{\mathcal{B},E}$ –cuyas columnas son los vectores de $\mathcal{B}$– satisface $p(C) = v$. Veamos ahora que, si $A_1, A_2 \in O_n$,

$$p(A_1) = p(A_2) \iff A_1^{-1}A_2 \in H. \tag{1.6.9}$$

Sean $\mathcal{B}_1$ y $\mathcal{B}_2$ las bases ortonormales formadas por las columnas de A_1 y A_2. Entonces $A_i = C_{\mathcal{B}_1,E}$, y $A_1^{-1}A_2 = C_{\mathcal{B}_2,\mathcal{B}_1}$. Que $p(A_1) = p(A_2)$ significa que $\mathcal{B}_1$ y $\mathcal{B}_2$ comparten el último vector, y por tanto la última columna de $C = C_{\mathcal{B}_2,\mathcal{B}_1}$ es e_n, el último vector de la base canónica. O sea $C = [C'|e_n]$. Como además C es ortogonal, tenemos

$$I = C^t C = \begin{bmatrix} (C')^t \\ e_n \end{bmatrix} \begin{bmatrix} C' & e_n \end{bmatrix}$$

Igualando el i-ésimo coeficiente de la última fila de la matriz identidad con el del producto de la derecha, obtenemos

$$\delta_{i,n} = C_{i,n}.$$

Llegamos así a que C es de la forma

$$C = \begin{bmatrix} C'' & 0 \\ 0 & 1 \end{bmatrix}$$

En otras palabras, $C \in H$, lo que prueba (1.6.9). En conclusión, $p : O_n \to S^{n-1}$ tiene la propiedad universal del cociente O_n/H.

Sean G un grupo, $H \lhd G$ y $s, t \in G$. Entonces

$$sHtH = st(t^{-1}Ht)H = stH.$$

Esto nos dice que el producto de dos coclases da una coclase, que el conjunto G/H, equipado con el producto de coclases es un grupo y que la proyección al cociente es un morfismo con respecto a esta estructura. Más aún, tenemos lo siguiente.

Teorema 1.6.10. *Sean G un grupo, $K \lhd G$ y $f : G \to H$ un morfismo de grupos.*

i) Si $\mathrm{Ker}(f) \supset K$, entonces existe un único morfismo de grupos $\bar{f} : G/K \to H$ tal que $\bar{f}\pi = f$.

ii) $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.

Demostración. Por el Corolario 1.6.7, en la situación de i), existe una única función $\bar{f}$ que satisface la condición $\bar{f} \circ \pi = f$. Veamos que $\bar{f}$ es morfismo. Tenemos $\bar{f}(H) = \bar{f}(\pi(1)) = f(1) = 1$, y si $s, t \in G$,

$$\bar{f}(stH) = \bar{f}(\pi(st)) = f(st) = f(s)f(t) = \bar{f}(sH)\bar{f}(tH).$$

Hemos probado la parte i). Para la parte ii), aplicamos el Corolario 1.6.7 para el subgrupo $\mathrm{Ker}(f)$ y para $Y = H$, y obtenemos que $\bar{f}$ es inyectiva y por tanto define una biyección $G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$. Por la parte i), esta biyección es un isomorfismo. □

Ejemplos 1.6.11.

i) Todo grupo cíclico de n elementos es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. En efecto, sea $G = \langle\sigma\rangle$ con $|G| = n$. Sea $f : \mathbb{Z} \to G$, $f(m) = \sigma^m$. Entonces f es suryectiva con $\mathrm{Ker}(f) = n\mathbb{Z}$, luego $G \cong \mathbb{Z}/nZ$, por el Teorema 1.6.10.

ii) $\mathbb{R}/\mathbb{Z} \cong S^1$. Sea $f : \mathbb{R} \to S^1$, $f(\theta) = e^{i2\pi\theta}$; f es un morfismo suryectivo con núcleo $\mathbb{Z}$.

iii) $\mathbb{Q}/\mathbb{Z} \cong G_\infty$. Sea f el morfismo de ii). Tenemos $\mathbb{Q} \supset \mathbb{Z}$ y $f(\mathbb{Q}) = G_\infty$. Luego la restricción de f a $\mathbb{Q}$ es un morfismo con imagen G_∞ y núcleo $\mathbb{Z}$.

iv) Sea $SO_n \subset O_n$ el subgrupo de las matrices ortogonales de determinante 1. Entonces $O_n/SO_n \cong \mathbb{Z}/2\mathbb{Z}$. En efecto la función determinante $\det : O_n \to \{\pm 1\}$ es un morfismo suryectivo con núcleo SO_n cuya imagen es un grupo cíclico de orden 2.

Ejercicio 1.6.12. Sea $\mathbb{R}_{>0}$ el conjunto de los reales positivos equipado con el producto. Probar que $\mathbb{C}^*/\mathbb{R}_{>0} \cong S^1$.

Ejercicio 1.6.13. Sea $n \geq 2$; si $x \in \mathbb{Z}$, escribimos $\bar{x}$ por la clase de x módulo n. Sea

$$\mathcal{U}_n = \{\bar{j} \in \mathbb{Z}/n\mathbb{Z} : (x : n) = 1\}.$$

i) Probar que $\mathcal{U}_n$, equipado con la operación $\overline{jk} = \bar{j}\bar{k}$ es un grupo abeliano.

ii) Usar los Ejemplos 1.4.4 y 1.4.21 para probar que $\mathcal{U}_n \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

iii) Probar que si p es primo entonces $\mathcal{U}_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Ejemplo 1.6.14. Sean G un grupo y $K \subset Z(G)$ un subgrupo. Notemos que $K \lhd G$; veremos que si G/K es cíclico, entonces G es abeliano. Sea $\pi : G \to G/K$ la proyección al cociente y sean $\sigma \in G$ tal que $\pi(\sigma)$ genera G/K y $H = \langle\sigma\rangle$. Sea $x \in G$ y sea i tal que $\pi(x) = \pi(\sigma)^i$. Entonces $x\sigma^{-i} \in K$, y por tanto $x \in KH$. Luego $G = KH$, con K y H abelianos tales que $kh = hk$ para todo $k \in K$ y $h \in H$. Por tanto G es abeliano.

Teorema 1.6.15. *Sean G un grupo y $S, K \subset G$ subgrupos tales que S normaliza a K. Hay un isomorfismo canónico*

$$SK/K \cong S/S \cap K.$$

Demostración. Sean $H = SK$ y $\pi : H \to H/K$ la proyección al cociente. Si $x \in H$, $\pi(x) \in \pi(S)$ si y sólo si existe $s \in S$ tal que $\pi(x) = \pi(s)$, lo que equivale a que $s^-1x \in K$, o lo que es lo mismo, a que $x \in sK$. Hemos probado que $\pi^{-1}(\pi(S)) = SK$. Luego π es un morfismo con imagen $\pi(S)$ y núcleo K. Luego $SK/K \cong \pi(S)$, por el Teorema 1.6.10. Por otro lado, la restricción de π a S es un morfismo con imagen $\pi(S)$ y núcleo $S \cap K$ lo que, nuevamente por el Teorema 1.6.10, nos dice que $S/S \cap K \cong \pi(S)$. □

Ejemplo 1.6.16. Sean S y K como en el Teorema 1.6.15 y supongamos que $S \cap K = 1$; en este caso KS es el producto semidirecto que definimos en la Sección 1.3. Por el teorema, tenemos

$$SK/K = S.$$

Luego hay un morfismo suryectivo $p : SK \to S$ con núcleo K, de modo que en la siguiente sucesión, la imagen de cada morfismo es igual al núcleo del morfismo siguiente

$$1 \to K \to SK \xrightarrow{p} S \to 1. \tag{1.6.17}$$

Decimos entonces que (1.6.17) es una sucesión exacta. Sea $\iota : S \to SK$ la inclusión; tenemos $p \circ \iota = \mathrm{id}_S$. Por esta razón decimos que p es una *retracción* con *sección* ι, o que ι *parte* a la sucesión (1.6.17). Recíprocamente, si

$$1 \to K \to H \xrightarrow{q} S \to 1$$

es exacta partida por un morfismo $j : S \to H$, entonces K es normal en H, por ser el núcleo del morfismo p y $j(S) \subset H$ es subgrupo, al ser la imagen de un morfismo. Además, si $x \in K \cap j(S)$

$$x = j(s) \text{ y } 1 = p(x) = p(j(s)) = s \Rightarrow x = 1.$$

Por tanto $K \cap j(S) = 1$. Además si $x \in H$,

$$p(xj(p(x))^{-1}) = p(x)p(x)^{-1} = 1,$$

luego $k := xp(x)^{-1} \in K$, y $x = kj(p(x)) \in KS$. Hemos probado entonces que $H = Kj(S)$ y que $K \cap j(S) = 1$, o sea que H es el producto semidirecto de $j(S)$ y K.

Observación 1.6.18. Sean K y S como en el Ejemplo 1.6.16 y supongamos que $sk = ks$ para todo $s \in S$ y $k \in K$. Entonces $f : K \times S \to KS$, $f(k,s) = ks$ es morfismo y es claramente suryectivo. Además $ks = 1 \iff k = s^{-1} \in K \cap S = 1$, por tanto f es un isomorfismo. Luego $KS \cong K \times S$.

Ejemplo 1.6.19. (Grupos de orden p^2). Sean $p > 0$ primo y G un grupo de orden p^2. Veremos que G es abeliano, e isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ o a $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Por el Corolario 1.7.12, $Z(G) \neq 1$, luego si $1 \neq Z(G) \neq G$, por Lagrange debería ser $|G/ZG| = p$, luego $G/Z(G)$ sería cíclico, lo que es absurdo por el Ejemplo 1.6.14. Por tanto G es abeliano. Si posee un elemento de orden p^2, es cíclico, isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ por el Ejemplo 1.6.11 i). Si no, todo elemento no trivial tiene orden p. Sean x un tal elemento, $K = \langle x \rangle$ y $\pi : G \to G/K$ la proyección al cociente. Sea $y \in G$ tal que $\pi(y)$ genere G/K. Entonces tanto y como $\pi(y)$ tienen orden p. Luego $\pi(y^i) = \pi(y)^i = 1 \iff p \backslash i \iff y^i = 1$. Se sigue que la restricción de π a $H = \langle y \rangle$ es inyectiva, es decir, $K \cap H = 1$. Luego $KH/K \cong H$, como vimos en 1.6.16. Por Lagrange, $|KH| = p^2$, luego $G = KH$ y por la Observación 1.6.18, $G \cong K \oplus H \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Teorema 1.6.20. *Sean G un grupo y $H \subset K$ subgrupos normales de G. Entonces K/H es un subgrupo normal de G/H y hay un isomorfismo canónico*

$$(G/H)/(K/H) \cong G/K.$$

Demostración. La proyección al cociente $\pi_K : G \to G/K$ tiene núcleo $K \subset H$. Luego en virtud del Teorema 1.6.10, existe un único morfismo $p : G/H \to G/K$ tal que

$$p\pi_H = \pi_K \tag{1.6.21}$$

y más aún, p es suryectivo. Aplicando de nuevo el Teorema 1.6.10, tenemos que $G/K = (G/H)/\mathrm{Ker}(p)$. Por otro lado, (1.6.21) nos dice que $(\pi_H)^{-1}(\mathrm{Ker}(p)) = K$. Como π_H es suryectiva, concluimos que $\mathrm{Ker}(p) = \pi_H(K) = H/K$. □

Ejemplo 1.6.22. Sean $C = \langle \sigma \rangle$ un grupo cíclico de orden n, d un divisor de n y $D = \langle \sigma^d \rangle$. Entonces el morfismo $p : \mathbb{Z} \to C$ $m \mapsto \sigma^m$ es suryectivo con núcleo $n\mathbb{Z}$. La preimagen de H es $p^{-1}(H) = d\mathbb{Z}$. Luego

$$C/D \cong (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}.$$

1.7. Acciones de gupos

Sean X un conjunto y G un grupo. Una *acción* de G en X es un morfismo de grupos

$$\rho : G \to S(X).$$

Dada una acción ρ, tenemos una aplicación

$$\cdot : G \times X \to X, \quad (g, x) \mapsto g \cdot x := \rho(g)(x).$$

Observamos que $\cdot$ tiene las siguientes propiedades

$$1 \cdot x = x, \quad (gh) \cdot x = g \cdot (h \cdot x) \qquad \forall g, h \in G, x \in X. \tag{1.7.1}$$

Recíprocamente, si tenemos una función $\cdot : G \times X \to X$ con las propiedades de arriba, entonces para cada $g \in G$, la aplicación $\rho(g) : X \to X$, $\rho(g)(x) = g \cdot x$ es una biyección con inversa $\rho(g^{-1})$, y $\rho : G \to S(X)$, $g \mapsto \rho(g)$ es morfismo de grupos.

En conclusión, dar una acción de G en X equivale a dar una función $\cdot : G \times X \to X$ que satisface (1.7.1).

Notación 1.7.2. Para decir que el grupo G actúa en el conjunto X, escribiremos $G \curvearrowright X$. La acción de un elemento $g \in G$ en un elemento $x \in X$ se denotará $g \cdot x$, o simplemente gx. Un conjunto X equipado con una acción de G se llama un *G-conjunto*. Un *morfismo* entre dos G-conjuntos X e Y es una función $f : X \to Y$ tal que $f(gx) = gf(x)$ $\forall g \in G, x \in X$. Un morfismo de G-conjuntos es un isomorfismo si es biyectivo. En este caso su inversa también es morfismo de G-conjuntos. Los morfismos de G-conjuntos son llamados también funciones *G-equivariantes*.

Ejemplos 1.7.3.

- En virtud del Ejemplo 1.4.2, dar una acción de $\mathbb{Z}$ en un conjunto X es lo mismo que dar un elemento $\sigma \in S(X)$.
- $S(X)$ actúa en X mediante $\sigma \cdot x = \sigma(x)$.
- Si $G \curvearrowright X$ y $H \subset G$, entonces $H \curvearrowright X$ por restricción de la acción. Así, por ejemplo, si k es un cuerpo, el subgrupo $\mathrm{GL}_n(k) \subset S(k^n)$ actúa en k^n.
- Un grupo G actúa en sí mismo por multiplicación a izquierda; el correspondiente morfismo $G \to S(G)$ es el morfismo L del Teorema de Cayley 1.4.18. Esta acción se suele llamar *acción por traslación* a izquierda. Más en general, si $H \subset G$ es un subgrupo, y $g, s \in G$, entonces $L_g(sH) = L_g(s)H$, luego G actúa también en G/H por traslación a izquierda.
- También podemos hacer actuar a G en sí mismo por conjugación; el morfismo $G \to S(G)$ resultante es la composición del morfismo ad de la Proposición 1.4.23 con la inclusión $\mathrm{Aut}(G) \subset S(G)$.

Sean X e Y conjuntos equipados con acciones de un mismo grupo G. Una función $f : X \to Y$ se dice *equivariante* si $f(g \cdot x) = g \cdot f(x)$ $\forall x \in X$. Sea $x \in X$; el *estabilizador* de x es

$$G_x = \{g \in G : g \cdot x = x\}.$$

La *órbita* de x es

$$\mathcal{O}_x = G \cdot x = \{g \cdot x : g \in G\}$$

Proposición 1.7.4. *Sea $G \curvearrowright X$ una acción y sea $x \in X$. Entonces*

i) G_x es un subgrupo de G.

ii) Hay un isomorfismo de G-conjuntos

$$G/G_x \cong \mathcal{O}_x.$$

En particular, $|O_x| = |G : G_x|$.

iii) Si $s \in X$, $G_{s\cdot x} = sG_xs^{-1}$.

Demostración. i) Por (1.7.1), $1 \in G_x$ y $G_xG_x = G_x$.

ii) Sea $p : G \to \mathcal{O}_x$, $p(g) = g \cdot x$. Por definición de $\mathcal{O}_x$, p es suryectiva. Además, si $g, h \in G$, entonces usando (1.7.1) en el segundo paso, tenemos

$$p(g) = p(h) \iff g \cdot x = h \cdot x \iff x = g^{-1}h \cdot x \iff g^{-1}h \in H.$$

La afirmación ii) se sigue ahora de la Proposición 1.6.2.

iii) Sea $g \in G$. Entonces, usando (1.7.1) en el segundo paso,

$$g \in G_{sx} \iff g \cdot (s \cdot x) = s \cdot x \iff (s^{-1}gs) \cdot x = x \iff g \in sG_xs^{-1}.$$

□

Sea $G \curvearrowright X$ una acción. Decimos que la acción es *fiel* si $\mathrm{Ker}(\rho) = 1$, que es *libre* si $G_x = 1$ $\forall x \in X$. La siguiente identidad explica la relación entre fidelidad y libertad:

$$\mathrm{Ker}(\rho) = \bigcap_{x \in X} G_x.$$

Decimos que la acción es *transitiva* si $X = \mathcal{O}_x$ para algún (y luego para todo) $x \in X$. Por la Proposición 1.7.4, G actúa transitivamente en X si y sólo si X es equivariantemente isomorfo a un cociente G/H por algún subgrupo $H \subset G$. Más aún, si $s \in G$, entonces $G/H \cong G/sHs^{-1}$ como G-conjuntos.

Ejercicio 1.7.5. Sean G un grupo, $H \subset G$ un subgrupo y $s \in G$. Dar explícitamente una biyección $G/H \to G/sHs^{-1}$ que sea equivariante con respecto a la acción por traslación a izquierda.

Ejemplo 1.7.6. Sean G un grupo, $H, K \subset G$ subgrupos y dejemos actuar a K en G/H por traslación a izquierda. La órbita de un elemento $x \in G$ es $\mathcal{O}_{xH} = \{kxH : k \in K\}$. El estabilizador de xH es

$$K_{xH} = \{k \in K : kxH = xH\} = \{k \in K : x^{-1}kxH = H\} = K \cap xHx^{-1}.$$

Luego

$$|\mathcal{O}_{xH}| = |K|/|K \cap xHx^{-1}|.$$

Por otra parte, cada uno de los elementos de $\mathcal{O}_{xH}$ es una coclase a izquierda yH, cada una de las cuales tiene $|H|$ elementos. Hay $|\mathcal{O}_{xH}|$ de tales coclases, y su unión disjunta es el subconjunto $KxH \subset G$. Tenemos entonces

$$|KxH| = |\mathcal{O}_{xH}||H| = |K||H|/|K \cap xHx^{-1}| = |H||K : K \cap xHx^{-1}|$$

Sean X un G-conjunto y $x, y \in X$. Entonces

$$\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset \iff (\exists g, h \in G) g \cdot x = h \cdot y \iff (\exists s \in G) s \cdot x = y \iff \mathcal{O}_x = \mathcal{O}_y$$

Luego cada elemento de X está en exactamente una órbita, y por tanto

$$x \sim y \iff \mathcal{O}_x = \mathcal{O}_y$$

es una relación de equivalencia en X. Escribimos $X/G := X/\sim$; por definición, $X/G = \{\mathcal{O}_x : x \in X\}$. Notemos que la acción es transitiva si y sólo si X/G tiene un único elemento.

Ejemplo 1.7.7. La acción de $S(X)$ en X de 1.7.3 i) es fiel y transitiva. Es libre si y sólo si X tiene a lo sumo 2 elementos.

Ejemplo 1.7.8. Sea k un cuerpo y $n \geq 1$, y consideremos la acción de $\mathrm{GL}_n(k)$ de 1.7.3 iii). Esta acción es fiel pues se obtiene por restricción de la acción de $S(k^n)$, que es fiel. La órbita del 0 consiste sólo del 0. Por otro lado dado $v \in k^n \setminus \{0\}$, lo podemos completar a una base $B = \{v, v_2 \ldots, v_n\}$, y la matriz $C = C_{B,E}$ satisface $C \cdot e_1 = v$. Esto muestra que $\mathcal{O}_{e_1} = k^n \setminus \{0\}$. Luego $k^n / \mathrm{GL}_n(k)$ tiene exactamente 2 elementos. El estabilizador de 0 es todo $\mathrm{GL}_n(k)$; el de e_1 es el subgrupo formado por todas las matrices inversibles cuya primera columna es e_1. El de un vector no nulo v cualquiera está formado por todas las matrices inversibles de las cuales v es autovector de autovalor 1.

Ejemplo 1.7.9. En el caso particular $k = \mathbb{R}$, podemos restringir la acción del ejemplo anterior al grupo ortogonal O_n. Nuevamente la acción es fiel por ser la restricción de una acción fiel. Todo vector $v \in S^1$ puede completarse a una base ortonormal; luego $\mathcal{O}_{e_1} = S^1$ por el mismo argumento que en el ejemplo anterior. Se sigue que si $r \in \mathbb{R}_{\geq 0}$ entonces $\mathcal{O}_{re_1} = \{x \in \mathbb{R}^n : |x| = r\}$. La aplicación $\mathcal{O}_x \mapsto |x|$ da una biyección $\mathbb{R}^n/O_n \xrightarrow{\sim} \mathbb{R}_{\geq 0}$.

Ejemplo 1.7.10. Consideremos la acción de G en sí mismo por automorfismos interiores. La Proposición 1.4.23 nos dice que esta acción es fiel si y sólo si $Z(G) = 1$. El estabilizador de un elemento g se llama el *centralizador* de g, y es usual denotarlo Z_g (en lugar de G_g). Por definición

$$Z_g = \{z \in G : zg = gz\}.$$

La órbita de g por esta acción se llama la *clase de conjugación* de g; la denotamos $\mathrm{con}(g)$. Por definición

$$\mathrm{con}(g) = \{sgs^{-1} : s \in G\}.$$

La Proposición 1.7.4 nos dice que $|\mathrm{con}(g)| = |G : Z_g|$. Notemos que $g \in Z(G) \iff |\mathrm{con}(g)| = 1 \iff Z_g = G$.

Teorema 1.7.11. *(Ecuación de clases) Sea G un grupo finito. Existen $n \geq 0$ y subgrupos $S_1, \ldots S_n \subsetneq G$ tales que*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : S_i|.$$

Demostración. Consideremos la acción de G en G por conjugación. Descompongamos a G como la unión disjunta de las órbitas con respecto a esta acción. Notemos que $|G|$ es la suma de los cardinales de esas órbitas. Como observamos en el ejemplo anterior, hay tantas órbitas de cardinal 1 como elementos tiene $Z(G)$. Si $G = \mathbb{Z}(G)$, el teorema es trivial. Si no, sean $\mathcal{O}_1, \ldots, \mathcal{O}_n$ las órbitas de 2 o más elementos y sea, para cada $1 \leq i \leq n$, $g_i \in G$ tal que $\mathcal{O}_i = \text{con}(g_i)$ y $S_i = Z_{g_i}$. Entonces $|\mathcal{O}_i| = |G : S_i|$ y se obtiene la fórmula del teorema. □

Un *p-grupo* es un grupo finito $G \neq 1$ cuyo orden es una potencia de p.

Corolario 1.7.12. *Sean p un número primo y $n \geq 1$. Si G es un p-grupo entonces $|Z(G)| > 1$.*

Demostración. En la ecuación de clases, tanto $|G|$ como cada sumando $|G : S_i|$ es una potencia positiva de p, por Lagrange. Luego $|Z(G)|$ tiene que ser divisible por p; en particular, no puede ser 1. □

Ejercicio 1.7.13. Sean G, H grupos y sea $\phi : G \to \text{Aut}(H)$ un morfismo. Llamamos $H \rtimes_\phi G$ al producto cartesiano $H \times G$ equipado con el siguiente producto

$$(h_1, g_1)(h_2, g_2) = (h_1\phi(g_1)(h_2), g_1g_2)$$

i) Probar que $H \rtimes_\phi G$ es un grupo.

ii) Probar que $G_1 = \{1\} \times G$ es un subgrupo de $H \rtimes_\phi G$ y que $H_1 = H \times \{1\} \lhd H \rtimes_\phi G$.

iii) Probar que $H \rtimes_\phi G$ es el producto semidirecto de H_1 y G_1.

iv Sea

$$1 \to H \to E \to G \to 1$$

una sucesión exacta que se parte. Probar que existe $\phi : G \to \text{Aut}(H)$ tal que $E \cong H \rtimes_\phi G$.

v) Sea C un grupo cíclico y sea $\phi : \mathbb{Z}/2\mathbb{Z} \to \text{Aut}(C)$, $\phi(x) = -x$. Sea $C_\phi = C \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$. Para $\theta \in \mathbb{R}$, sea $D(\theta)$ como en el Ejemplo 1.2.15. Probar que si $\theta/2\pi$ es irracional, entonces $D(\theta) \cong \mathbb{Z}_\phi$, y que si $\theta/2\pi = k/n$ con $k \in \mathbb{Z}$, $n \in \mathbb{N}$ y $(k : n) = 1$, entonces $D(\theta) \cong (\mathbb{Z}/n\mathbb{Z})_\phi$.

Sea G un grupo actuando en un conjunto X. Sea

$$X^G = \{x \in X : g \cdot x = x \quad \forall g \in G\}.$$

Los elementos de X son los *puntos fijos* de la acción. Notemos que

$$x \in X^G \iff G_x = G \iff |G : G_x| = 1.$$

Supongamos que X es finito; entonces X se descompone como unión disjunta de finitas órbitas. Observamos que $|X^G|$ es el número de órbitas de que tienen sólo un elemento. Si la acción no es trivial, $X \setminus X^G \neq \emptyset$, luego hay $n \geq 1$

órbitas $\mathcal{O}_1, \ldots, \mathcal{O}_n$ con $|\mathcal{O}_i| > 1$ para todo i. Elijamos para cada i un elemento $x_i \in \mathcal{O}_i$; sea $G_i = G_{x_i}$ entonces $|\mathcal{O}_i| = |G : G_{x_i}|$. Luego tenemos la identidad

$$|X| = |X^G| + \sum_{i=1}^{n} |G : G_i|. \tag{1.7.14}$$

La ecuación (1.7.14) es la versión general de la ecuación de clases. En efecto en el caso particular en que $X = G$ y G actúa por conjugación, (1.7.14) es precisamente la ecuación del Teorema 1.7.11. El Corolario 1.7.12 es un ejemplo de cómo se aplica el teorema. El próximo lema, que será de utilidad en la sección siguiente, es un ejemplo de aplicación de (1.7.14).

Lema 1.7.15. *Sean $r \geq 1$, G un grupo con $|G| = p^r$ actuando en un conjunto finito X. Entonces $|X| \cong |X^G|$ mód (p). En particular, si $p \nmid |X|$, X tiene un punto fijo por G.*

Demostración. Consideremos la fórmula (1.7.14). Los índices $|G : G_i|$ son > 1 y dividen a p^r; por tanto son divisibles por p. Luego $|X| - |X^G|$ es divisible por p, es decir $|X| \equiv |X^G|$ mód (p). □

Teoremas de Sylow

Lema 1.7.16. *Sea G un grupo abeliano finito. Si $p > 0$ es primo y $p \backslash |G|$, entonces G tiene un elemento de orden p.*

Demostración. Hacemos inducción en $m = |G|/p$. El caso base es $m = 1$; sabemos del Corolario 1.5.6 que un grupo de p elementos es cíclico, luego el lema es cierto en este caso. Vamos al paso inductivo con $m \geq 2$. Sea $G \ni \sigma \neq 1$; si $p \backslash n = \text{ord}(\sigma)$, entonces $\text{ord}(\sigma^{n/p}) = p$ y el lema es cierto. Supongamos entonces que $(n : p) = 1$. Por hipótesis inductiva, $H = G/\langle\sigma\rangle$ posee un elemento $\bar{\tau}$ de orden p. Sea $\pi : G \to H$ la proyección y sea $\tau \in G$ tal que $\pi(\tau) = \bar{\tau}$. Consideremos el elemento $x = \tau^n$. Tenemos $\pi(x) = \bar{\tau}^n \neq 1$ pues $(p : n) = 1$. En particular, $x \neq 1$. Por otro lado $\pi(\tau^p) = \bar{\tau}^p = 1$, luego $\tau^p \in \langle\sigma\rangle$, y por tanto $x^p = (\tau^p)^n = 1$. □

Proposición 1.7.17. *Sean $p > 0$ primo, $r \geq 1$ y G un grupo de orden p^r. Entonces G posee un subgrupo de orden p^s para cada $0 \leq s \leq r$.*

Demostración. El caso $s = 0$ de la proposición es trivial. Para probar el caso $s \geq 1$, hacemos inducción en r. Si $r = 1$, $|G| = p$ y no hay nada que probar. Sea $r \geq 2$ $|G| = p^r$, y supongamos la proposición cierta para p-grupos de orden menor a p^r. Por el Corolario 1.7.12, $p \backslash |Z(G)|$. Por el Lema 1.7.16, $Z(G)$ tiene un elemento σ de orden p. En particular se cumple el caso $s = 1$ de la proposición. Además $K = \langle\sigma\rangle \lhd G$ y $|G/K| = p^{r-1}$. Por hipótesis inductiva, para cada $r \geq s \geq 2$, hay un subgrupo $T_s \subset G/K$ de orden p^{s-1}; sea $H_s \subset G$ su preimagen por la proyección al cociente. Por Lagrange, $|H_s| = p^s$. □

Sean G un grupo finito, $p > 0$ un primo que divide a $|G|$ y r la mayor potencia de p que lo divide, de modo que $|G| = p^r m$ con $(p : m) = 1$. Un *p-subgrupo de Sylow* de G es un subgrupo de orden p^r.

Teorema 1.7.18. *(Primer teorema de Sylow) Sean $p > 0$ primo, $r \geq 1$, G un grupo de orden $|G| = p^r m$ con $(p : m) = 1$. Entonces G tiene un p-subgrupo de Sylow.*

Demostración. Supongamos primero que $p \backslash |Z(G)|$. Por el Lema 1.7.16, $Z(G)$ tiene un subgrupo C de orden p. Si además $r = 1$, listo. Supongamos que $r \geq 2$ y que el teorema es cierto para todo grupo H con $p \backslash |Z(H)|$ y $|H| = p^{r-1}m$. Entonces $H = G/C$ posee un subgrupo T de orden p^{r-1} y su preimagen por la proyección es un subgrupo $S \subset G$ de orden p^r.

Vayamos ahora al caso general. Hacemos inducción en $|G|$. El caso base $|G| = p$ ya fue considerado antes. Supongamos entonces que $|G| > p$ y que p no divide a $|Z(G)|$. Por la ecuación de clases (Teorema 1.7.11), existen subgrupos $S_1, \ldots, S_n \subsetneq G$ tales que

$$p^r m = |G| = |Z(G)| + \sum_{i=1}^{n} |G : S_i|.$$

Dado que p divide al lado izquierdo y no divide al primer sumando del lado derecho, no puede dividir a todos los demás sumandos. Debe entonces existir $1 \leq i \leq n$ tal que $p \not\backslash |G : S_i|$. Por Lagrange, $|S_i| = p^r m'$ con $m' < m$. Por hipótesis inductiva, S_i posee un subgrupo T de orden p^r. Este subgrupo es también subgrupo de G, y cumple lo pedido. □

Sean G un grupo y $S \subset G$ un subgrupo. El *normalizador* de S en G es

$$N_G(S) = \{g \in G : gSg^{-1} = S\}.$$

Notemos que $N_G(S)$ es un subgrupo de G; precisamente es el estabilizador de S para la acción de G por conjugación en el conjunto de todos los subgrupos de G. Observemos además que $S \lhd N_G(S)$ y que $N_G(S)$ es el subgrupo más grande de G con esa propiedad.

Teorema 1.7.19. *Sean G y p como en el Teorema 1.7.18 y sean S y T p-subgrupos de Sylow de G. Entonces existe $g \in G$ tal que $gTg^{-1} = S$.*

Demostración. Sea $X = \{gTg^{-1} : g \in G\}$; G actúa en X con una sola órbita, la órbita de T. Luego $|X| = |G : G_T|$, donde

$$G_T = \{g \in G : gTg^{-1}\} = N_G(T) \supset T.$$

Luego con la notación del Teorema 1.7.18, $|G : G_T| \backslash |G|/|T| = m$. En particular, $p \not\backslash |X|$. Aplicamos entonces el Lema 1.7.15 a la acción de S en X por conjugación y obtenemos que existe $g \in G$ tal que el subgrupo $T' = gTg^{-1}$ cumple que para todo $s \in S$, $\mathrm{ad}(s)(T') = T'$. En otras palabras, S normaliza T'. Por tanto $T'S$ es un subgrupo de G. Por Lagrange y el Teorema 1.6.15, $|T'S| = |S||T'|/|S \cap T'|$. Luego $T'S$ es un p-subgrupo de G que contiene a S, que es un p-subgrupo maximal, ya que $|G|/|S| = m$ no es divisible por p. Se sigue que $T'S = S$ y por tanto $T' \subset S$. Pero T' también es maximal, al ser conjugado de T; luego $S = T' = gTg^{-1}$. □

Notación 1.7.20. Sean p y G como en el Teorema 1.7.19. Escribimos

$$r_p(G) = \{S \subset G : S \text{ } p\text{-subgrupo de Sylow }\}.$$

Corolario 1.7.21. *Sean G, p, r y m como en el Teorema 1.7.18. Entonces $r_p(G) \backslash m$.*

Demostración. Por el Teorema 1.7.18, G tiene un p-subgrupo de Sylow S. Por el Teorema 1.7.19, el conjunto de todos los p-subgrupos de Sylow coincide con la órbita de S en la acción de G por conjugación. Luego $r_p(G) = [G : N_G(S)]$. Como $N_G(S) \supset S$, tenemos $[N_G : S] \backslash m$. □

Teorema 1.7.22. *Con la Notación 1.7.20, tenemos* $r_p(G) \equiv 1 \mod (p)$.

Demostración. Sea X el conjunto de todos los p-subgrupos de Sylow de G y sea $S \in X$. Hagamos actuar a S en X por conjugación; S es un punto fijo de esta acción. Más aún, es el único punto fijo, pues si T es fijado por S entonces $S \subset N_G(T) \supset T$ y procediendo como en la demostración del Teorema 1.7.19, llegamos a que $S = T$. Hemos probado que $|X^S| = 1$; por el Lema 1.7.15, esto implica que $r_p(G) = |X| \equiv 1 \mod (p)$. □

Un grupo G se dice *simple* si tiene exactamente 2 subgrupos normales, 1 y G.

Ejemplo 1.7.23. Un grupo abeliano finito G es simple $\iff n = |G|$ es primo. En efecto, si no lo es, hay $p > 0$ primo que divide a n estrictamente. Por Lema 1.7.16, G tiene un subgrupo propio de orden p, que es normal pues G es abeliano. La clasificación de los grupos finitos simples no abelianos es mucho más compleja ([6]).

Ejemplo 1.7.24. Veamos que no hay grupos simples de orden 20. Escribimos $20 = 2^2 \cdot 5$. Sea G un grupo de 20 elementos. Por el Corolario 1.7.21, $r = r_5(G) \backslash 4$ y por el Teorema 1.7.19, $r \equiv 1 \mod (5)$. Luego $r = 1$, es decir, G tiene un solo 5-subgrupo de Sylow S. Por el Teorema 1.7.19, $S \lhd G$.

Ejemplo 1.7.25. Sea G un grupo con $|G| = 30$. Veamos que G no puede ser simple. Factorizamos $30 = 2 \cdot 3 \cdot 5$. Aplicando como antes el Corolario 1.7.21 y el Teorema 1.7.22, vemos que $r_5 = r_5(G) \in \{1, 6\}$. Si $r_5 = 1$, G no es simple, por el Teorema 1.7.19. Supongamos entonces que $r_5 = 6$. Entonces G tiene 6 subgrupos de orden 5. Por el Ejemplo 1.7.23, cada uno de ellos es simple, y por tanto 1 es el único elemento que dos distintos pueden compartir. Así, la unión de todos los subgrupos de orden 5 de G tiene $1 + 4 \times 6 = 25$ elementos, uno de ellos de orden 1 y los 24 restantes de orden 5. Por otro lado, cada 3-subgrupo de Sylow aporta 2 nuevos elementos de orden 3, lo cual como antes implica que G tiene $2r_3$ elementos de ese orden, que no pueden ser ninguno de los 24 de orden 5, lo que nos da una cota $r_3 \leq 2$. Por otro lado, $r_3 \backslash 10$ y $r_3 \equiv 1 \mod (3)$ nos dice que $r_3 \neq 2$, así que $r_3 = 1$ y por tanto G tiene un subgrupo normal de orden 3.

Ejemplo 1.7.26. (Grupos de orden pq) Sean p, q primos con $p < q$. Vamos a utilizar buena parte de lo que vimos hasta ahora para caracterizar los grupos de pq elementos a menos de isomorfismo. Veremos que si $p \not\backslash q - 1$, hay un solo tal grupo, que es abeliano, mientras que si $p \backslash q - 1$ hay exactamente 2, uno abeliano y el otro no. Sea G un grupo con $|G| = pq$. Por el Corolario 1.7.21 y el tercer teorema de Sylow (1.7.22), r_q / p y $r_q \equiv 1 \mod p$, lo que implica que G tiene un subgrupo $K \lhd G$ con $|K| = q$, y por tanto $K = \langle x \rangle$ para algún elemento x con $\text{ord}(x) = q$. Por el primer teorema de Sylow, G tiene además un elemento y de orden p, que genera un subgrupo $S = \langle y \rangle$. Dado que K y S son simples, tenemos $K \cap S = 1$. Por tanto $G = KS$ es el

producto semidirecto de K y S. Además $K \cong \mathbb{Z}/q\mathbb{Z}$, $S \cong \mathbb{Z}/p\mathbb{Z}$, lo que por el Ejercicio 1.7.13 implica que $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ para algún morfismo $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Por el Ejercicio 1.6.13, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathcal{U}_q \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Si ϕ es el morfismo trivial, G es abeliano. Supongamos entonces que G no es abeliano. Entonces $\phi(1)$ es un elemento de orden p, y por tanto $p \backslash q - 1$. Entonces $q = p^r m + 1$ con $r \geq 1$ y $(p : m) = 1$. Como $\mathbb{Z}/(q-1)\mathbb{Z}$ es abeliano y cíclico, tiene un único p-subgrupo de Sylow, y éste es isomorfo a $\mathbb{Z}/p^r\mathbb{Z}$. Por el Lema 1.4.8 y el Ejemplo 1.4.25, $p^{r-1}\mathbb{Z}/p^r\mathbb{Z}$ es el único subgrupo de orden p de $\mathbb{Z}/p^r\mathbb{Z}$. Volviendo atrás por las identificaciones, tenemos que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ tiene un único subgrupo de orden p, y si σ genera este subgrupo, entonces hay exactamente $p-1$ morfismos no triviales $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, $\phi_1, \ldots, \phi_{p-1}$, y están determinados por $\phi_i(\bar{1}) = \sigma^i$. Sea $G_i = \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_i} \mathbb{Z}/p\mathbb{Z}$ con $i = 1, \ldots, p-1$; hemos visto que si $p \backslash q - 1$, cada grupo no abeliano de orden pq es isomorfo a un G_i. Resta ver que $G_1 \cong G_i$ para todo i. Fijo i, sea $j \in \mathbb{Z}$ tal que $ji \cong 1 \mod (p)$. Definimos $\psi : G_1 \to G_i$, $\psi(x, y) = (x, jy)$. Notemos que ψ es biyectiva; su inversa manda $(x, y) \mapsto (x, iy)$. Es claro que $\psi(0, 0) = (0, 0)$. Resta ver que ψ preserva productos. Escribiendo, como es usual, $\bar{k}$ por la clase de un entero k módulo p, tenemos

$$\begin{aligned}
\psi((x, \bar{a}) \cdot_{\phi_1} (y, \bar{b})) &= \psi(x + \sigma^a(y), a \bar{+} b) \\
&= (x + \sigma^a(y), ja \bar{+} b) \\
&= (x + \sigma ija(y), ja \bar{+} jb) \\
&= (x, j\bar{a}) \cdot_{\phi_i} (y, j\bar{b}) \\
&= \psi(x, \bar{a}) \cdot_{\phi_i} \psi(y, \bar{b}).
\end{aligned}$$

Capítulo 2

Anillos

2.1. Anillos y subanillos

Un *anillo* es un conjunto A equipado con dos operaciones. Una operación $+$ que hace de A un grupo abeliano y una operación $\cdot$ que hace de A un monoide, de forma que se cumplen las siguientes identidades para todo $a, b, c \in A$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Estas identidades nos dicen que el producto es *distributivo* con respecto a la suma. Decimos que A es *conmutativo* si $\cdot$ lo es.

Notación 2.1.1. Llamamos 0 al neutro de $+$ y 1 al de $\cdot$ y escribiremos $-a$ por el inverso de un elemento $a \in A$ con respecto a $+$. El elemento 1 es la *unidad* de A. A menudo omitiremos el símbolo $\cdot$ y escribiremos ab por $a \cdot b$. Escribimos $(A, +)$ y $(A, \cdot)$ para referirnos a A pensado sólo como grupo o sólo como monoide con respecto a $+$ y a $\cdot$.

Ejercicio 2.1.2. Sea A un anillo; para $a \in A$ escribimos $L_a, R_a : A \to A$, $L_a(x) = a \cdot x$ y $R_a(x) = x \cdot a$. Probar $\forall a \in A$:

i) $0 \cdot a = a \cdot 0 = 0$.

ii) $(-1) \cdot a = -a$.

iii) L_a y R_a son endomorfismos del grupo $(A, +)$.

Decimos que un elemento $a \in A \setminus \{0\}$ es *divisor de cero a izquierda* si L_a no es inyectiva y que es *divisor de cero a derecha* si A_a no lo es; a es *divisor de cero* si lo es a alguno de los dos lados. Un elemento $a \in A$ es *inversible a izquierda* si $1 \in \mathrm{Im}(R_a)$ y es *inversible a derecha* si $1 \in \mathrm{Im}(L_a)$. Un elemento es *inversible* si lo es a ambos lados. Escribimos $A^* = \mathrm{inv}(A, \cdot)$ por el conjunto de elementos inversibles de A.

Observación 2.1.3. (Anillo 0). El conjunto $\{0\}$ con la única operación que tiene como suma y como producto, es un anillo conmutativo, sin divisores de 0 y en

el cual su único elemento es inversible. Esta última propiedad lo caracteriza; si A es un anillo donde 0 tiene inversa a derecha x, entonces para todo $a \in A$

$$a = a \cdot 1 = a \cdot (0 \cdot x) = (a \cdot 0) \cdot x = 0 \cdot x = 0.$$

Cambiando el orden de los factores obtenemos también que si 0 tiene inversa a izquierda en A, entonces $A = \{0\}$. En concordancia con la notación que usamos para grupos, llamaremos 0 al anillo $\{0\}$.

Decimos que un anillo $A \neq 0$ es un *dominio* si no posee divisores de cero (a ninguno de los lados) y que A es *de división* si $A^* = A \setminus \{0\}$. Un *cuerpo* es un anillo de división conmutativo.

Un *subanillo* de un anillo A es un subgrupo $S \subset A$ tal que $1 \in S$ y $S \cdot S \subset S$. En otras palabras S es a la vez subgrupo de $(A, +)$ y submonoide de $(A, \cdot)$.

Ejemplos 2.1.4. He aquí algunos ejemplos de anillos.

- Algunos anillos que conocemos de Álgebra I son: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$; todos son dominios conmutativos; los últimos tres son cuerpos. Cada uno de ellos es subanillo del siguiente.

- Si A es un anillo (e.g. uno de los anteriores), el conjunto $M_n A$ de todas las matrices de $n \times n$ con coeficientes en A, con la suma y el producto que ya conocemos, es de nuevo un anillo.

- El conjunto $A[x]$ de polinomios en una variable con coeficientes en A, equipado con la suma y el producto habituales, es un anillo. Aclaramos aquí que en $A[x]$, la variable x conmuta con los elementos de A, sea éste conmutativo o no. Si k es un cuerpo y $\mathbb{V}$ es un k-espacio vectorial, entonces el conjunto $\mathrm{End}_k(\mathbb{V})$ de todos los endomorfismos k-lineales de $\mathbb{V}$, equipado con la suma y la composición de morfismos, es un anillo. Recordemos aquí que la suma de dos transformaciones k-lineales f y g es la *suma puntual* definida por $(f + g)(x) = f(x) + g(x)$.

Ejemplo 2.1.5. Sea R un anillo. El subconjunto

$$Z(R) = \{z \in R : za = az \forall a \in R\} \subset R$$

es un subanillo, el *centro* de R.

Ejercicio 2.1.6. Sean R un anillo y $n \geq 1$. Sea

$$\Delta : R \to M_n R, \quad \Delta(a) = aI \tag{2.1.7}$$

la inclusión que manda un elemento de a a la matriz escalar correspondiente. Probar que $Z(M_n R) = \Delta(Z(R))$.

Ejercicio 2.1.8. Probar que la suma puntual $(f + g)(x) = f(x) + g(x)$ de dos morfismos de grupos abelianos es de nuevo un morfismo de grupos y que si M es un grupo abeliano, entonces el conjunto $\mathrm{End}_{\mathbb{Z}}(M)$ de todos sus endomorfismos, equipado con la suma puntual y la composición de morfismos, es un anillo.

Ejemplo 2.1.9. Sean k un cuerpo, $\mathbb{V}$ el k-espacio vectorial de todas las sucesiones $a = (a_1, , a_2, \dots)$ de elementos de k y $A = \mathrm{End}_k(\mathbb{V})$. Sean $S, T, p \in A$ las transformaciones k-lineales definidas para $a = (a_1, a_2, \dots)$ como sigue:

$$S(a) = (0, a_1, a_2, \dots), \quad T(a) = (a_2, a_3, \dots), p(a) = (a_1, 0, 0, \dots).$$

Notemos que $TS = \mathrm{id}$ y que $Tp = pS = 0$. Luego S tiene inversa a izquierda pero es divisor de cero a derecha y T tiene inversa a derecha pero es divisor de cero a izquierda; ninguno de los tres es inversible en A.

Notación 2.1.10. Sean A un grupo abeliano, X un conjunto y $f : X \to A$ una función. El *soporte* de f es el subconjunto $\mathrm{sop}(f) = \{x \in X : f(x) \neq 0\}$. Escribimos A^X por el grupo abeliano de todas las funciones $X \to A$ equipado con la suma puntual, y $A^{(X)} \subset A^X$ por el subgrupo formado por todas las funciones de soporte finito. Si $a \in A$ y $x \in X$, escribimos $a\chi_x$ por la función de soporte $\{x\}$ que vale a en x. Si $f \in A^{(X)}$, podemos escribirla como una suma

$$f = \sum_{x \in X} f(x)\chi_x \tag{2.1.11}$$

donde todos los sumandos salvo un número finito, son cero.

Ejemplo 2.1.12. Si A es un anillo, el grupo abeliano A^X, equipado con el producto puntual, es un anillo, cuyo elemento unidad es χ_X, la función característica de X. El subgrupo $A^{(X)}$ es cerrado para el producto; más aún, fg y $gf \in A^{(X)}$ para todo $f \in A^X$ y $g \in A^{(X)}$. Sin embargo no es un anillo –en el sentido de estas notas– pues no posee unidad. Más generalmente, si $\{A_x : x \in X\}$ es una familia de anillos, su producto cartesiano $\prod_{x \in X} A_x$, equipado con la suma y el producto puntuales es un anillo.

Ejemplo 2.1.13. (Anillo de un monoide) Sean M un monoide y A un anillo. Dadas $f, g \in A^{(M)}$, su *producto de convolución* se define como

$$(f \star g)(x) = \sum_{\{y,z \in X : yz = x\}} f(y)g(z).$$

Cuentas sencillas muestran que $\star$ es asociativo con neutro χ_1 y que es distribuivo con respecto a la suma de $A^{(M)}$. Notemos además que si $x, y \in M$, entonces

$$\chi_x \star \chi_y = \chi_{xy}.$$

Utilizando esto y la distributividad de $\star$ junto con la identidad (2.1.11), obtenemos

$$f \star g = \sum_{x \in M} \Big(\sum_{\{y,z \in X : yz = x\}} f(y)f(z) \Big) \chi_x.$$

Escribiremos $A[M]$ por anillo que resulta de equipar el grupo $A^{(M)}$ con el producto $\star$, al que llamaremos *anillo de M con coeficientes en A*.

Notación 2.1.14. Sean A un anillo y M un monoide. La función $\mathrm{inc} : A \to A[M]$, $a \mapsto a\chi_1$ es un monomorfismo. En adelante, si $a \in A$ y $m \in M$ identificaremos $a = \mathrm{inc}(a)$ y a menudo escribiremos $x = \chi_x$. De este modo, tenemos $A \subset A[M] \supset M$. A es un subanillo de $A[M]$ y M un submonoide de $(A[M], \cdot)$.

Ejemplo 2.1.15. Sean G un grupo y $g \in G \setminus \{1\}$ un elemento de orden finito n y k un cuerpo tal que $n \cdot 1$ es inversible en k. Sea $p = (1/n)\sum_{j=0}^{n-1} g^j \in k[G]$. Notemos que p es idempotente; en efecto

$$p^2 = 1/n^2 \sum_{0 \leq i,j \leq n-1} g^i g^j = (1/n) \sum_{i=0}^{n-1} (1/n)(\sum_{\{p,q : p+q=i\}} g^i) = p.$$

Luego $p(1-p) = 0$; como además $p \notin \{0,1\}$ concluimos que $k[G]$ no es un dominio. Si además G es finito y $|G|$ es inversible en k, entonces $q = (1/|G|)\sum_{g \in G} g$ también es idempotente, y $gq = q$ para todo $g \in G$.

Notación 2.1.16. Sea R un anillo. Escribimos

$$\mathrm{Idem}(R) = \{p \in R : p^2 = p\}.$$

Conjeturas sobre $R[G]$. Sea G un grupo. Decimos que G es *libre de torsión* si todo elemento $g \in G \setminus \{1\}$ tiene orden infinito. Sean G libre de torsión y R un dominio.

- (Conjetura del idempotente) Los únicos idempotentes de $R[G]$ son 0 y 1.
- (Conjetura del divisor de cero) $R[G]$ es un dominio.
- (Conjetura de las unidades) $R[G]^* = \{ug : u \in R^*, g \in G\}$

A la fecha de hoy, se sabe que las tres conjeturas son verdaderas para numerosas familias de grupos sin torsión G y de dominios R, pero el caso general continúa abierto.

2.2. Morfismos de anillos

Sean A y B anillos. Un *morfismo* de A a B es una función $f : A \to B$ que es a la vez morfismo de grupos $(A,+) \to (B,+)$ y morfismo de monoides $(A,\cdot) \to (B,\cdot)$, es decir, manda la suma en la suma y el producto en el producto y preserva ambos elementos neutros. El morfismo f es un *monomorfismo* si es inyectivo y un *isomorfismo* si es biyectivo.

Ejercicio 2.2.1. Probar que si $f : A \to B$ es un isomorfismo de anillos entonces la función inversa $f^{-1} : B \to A$ también lo es.

Ejemplo 2.2.2. Sea A un anillo. Si $\mathbb{Z} \to A$ es morfismo de anillos, debe enviar $1 \mapsto 1$, y por tanto $n \mapsto n \cdot 1$. Luego cada anillo recibe un único morfismo de $\mathbb{Z}$; este único morfismo se llama el morfismo *estructural* de A.

Sea A un anillo. Un *álgebra* sobre A consiste de un anillo B y un morfismo de anillos $i : A \to B$, que se llama *morfismo estructural* del álgebra. Por ejemplo todo anillo A es un álgebra sobre $\mathbb{Z}$, con el único morfismo $Z \to A$ como morfismo estructural (ver 2.2.2). Usualmente el morfismo se sobreentiende y se omite de la notación; decimos así que B es un álgebra sobre A. Un *morfismo de álgebras* de B en otra álgebra $j : A \to C$ es un morfismo de anillos $f : B \to C$ tal que $f \circ i = j$.

Notación 2.2.3. Si A es un anillo y B, C son A-álgebras, denotamos por

$\hom_{A-\mathfrak{Alg}}(B,C)$ al conjunto de todos los morfismos de A-álgebras $B \to C$. Abreviamos $\hom(B,C) = \hom_{\mathbb{Z}-\mathfrak{Alg}}(B,C)$. Si M y N son monoides,

$\hom_{\mathrm{Mon}}(M,N)$ es el conjunto de todos los morfismos de monoides $M \to N$.

Ejemplo 2.2.4. Sean $f : A \to B$ un morfismo y M un monoide. Consideremos a B como A-álgebra a través de f. Si $\hat{f} : A[M] \to B$ es un morfismo de A-álgebras, entonces para todo $a \in A$, $\tilde{f}(a) = f(a)$, y la restricción de $\tilde{f}$ a M es un morfismo de monoides $\phi : M \to (B,\cdot)$ con la propiedad de que

$$\phi(m)f(a) = f(a)\phi(m), \quad \forall a \in A, m \in M. \tag{2.2.5}$$

Notemos además que $\hat{f}$ está completamente determinado por f y por ϕ; en efecto, tenemos

$$\tilde{f}(\sum_m a_m \chi_m) = \sum_m f(a_m)\phi(m). \tag{2.2.6}$$

Recíprocamente, es un ejercicio ver que si ϕ y f cumplen (2.2.5), entonces (2.2.6) es morfismo de anillos. En otras palabras, la función

$$\hom(A[M],B) \to \hom(A,B) \times \hom_{\mathrm{Mon}}(M,B), \quad \hat{f} \mapsto (\hat{f}_{|A}, \hat{f}_{|M}), \tag{2.2.7}$$

es inyectiva, y su imagen está formada por todos los pares (f,ϕ) que cumplen (2.2.5). Fijando un morfismo de anillos $f : A \to B$ y considerando a B como A-álgebra mediante f, obtenemos una biyección entre $\hom_{A-\mathfrak{Alg}}(A[M],B)$ y el conjunto de los ϕ que cumplen (2.2.5).

La condición (2.2.5) se cumple, por ejemplo, si $B = A[N]$ es el álgebra de otro monoide N y $\phi : M \to N$ es morfismo de monoides. Otro ejemplo es el caso en que $f(A) \subset Z(B)$, que se da, e.g. cuando B es conmutativo.

Ejemplo 2.2.8. Sean A un anillo y $A[x]$ el álgebra de polinomios en una variable x. Sea

$$x^{\mathbb{N}_0} := \{x^n : n \in \mathbb{N}_0\} \subset A[x].$$

Notemos que $x^{\mathbb{N}_0}$ es un monoide; de hecho es un submonoide del monoide $(A[x],\cdot)$. La función

$$\mathbb{N}_0 \to x^{\mathbb{N}_0}, \quad n \mapsto x^n$$

es un isomorfismo de monoides. Por tanto induce un isomorfismo $A[\mathbb{N}] \cong A[x]$. Del mismo modo, para $m \geq 2$, $A[\mathbb{N}^m]$ es isomorfo al anillo

$$A[x_1,\dots,x_m] = (\dots((A[x_1])[x_2])\dots)[x_m]$$

de polinomios en m variables conmutativas con coeficientes en A. El isomorfismo es la identidad sobre A y manda $\chi_{(n_1,\dots,n_m)}$ en $x_1^{n_1}\cdots x_m^{n_m}$.

Proposición 2.2.9. *Sean R un anillo. Si R es dominio, $R[x]$ también lo es.*

Demostración. Sean $f,g \in R[x]$, ambos no nulos. Entonces podemos escribir $f = \sum_{i=0}^n a_i x^i$ y $g = \sum_{i=0}^m b_i x^i$ con $a_n \neq 0 \neq b_m$. Entonces $fg \neq 0$, ya que el coeficiente de x^{n+m} de fg es $a_n b_n \neq 0$. □

Ejemplo 2.2.10. (Polinomios de Laurent.) El *álgebra de polinomios de Laurent* en una variable sobre un anillo A es el anillo $A[x, x^{-1}]$ que consiste de todas las sumas formales finitas (i.e. con finitos sumandos no nulos) $\sum_{n\in\mathbb{Z}} a_n x^n$ con coeficientes en A. La aplicación $\mathbb{Z} \to x^{\mathbb{Z}} = \{x^n : n \in \mathbb{Z}\}$ es un isomorfismo de grupos, e induce un isomorfismo $A[\mathbb{Z}] \cong A[x, x^{-1}]$. Análogamente, si $m \geq 2$, $A[\mathbb{Z}^n]$ es isomorfo al álgebra $A[x_1, x_1^{-1}, \ldots, x_m, x_m^{-1}]$ de polinomios de Laurent en m-variables.

Proposición 2.2.11. *Sean $f : A \to B$ un morfismo de anillos y $n \geq 1$. Consideremos a B como A-álgebra a través de f. La aplicación*

$$\mathrm{ev} : \hom_{A-\mathfrak{Alg}}(A[x_1, \ldots, x_n], B) \to B^n, \quad \mathrm{ev}(f) = (f(x_1), \ldots, f(x_n))$$

es inyectiva, con

$$\mathrm{Im}(\mathrm{ev}) = \{(b_1, \ldots, b_n) : b_i b_j = b_j b_i, \quad f(a)b_i = b_i f(a) \quad \forall 1 \leq i, j \leq n, a \in A\}.$$

Demostración. En virtud de los Ejercicios 2.2.4 y 2.2.8 dar un morfismo de A-álgebras $A[x_1, \ldots, x_n] \to B$ equivale a dar un morfismo de monoides

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in \mathbb{N}_0^n\} \to B$$

cuya imagen consista de elementos que conmuten con los de la imagen de f. Si ϕ es un tal morfismo de monoides y $b_i = \phi(x_i)$, entonces

$$\phi(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = b_1^{\alpha_1} \cdots b_n^{\alpha_n} \tag{2.2.12}$$

Como además las variables x_i conmutan entre sí, lo mismo ocurre con los b_i. Recíprocamente si los b_i conmutan, (2.2.12) define un morfismo de monoides $\mathbb{N}_0^n \to B$. Si además los b_i conmutan con todos los elementos de la imagen de f, lo mismo pasa con todos los elementos de la imagen de ϕ. □

Ejercicio 2.2.13. Sean B una A-álgebra y $n \geq 1$. Probar que dar un morfismo de A-álgebras $A[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}] \to B$ equivale a dar un morfismo de A-álgebras $f : A[x_1, \ldots, x_n] \to B$ tal que $f(x_i) \in B^*$ $\forall 1 \leq i \leq n$.

Ejemplo 2.2.14. (Monoide libre y álgebra libre.) Sean X y Y conjuntos y sea X^Y el conjunto de todas las funciones $Y \to X$. Si Z es otro conjunto, escribimos $Y \coprod Z$ por la *unión disjunta*. Si $f \in X^Y$ y $g \in X^Z$, la *concatenación* de f y g es la única función $f \cup g : Y \coprod Z \to X$ que coincide con f sobre Y y con g sobre Z. En particular, $X^\emptyset$ tiene un único elemento, la función vacía $\emptyset$, y $\emptyset \cup f = f \cup \emptyset$ para toda $f \in X^Y$. Si Y tiene n elementos, identificamos X^Y con el producto cartesiano X^n de n copias de X. En particular $X^0 = X^\emptyset$. Si $n, m \geq 1$,

$$(x_1, \ldots, x_n) \cup (y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m).$$

El *monoide libre* en X es la unión disjunta

$$\mathrm{Mon}(X) = \coprod_{n=0}^{\infty} X^n$$

equipada con el producto de concatenación. Siguiendo las convenciones que adoptamos antes, llamamos 1 al elemento neutro $\emptyset$ de $\mathrm{Mon}(X)$. El *álgebra libre* en X con coeficientes en un anillo A es

$$A\{x \in X\} = A[\mathrm{Mon}(X)].$$

Si $X = \{x_1, \ldots, x_n\}$ escribimos $A\{x_1, \ldots, x_n\}$ por $A = \{x \in X\}$.

Ejercicio 2.2.15. Probar que dar un morfismo de anillos $A\{x \in X\} \to B$ equivale a dar un morfismo de anillos $f : A \to B$ y una función $\phi : X \to B$ tal que $f(a)\phi(x) = \phi(x)f(a)\ \forall a \in A, x \in X$.

2.3. Ideales

Sean R un anillo, e $I, J \subset (R, +)$ subgrupos. Escribimos

$$IJ = \{\sum_{i=1}^{n} x_i y_i : n \geq 1, x_i \in I, y_i \in J\}.$$

Decimos que I es ideal *ideal a izquierda* si $RI \subset I$, que es *ideal a derecha* si $IR \subset R$ y que es *ideal bilátero* (o, simplemente, ideal) si es ideal a ambos lados, lo que indicamos escribiendo $I \lhd R$.

Observación 2.3.1. Sea R un anillo. Sea R^{op} el anillo que resulta de equipar el grupo $(R, +)$ con el producto

$$x \cdot_{\mathrm{op}} y = yx.$$

Un ideal a izquierda de un anillo R es lo mismo que un ideal a derecha del anillo R^{op}.

Ejemplo 2.3.2. Sean R un anillo y $n \geq 1$. Entonces $M_n R \to M_n R$, $A \mapsto A^t$, es claramente un isomorfismo de grupos abelianos. Además

$$\begin{aligned}(AB)^t_{i,j} = (AB)_{j,i} &= \sum_{k=1}^{n} A_{j,k} B_{k,i} \\ &= sum_{k=1}^{n} B_{k,i} \cdot_{\mathrm{op}} A_{j,k} \\ &= \sum_{k=1}^{n} B^t_{i,k} \cdot A^t_{k,j}.\end{aligned}$$

Luego la transpuesta es también un isomorfismo de anillos $M_n R \xrightarrow{\sim} M_n(R^{\mathrm{op}})^{\mathrm{op}}$.

Ejemplo 2.3.3. Los ideales de $\mathbb{Z}$ son los subconjuntos de la forma $n\mathbb{Z}$ con $n \in \mathbb{Z}$. En efecto, vimos en el Ejemplo 1.2.13 que esos son todos los subgrupos de $\mathbb{Z}$; dado que son ideales, son todos los ideales.

Ejemplo 2.3.4. Si R es un anillo, $I \subset R$ un ideal a izquierda y $J \subset R$ un ideal a derecha, entonces $IJ \lhd R$.

Ejemplo 2.3.5. Sean R un anillo y $n \geq 2$. Si $I \lhd R$, el subconjunto $M_n I \subset M_n R$ de las matrices con todos sus coeficientes en I es un ideal bilátero de $M_n R$. Veremos a continuación que todo ideal bilátero de $M_n R$ es de esa forma. Sea $K \lhd M_n R$ un ideal. Sea

$$I = \{x \in R : xE_{1,1} \in K\}.$$

Es claro que I es cerrado por sumas; notemos además que si $a \in R$, $x \in I$ y Δ es como (2.1.7), entonces $\Delta(a)xE_{1,1} = (ax)E_{1,1}$ y $xE_{1,1}\Delta(a) = (xa)E_{1,1}$ están

ambos en K. Luego $I \lhd R$. Notemos además que si $a \in R$ y $1 \leq i, j, p, q \leq n$, entonces

$$aE_{i,j} = E_{i,p}aE_{p,q}E_{q,j}.$$

Aplicando esto para $a \in I$ y $p = q = 1$ obtenemos que $K \supset M_n I$, y aplicándolo para $a = A_{p,q}$ con $A \in K$, sale que $K \subset M_n I$.

Ejercicio 2.3.6. Sean R un anillo, $n \geq 1$ y $S \subset R^n$ un subgrupo tal que $RS \subset S$.

i) Sea $I(S) \subset M_n R$ el subconjunto formado por las matrices A tales que cada fila de A es un elemento de S. Probar que $I(S)$ es un ideal a izquierda.

ii) Se $I \subset M_n R$ un ideal a izquierda, y sea

$$R^n \supset S(I) = \{(A_{1,1}, \ldots, A_{1,n}) : A \in I\}.$$

Probar que $S(I) \subset R^n$ es un subgrupo que satisface $RS(I) \subset S(I)$.

iii) Probar que las aplicaciones $I \to S(I)$ y $S \to I(S)$ son biyecciones inversas entre los conjuntos de ideales a izquierda de $M_n R$ y de subgrupos $S \subset R^n$ tales que $RS \subset S$.

iv) Caracterizar los ideales a derecha de $M_n R$.

Sean R un anillo y $X \subset R$ un subconjunto y $\mathcal{F}(X)$ el conjunto de todos los subconjuntos finitos de X. El *ideal a izquierda generado por* X es

$$RX = \{\sum_{x \in F} a_x x : F \in \mathcal{F}(X), a_x \in R\}$$

Análogamente el *ideal a derecha de* R *generado por* X es $XR : R \cdot_{\text{op}} X$. El *ideal bilátero generado por* X es $\langle X \rangle := RXR$.

Ejemplo 2.3.7. Sean R un anillo y $x \in R$. Entonces

$$Rx = \{ax : a \in R\}, \quad xR = \{xa : a \in R\}, RxR = \{\sum_{i=1}^{n} a_i x b_i : a_i, b_i \in R\}. \tag{2.3.8}$$

Ejemplo 2.3.9. Sean R un anillo y $1 \leq i \leq n$. Entonces

$$M_n(R)E_{i,i} = \{A : A_{p,q} = \delta_{q,i}A_{p,q}\}$$
$$E_{i,i}M_n(R) = \{A : A_{p,q} = \delta_{p,i}A_{p,q}\}$$
$$M_n(R)E_{i,i}M_n(R) = M_n R.$$

Ejercicio 2.3.10. Sean R un anillo, $t \in \{$ izquierda, derecha, bilátero$\}$ y $\{I_\lambda : \lambda \in \Lambda\}$ una familia de ideales, todos de tipo t.

- Probar que $\bigcap_{\lambda \in \Lambda} I_\lambda$ es un ideal de tipo t.
- Sea $X \subset R$. Probar que el ideal de tipo t generado por X es la intersección de todos los ideales de tipo t que lo contienen.

- Sea
$$\sum_{\lambda\in\Lambda} I_\lambda = \{\sum_{\lambda\in F} x_\lambda : F \in \mathcal{F}(\Lambda), x_\lambda \in I_\lambda\}.$$
Probar que $\sum_{\lambda\in\Lambda} I_\lambda$ es la intersección de todos los ideales de tipo t que contienen a $\bigcup_{\lambda\in\Lambda} I_\lambda$.
- Sea $\{X_\lambda : \lambda \in \Lambda\}$ una familia de subconjuntos de R y sea $X = \bigcup_{\lambda\in\Lambda} X_\lambda$. Probar que el ideal de tipo t generado por X es la suma de los ideales de tipo t generados por cada uno de los X_λ.

Sea R un anillo conmutativo. Un ideal $I \lhd R$ se dice *principal* si existe $f \in R$ tal que $I = Rf$. Decimos que R es *principal* si todo ideal a izquierda de R es principal.

Ejemplo 2.3.11. Se sigue del Ejemplo 2.3.3 que $\mathbb{Z}$ es principal. Más generalmente esto ocurre en todo *dominio euclídeo*, que informalmente es un dominio conmutativo en el cual hay algoritmo de división, como por ejemplo el anillo $k[x]$ de polinomios en una variable sobre un cuerpo k. Formalmente un dominio conmutativo R es euclídeo si existe una función $f : R \setminus \{0\} \to \mathbb{N}_0$ tal que si $a, b \in R$, $b \neq 0$, entonces existen $q, r \in R$ con $a = bq + r$ de modo que $r = 0$ o $f(r) < f(b)$. Si R es euclídeo y $0 \neq I \lhd R$, entonces el conjunto $\{n \in \mathbb{N}_0 : (\exists a \in I) f(a) = n\}$ es no vacío. Luego tiene primer elemento m y hay $d \in I$ tal que $f(d) = m$. Si $a \in I$ y $a = dq + r$, entonces $r \in I$, por lo que si $r \neq 0$, $f(r) \geq m = f(d)$. Luego a es múltiplo de d, y por tanto $I = Rd$.

Ejemplo 2.3.12. Veremos que el anillo $\mathbb{Z}[x]$ no es principal. Sea $d \in \mathbb{Z} \setminus \{0, 1, -1\}$; consideremos el ideal

$$I = \langle d, x\rangle = \{\sum_{i=0}^{n} a_i x^i : d \backslash a_0\}$$

Sea $f \in I$. Si $\mathrm{gr}(f) > 0$, entonces todo múltiplo no nulo de f será también de grado positivo; en particular, $d \notin \mathbb{Z}[x]f$. Si $\mathrm{gr}(f) = 0$, entonces $f \in d\mathbb{Z}$, y todo múltiplo de f está en $\mathbb{Z}[x]d$; en particular, $x \notin \mathbb{Z}[x]f$. Luego I no es principal.

Ejercicio 2.3.13. Sean k un cuerpo y $n \geq 2$. Probar que el ideal $\langle x_1, x_2, \ldots, x_n\rangle \lhd k[x_1, \ldots, x_n]$ no es principal.

Proposición 2.3.14. *Sea $R \neq 0$ un anillo. Son equivalentes*

i) R es anillo de división.

ii) Si $0 \neq I \subset R$ es ideal a izquierda, entonces $I = R$.

iii) Si $0 \neq I \subset R$ es ideal a derecha, entonces $I = R$.

Demostración. Un ideal I de R –de cualquier tipo– es todo R si y sólo si $1 \in R$. La condición $i)$ equivale a que si $x \in R \setminus \{0\}$, entonces $Rx = R$, es decir, $1 \in Rx$, o lo que es lo mismo, x tiene inversa a izquierda y. Como esto vale para todo elemento no nulo, y y también tiene inversa a izquierda z. Luego por el Ejemplo 1.1.1 ii), x es inversible y $x^{-1} = y$. En conclusión, i) y ii) son equivalentes. En particular, por la Observación 2.3.1, R^{op} es de división si y sólo si se cumple iii). Pero por otro lado R^{op} es de división si y sólo si R lo es, lo que termina la demostración. □

Podemos sintetizar la Proposición 2.3.14 diciendo que un anillo es de división si y sólo si tiene exactamente 2 ideales a izquierda si y sólo si tiene exactamente 2 ideales a derecha. Un anillo R se dice *simple* si tiene exactamente 2 ideales biláteros.

Ejemplo 2.3.15. Sean R un anillo y $n \geq 2$. Por el Ejemplo 2.3.5, $M_n R$ es simple si y sólo si R lo es. En particular, si R es de división, entonces $M_n R$ es simple; sin embargo no es de división, ya que tiene ideales laterales no triviales, por el Ejercicio 2.3.6.

2.4. Cocientes

Lema 2.4.1. *Si $f : R \to S$ es morfismo de anillos, entonces*

i) $\mathrm{Ker}(f) \lhd R$ *e* $\mathrm{Im}(f) \subset S$ *es subanillo.*

ii) Las biyecciones inversas de la Proposición 1.4.24 entre subgrupos de R que contienen a $\mathrm{Ker}(f)$ *y subgrupos de* $\mathrm{Im}(f)$ *preservan subanillos e ideales.*

Demostración. Las identidades

$$f(1) = 1, \quad f(xy) = f(x)f(y)$$

nos dicen que si $\mathcal{A} \subset R$ es un ideal o un subanillo, lo mismo ocurre con el grupo aditivo $f(\mathcal{A})$ y que si $\mathcal{B} \subset \mathrm{Im}(f)$ es ideal o subanillo, lo mismo es cierto del grupo $f^{-1}(\mathcal{B})$. □

Lema 2.4.2. *Sean R un anillo, A un grupo abeliano y $f : R \to A$ un epimorfismo de grupos abelianos. Supongamos que* $\mathrm{Ker}(f) \lhd R$. *Entonces existe un único producto que hace de A un anillo y de f un morfismo de anillos.*

Demostración. Para que f sea morfismo, debe ser

$$f(x)f(y) = f(xy). \tag{2.4.3}$$

Sea $K = \mathrm{Ker}(f)$. Como f es suryectiva por hipótesis, hay a lo sumo un producto en A con esa propiedad. Para ver que (2.4.3) define una función $A \times A \to A$ debemos verificar que $f(xy)$ depende sólo de $f(x)$ y $f(y)$. En efecto, si $f(x') = f(x)$ y $f(y') = f(y)$ entonces $x' = x + k$, $y' = y + l$ con $k, l \in K$, y por tanto $x'y' = xy + xl + ky + kl \in xy + K$, lo que implica que $f(x'y') = f(xy)$. Luego (2.4.3) define un producto en A; todas las propiedades que debe cumplir para hacer del grupo A un anillo son inmediatas de (2.4.3). □

Ejemplos 2.4.4.

- Sea $n \in \mathbb{N}$ y sea $r : \mathbb{Z} \to \mathbb{Z}_n := \{0, \ldots, n-1\}$ la función que asigna a cada entero su resto en la división por n. La suma módulo n hace de $\mathbb{Z}_n$ un grupo abeliano; por el Teorema 1.6.10, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. La operación del Lema 2.4.2 es el producto módulo n.
- Sean k un cuerpo, $f \in k[x]$ un polinomio de grado $n > 0$ y $k[x]_{<n} \subset k[x]$ el k-espacio vectorial generado por $1, x, \ldots, x^{n-1}$. Sea $r : k[x] \to k[x]_{<n}$ la función que asigna a cada polinomio su resto en la división por f. El producto del Lema 2.4.2 en este caso es el producto módulo f; escribimos $k[x]_f$ por el anillo resultante. Así por ejemplo, $\mathbb{R}[x]_{x^2+1} \cong \mathbb{C}$, mediante el isomorfismo $a + bx \mapsto a + bi$.

Ejercicio 2.4.5. Generalizar los Ejemplos (2.4.4) en las siguientes dos direcciones.

i) Sea R un dominio euclídeo y $f : R \to \mathbb{N}_0$ como en el Ejemplo 2.3.11. Sea $a \in R$ tal que $f(a) > 0$, $r : R \to R$ la función resto de dividir por a y $\mathcal{R} = \mathrm{Im}(r) \subset R$. Probar que existe una única estructura de anillo en $\mathcal{R}$ que hace de $r : R \to \mathcal{R}$ morfismo de anillos.

ii) Sean k un anillo conmutativo y $f = \sum_{i=0}^{n} a_i x^i \in k[x]$ un polinomio de grado $n > 0$. Probar que si $a_n \in k^*$ entonces para todo $p \in k[x]$ existen únicos $q \in k[x]$ y $r \in k[x]_{<n}$ tales que $p = fq + r$. Utilizar esto para ver que el subgrupo $k[x]_{<n} \subset k[x]$ tiene una única estructura de anillo que hace de la función "resto en la división por f"morfismo de anillos.

Observación 2.4.6. El Lema 2.4.2 se aplica, por ejemplo cuando A es el grupo cociente $R/K = \{a + K : a \in R\}$; siempre consideraremos al cociente equipado con el único producto que hace de la proyección al cociente morfismo de anillos. Por definición, ese producto es $(a + K) \cdot (b + K) = ab + K$. Notemos que este producto no es igual al conjunto $S(a, b)$ de todos los productos de elementos de $a + K$ con elementos de $b + K$, que es

$$S(a, b) = ab + aK + Kb + \{k_1 k_2 : k_i \in K\};$$

en general $S(a, b) \subset ab + aK + Kb + K^2 \subsetneq ab + K$. Por ejemplo $S(0, 0) \subset K^2$ y la inclusión $K^2 \subset K$ puede ser estricta, e.g. si $R = \mathbb{Z}$ y $K = n\mathbb{Z}$, $K^2 = n^2\mathbb{Z} \subsetneq n\mathbb{Z}$.

Teorema 2.4.7. *Sean R un anillo, $K \lhd R$, $\pi : R \to R/K$ la proyección y $f : R \to S$ un morfismo de anillos tal que* $\mathrm{Ker}(f) = K$.

i) Existe un único morfismo de anillos $\bar{f} : R/K \to S$ tal que $\bar{f}\pi = f$.

ii) $\mathrm{Im}(f) \cong R/\mathrm{Ker}(f)$.

Demostración. Sabemos del Teorema 1.6.10 que existe un único morfismo de grupos $\bar{f}$ tal que $f = \bar{f}\pi$. Además, $\bar{f}(\pi(1)) = f(1) = 1$ y tenemos

$$\bar{f}(\pi(x)\pi(y)) = \bar{f}(\pi(xy)) = f(xy) = f(x)f(y) = \bar{f}(\pi(x))\bar{f}(\pi(y)).$$

Sabemos también del Teorema 1.6.10 que para $K = \mathrm{Ker}(f)$, $\bar{f} : R/K \to \mathrm{Im}(f)$ es biyectiva; por la parte i), es isomorfismo de anillos. □

Ejemplo 2.4.8. Se sigue del Teorema 2.4.7 que el anillo A que resulta del Lema 2.4.2 es isomorfo a $R/\mathrm{Ker}(f)$. Aplicando esto a los Ejemplos 2.4.4, tenemos isomorfismos de anillos $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, $k[x]_f \cong k[x]/fk[x]$.

Ejemplo 2.4.9. Sean R un anillo, $I \lhd R$ un ideal y $\pi : R \to R/I$ la proyección al cociente. Abusando notación, designamos también π al morfismo $M_n R \to M_n(R/I)$, $\pi(A)_{i,j} = \pi(A_{i,j})$. Este morfismo es suryectivo con núcleo $M_n I$; por el Teorema 2.4.7, deducimos que $M_n R/M_n I \cong M_n(R/I)$.

Ejemplo 2.4.10. Sean k un cuerpo, $\mathbb{V}$, A y $S, T \in A$ como en el Ejemplo 2.1.9. Por el Ejercicio 2.2.15, existe un único morfismo de k-álgebras $p : k\{x, y\} \to A$ que manda $x \mapsto S$, $y \mapsto T$. Consideremos la *k-álgebra de Toeplitz* $\mathcal{T}(k) = k\{x, y\}/\langle yx - 1\rangle$. Dado que $TS = 1$, $\langle yx - 1\rangle \subset \mathrm{Ker}(p)$; luego por el Teorema 2.4.7, p induce un morfismo $\bar{p} : \mathcal{T}(k) \to A$. Veremos que $\bar{p}$ es inyectiva.

Comencemos por observar que en $\mathcal{T}(k)$ todo elemento se escribe como combinación lineal, con coeficientes en k, de las imágenes de los monomios $x^i y^j$, $i, j \geq 0$ y que $p(x^i y^j) = S^i T^j$. Por tanto, para probar que $\bar{p}$ es inyectiva, basta probar que el subconjunto $\{S^i T^j : i, j \geq 0\} \subset A$ es linealmente independiente. Sea $\mathcal{B} = \{e_n : n \geq 1\}$ la base canónica de $\mathbb{V}$. Entonces

$$S^i T^j(e_n) = \begin{cases} e_{n-j+i} & \text{si } n \geq j+1 \\ 0 & \text{si no} \end{cases} \tag{2.4.11}$$

Sea $E_{p,q} \in A$ el morfismo determinado por $E_{p,q}(e_n) = \delta_{q,n} e_p$. Se sigue de (2.4.11) que

$$S^i T^j = \sum_{n \geq 1} E_{i+n, j+n}. \tag{2.4.12}$$

A partir de la descripción (2.4.12) es un ejercicio verificar que $\{S^i T^j : i, j \geq 0\}$ es l.i.

Ejemplo 2.4.13. Sean k un cuerpo, $n \geq 2$ y $J_n \lhd k\{x_1, \dots, x_n, y_1, \dots, y_n\}$

$$J_n = \langle 1 - \sum_{i=1}^{n} x_i y_i, \quad y_i x_j - \delta_{i,j} \quad (1 \leq i, j \leq n) \rangle$$

Consideremos la *k-álgebra de Leavitt* $L_n(k) = k\{x_1, \dots, x_n, y_1, \dots, y_n\}/J_n$. Abusando notación y escribiendo x_i y y_i por sus imágenes en $L_n(k)$, e I_n por la matriz identidad de $n \times n$, tenemos

$$[x_1, \dots, x_n] \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = 1 \tag{2.4.14}$$

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} [x_1, \dots, x_n] = I_n \tag{2.4.15}$$

Sabemos de álgebra lineal que $k^m \cong k \iff m = 1$; por tanto no existe ningún morfismo de k-álgebras de $L_n(k)$ en k. Más generalmente, dos espacios vectoriales finitamente generados sobre un anillo de división son isomorfos si y sólo si tienen la misma dimensión, por lo que $L_n(k)$ tampoco admite morfismos con valores en k-álgebras de división. Veamos que sin embargo $L_n(k)$ no es cero. Sean $\mathbb{V}$ y A como en el Ejemplo 2.4.10. Sean $r, q : \mathbb{Z} \to \mathbb{Z}$ las funciones que asignan a cada entero su resto y su cociente en la división por n. Sean $S_i, T_i \in A$, $(i = 0, \dots, n-1)$,

$$S_i(e_m) = e_{nm+i}, \quad T_i(e_m) = \delta_{i,r(m)} q(m).$$

Cálculos sencillos muestran que $T_i S_j = \delta_{i,j}\,\mathrm{id}$, $\sum_{i=0}^{n} S_i T_i = \mathrm{id}$. Luego por el Ejercicio 2.2.15 y el Teorema 2.4.7, existe un único morfismo de k-álgebras $L_n(k) \to A$ que manda las clases de x_i y y_i en S_{i-1} y T_{i-1} $\forall 1 \leq i \leq n$. Se sigue que $L_n(k) \neq 0$.

Observación 2.4.16. Sea R un anillo conmutativo principal. Entonces R/I es principal para todo ideal $I \lhd R$, por Lema 2.4.1.

Sean R un anillo, $t \in \{\text{izquierda, derecha, bilátero}\}$ e $I \subset R$ un ideal de tipo t. Decimos que I es *maximal* de tipo t si $I \neq R$ y R es el único ideal de tipo t que lo contiene. En otras palabras si $J \subsetneq R$ es otro ideal de tipo t e $I \subset J$ entonces $J = I$.

Un ideal bilátero $K \lhd R$ es *primo* si $ab \in K$ con $a, b \in R$ implica $a \in K$ o $b \in K$.

Proposición 2.4.17. *Sean R un anillo y $K \lhd R$.*

i) R/K es anillo de división si y sólo si K es maximal a izquierda, si y sólo si K es maximal a derecha.

ii) R/K es simple si y sólo si K es maximal entre todos los ideales biláteros de R.

iii) R/K es dominio si y sólo si K es primo.

Demostración. Sea $\pi : R \to R/K$ la proyección al cociente. Por el Lema 2.4.1, para cada tipo t de ideales, la función $I \mapsto \pi(I)$ es una biyección entre los ideales de tipo t de R que contienen a K y los ideales de tipo t de R/K. Claramente esa biyección preserva la relación de inclusión, y por tanto preserva ideales maximales de cada tipo; las partes i) y ii) se siguen de esta observación. Para probar iii), observemos que la identidad $\pi(x)\pi(y) = \pi(xy)$ nos dice que $\pi(x)\pi(y) = 0$ si y sólo si $xy \in K$. Como además $\pi(x) = 0 \iff x \in K$, tenemos que $\pi(x)$ es divisor de cero si y sólo si $x \notin K$ y existe $y \in R \setminus K$ tal que o bien $xy \in K$ o $yx \in K$. Esto termina la demostración. □

Ejemplo 2.4.18. Sea R un dominio conmutativo. Un elemento $f \in R$ se dice *irreducible* si no es inversible y si $f = g_1 g_2$ y $g_1 \notin R^*$ entonces $g_2 \in R^*$. Notar que como $fR \subset gR$ si y sólo si $g \backslash f$, decir que f es irreducible equivale a decir que fR es maximal entre los ideales principales propios. Si R es principal, todos los ideales lo son, y por tanto en ese caso, f es irreducible si y sólo si fR es maximal. Luego R/fR es cuerpo si y sólo si f es irreducible.

Un anillo $R \neq 0$ se dice *simple puramente infinito* si no es un anillo de división y para todo $a \in R \setminus \{0\}$ existen $x, y \in R$ tales que $xay = 1$.

Ejemplo 2.4.19. Vimos en el Ejemplo 2.3.5 que si R es un anillo y $n \geq 1$, entonces los ideales biláteros de $M_n R$ son todos los subconjuntos de la forma $M_n I$ con $I \lhd R$. En particular, $M_n R$ es simple si y sólo si R lo es. Así, por ejemplo $M_n(D)$ es simple para todo anillo de división D. Sin embargo $M_n(D)$ no es puramente infinito; si $n = 1$ esto es por definición. Si $n \geq 2$ y D es un cuerpo, sabemos que si $a \in M_n D$ tiene rango $\mathrm{rk}(a) \in \{1, \dots, n-1\}$ entonces $\mathrm{rk}(xay) < n$ para todo $x, y \in M_n D$, y por tanto $xay \neq 1$. Notemos que esencialmente la propiedad que usamos es que un subespacio propio (en este caso $\mathrm{Im}(a)$) de un espacio vectorial de dimensión finita tiene dimensión finita menor que la del espacio. Veremos más adelante que esto también vale para espacios vectoriales sobre anillos de división, por lo que el argumento de antes se aplica también para D anillo de división.

Ejemplo 2.4.20. Sean k un cuerpo, $V = k^{(\mathbb{N})}$, $\mathcal{B} = \mathrm{End}_k(\mathbb{V})$ y

$$\mathcal{F} = \{f \in \mathcal{B} : \dim(\mathrm{Im}(f)) < \infty\}.$$

Notemos que $\mathcal{F} \lhd \mathcal{B}$. Sea $\mathcal{Q} = \mathcal{B}/\mathcal{F}$; veremos que $\mathcal{Q}$ es simple puramente infinito. Para ello utilizaremos que el el hecho –que ya conocemos en dimensión

finita– de que un subespacio de un espacio vectorial tiene dimensión menor o igual a la del espacio es válido también en dimensión infinita. Esto se demostrará más adelante en el curso. Podemos escribir a $\mathbb{V}$ como suma directa de dos subespacios de dimensión infinita, $\mathbb{V} = \mathbb{V}_0 \oplus \mathbb{V}_1$; sean p_0 y p_1 las proyecciones sobre $\mathbb{V}_0$ y $\mathbb{V}_1$ correspondientes a esa descomposición. Entonces $p_0, p_1 \notin \mathcal{F}$ pero $p_0 p_1 = 0$. En particular ni p_0 ni p_1 son nulas ni inversibles módulo $\mathcal{F}$, de lo que se sigue que Q no es de división. Sea $a \in \mathcal{B} \setminus \mathcal{F}$; entonces $\mathrm{Im}(a)$ tiene dimensión infinita numerable. Sea $\{a(w_n)\}$ una base de $\mathrm{Im}(a)$; entonces los w_n son l.i. y generan un subespacio $\mathbb{W} \subset \mathbb{V}$ que también tiene dimensión infinita numerable. Sean $\{e_n\}$ la base canónica de $\mathbb{V}$ y sean $x : \mathrm{Im}(a) \to \mathbb{V}$, $x(a(w_n)) = e_n$ y $y : \mathbb{V} \to \mathbb{W}$, $y(e_n) = w_n$. Entonces $xay = 1$ y lo mismo sucede con sus imágenes en $\mathcal{Q}$.

Ejemplo 2.4.21. Sea k un cuerpo. Leavitt probó en [4] que el álgebra $L_n(k)$ del Ejemplo 2.4.13 es simple puramente infinita para todo $n \geq 2$.

Lema 2.4.22. *Sean R un anillo, $n \geq 2$ y $K_1, \dots, K_n \lhd R$. Sea $L_i = \bigcap_{j \neq i} K_j$. Supongamos que $K_i + K_j = R$ $(\forall i \neq j)$. Entonces $K_i + L_i = R$ $\forall 1 \leq i \leq n$.*

Demostración. Hacemos inducción en n. Si $n = 2$ no hay nada que probar. Sea $n \geq 3$ y supongamos el lema cierto para $n-1$ ideales. Para $1 \leq i \neq j \leq n$, sea $M_{i,j} = \bigcap_{l \notin \{i,j\}} K_l$. Sean $1 \leq i \neq j \leq n$; por hipótesis inductiva, $K_i + M_{i,j} = R$. Luego

$$\begin{aligned} R = K_i + R =& K_i + (K_i + M_{i,j})(K_i + K_j) \\ =& K_i + K_i^2 + K_i K_j + M_{i,j} K_i + M_{i,j} K_j \\ \subset& K_i + L_i \subset R. \end{aligned}$$

□

Teorema 2.4.23. *(Teorema chino del resto) Sean R un anillo, $n \geq 2$ y $K_1, \dots, K_n$ ideales biláteros de R tales que $K_i + K_j = R$ para todo $i \neq j$. Sea $K = \bigcap_{i=1}^n K_i$. Entonces $R/K \cong \bigoplus_{i=1}^n R/K_i$.*

Demostración. Para cada $1 \leq i \leq n$, sea $\pi_i : R \to R/K_i$ la proyección. Sea $\pi : R \to \bigoplus_{i=1}^n R/K_i$, $\pi(a) = (\pi_1(a), \dots, \pi_n(a))$. Observemos que $\mathrm{Ker}(\pi) = K$; luego $R/K \cong \mathrm{Im}(\pi)$ por el Teorema 2.4.7. Resta ver que π es suryectiva. Por el Lema 2.4.22, para cada i existen $k_i \in K_i$ y $l_i \in L_i$ tales que $1 = k_i + l_i$. Sean $a = (a_1, \dots, a_n) \in R^n$; entonces $a_i = a_i k_i + a_i l_i \equiv a_i l_i \mod K_i$. Sea $x = \sum_{i=1}^n a_i l_i$; para todo i, $x \equiv a_i \mod K_i$. Luego $\pi(x) = a$. □

Ejemplo 2.4.24. Sean k un cuerpo, $f \in k[x]$ un polinomio mónico de grado positivo, y $f = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su factorización irreducible. Notemos que si $i \neq j$, $\langle p_i^{\alpha_i}, p_j^{\alpha_j} \rangle = k[x]$, por Euclides. Podemos aplicar entonces el Teorema 2.4.23 y resulta $R = k[x]/fk[x] = \bigoplus_{i=1}^n k[x]/p_i^{\alpha_i} k[x]$. En particular, si $\alpha_i = 1$ para todo i, R es producto directo de cuerpos, por el Ejemplo 2.4.18.

Teorema 2.4.25. *Sean R un anillo y $K \lhd R$.*

i) Sean $A \subset R$ un subanillo. Entonces $A + K \subset R$ es subanillo y $(A + K)/K \cong A/A \cap K$.

ii) Sea $K \subset I \lhd R$ un ideal. Entonces $I/K \lhd R/K$ y $(R/K)/(I/K) \cong R/I$.

Demostración. Sea $\pi : R \to R/K$ la proyección al cociente. Para la parte i), observemos que $A + K = \pi^{-1}(\pi(A))$, que es subanillo por el Lema 2.4.1. La demostración de i) se termina como la del Teorema 1.6.15, usando el Teorema 2.4.7 en lugar del Teorema 1.6.10. La parte ii) sale como en el Teorema 1.6.20. □

Terminaremos esta sección probando que todo anillo tiene ideales maximales. Usaremos para ello el *Lema de Zorn*, un enunciado acerca de conjuntos parcialmente ordenados que es equivalente al *Axioma de elección*. Un *orden parcial* en un conjunto X es una relación $\leq$ entre elementos de X que es reflexiva ($x \leq x$), transitiva ($x \leq y \wedge y \leq z \Rightarrow x \leq z$) y antisimétrica ($x \leq y \wedge y \leq x \Rightarrow x = y$). Si $\leq$ es un orden parcial, escribimos $x < y$ para indicar que $x \leq y$ pero $x \neq y$. Un *conjunto parcialmente ordenado* $X = (X, \leq)$ es un conjunto X junto con un orden parcial $\leq$. Un orden parcial es *total* si $x \not\leq y \Rightarrow y < x$. Un conjunto con un orden total se llama una *cadena*.

Lema 2.4.26. *(Lema de Zorn) Sea $(X, \leq)$ un conjunto no vacío parcialmente ordenado. Supongamos que toda cadena en X tiene cota superior. Entonces X tiene un elemento maximal.*

Teorema 2.4.27. *Sea R un anillo y sea $t \in \{$izquierda, derecha, bilátero$\}$. Entonces cada ideal $I \subsetneq R$ de tipo t está contenido en un ideal maximal de tipo t.*

Demostración. Sea X el conjunto de todos los ideales propios (i.e. $\neq R$) de tipo t de R que contienen a I, parcialmente ordenado por inclusión. Sea $Y \subset X$ una cadena; queremos ver que Y es acotada, es decir que hay $J \in X$ que contiene a todos los elementos de Y. Si $Y = \emptyset$, I cumple con esto. Supongamos entonces que $Y \neq \emptyset$ y sea $J = \bigcup_{K \in Y} K$. Es claro que $J \supset K$ para todo $K \in Y$ y que $J \supset I$. Afirmo que J es un ideal de tipo t. En efecto, $0 \in I \subset J$ y si $x, y \in J$ y $a \in R$ entonces existe $K \in Y$ tal que $x, y \in K$ y por tanto $x + y \in K$, lo mismo que, según el tipo t, ax y/o xa. Así, por Lema de Zorn, X tiene un elemento maximal M. Por definición de X, M es un ideal de tipo t y es maximal entre todos los ideales del mismo tipo *que contienen a I*. Resta ver que M es maximal entre todos los ideales de tipo t de R. Si M no fuera maximal, existiría un ideal propio $N \subset R$ de tipo t tal que $M \subsetneq N$. Pero entonces $N \supset I$ y por tanto $N \in X$, contradiciendo la maximalidad de M. □

Observación 2.4.28. Se sigue del Teorema 2.4.27 y de la Proposición 2.4.17 que todo anillo R tiene un cociente R/I que es un anillo simple. Si además R es conmutativo, R/I es un cuerpo. Destaquemos, sin embargo, que un anillo no conmutativo R puede no admitir ningún cociente que sea anillo de división; esto ocurre, por ejemplo, si $R = M_n S$ para algún anillo S y algún $n \geq 2$. En efecto, por el Ejemplo 2.3.5, todo cociente de R es M_n de algún cociente de S, y un tal anillo siempre tiene divisores de cero; e.g. $E_{1,1}E_{2,2} = 0$. También hay anillos que no tienen nigún cociente isomorfo al anillo de matrices de ningún anillo de división; tal es el caso de los anillos simples puramente infinitos (e.g. los de los ejemplos 2.4.20 y 2.4.21).

Proposición 2.4.29. *Sea R un anillo y sea $\mathfrak{M} = R \setminus R^*$. Son equivalentes:*

i) $\mathfrak{M}$ es un ideal a izquierda.

ii) $\mathfrak{M}$ es un ideal a derecha.

iii) R tiene un único ideal a izquierda maximal.

iv) R tiene un único ideal a derecha maximal.

Demostración. Sean $x, y \in R$.

$$\text{Si } xy = 1, \text{ entonces } x \in \mathfrak{M} \iff y \in \mathfrak{M}. \tag{2.4.30}$$

Si $\mathfrak{M}$ es ideal a izquierda o a derecha, no puede ser que $x \vee y \in \mathfrak{M}$, pues si no $1 \in \mathfrak{M}$, es decir, $1 \notin R^*$, lo que es absurdo. Así, si se satisfacen i) o ii), todo elemento que tiene inversa a izquierda o a derecha es inversible. Esto implica, por ejemplo, que, bajo la hipótesis i), si $x \in \mathfrak{M}$ y $a \in R$, entonces xa no puede ser inversible, por lo que debe estar en $\mathfrak{M}$. Es decir que $\mathfrak{M}$ es un ideal bilátero. Si suponemos ii) llegamos a la misma conclusión. Luego i) y ii) son equivalentes, y si suponemos cualquiera de las dos, como todo ideal propio (a izquierda, a derecha o bilátero) está contenido en $\mathfrak{M}$, se sigue que valen tanto iii) como iv). Recíprocamente, supongamos que iii) se satisface, y sea $\mathfrak{N}$ el único ideal a izquierda maximal. Entonces $\mathfrak{N} \cap R^* = \emptyset$, y por tanto $\mathfrak{N} \subset \mathfrak{M}$. Por otro lado si $x \in R \setminus \mathfrak{N}$, x no puede estar en ningún ideal maximal a izquierda, lo que por el Teorema 2.4.27 implica que existe un $a \in R$ tal que $ax = 1$. Sea $p = xa$; tenemos $p^2 = xaxa = ax = p$, es decir

$$0 = p(1-p) = (1-p)p. \tag{2.4.31}$$

Luego si $p \notin \mathcal{N}$, existe $b \in R$ tal que $bp = 1$, lo que por (2.4.31) implica que $p = 1$ y por tanto $x \in R^*$. Si $p \in \mathcal{N}$, entonces $1 - p \notin \mathcal{N}$ y por tanto $p = 0$, de nuevo por (2.4.31). Pero entonces $1 = 1^2 = axax = apx = 0$, lo que es absurdo, ya que $R \neq 0$ pues posee un ideal maximal. Concluimos así que $\mathcal{N} = \mathcal{M}$, lo que prueba que iii)⇒ i). Análogamente, iv)⇒ii), lo que termina la demostración. □

Un anillo R se dice *local* si satisface las condiciones equivalentes de la Proposición 2.4.29.

Ejercicio 2.4.32. Probar que si R es un anillo local entonces $\mathrm{Idem}(R) = \{0, 1\}$.

Sean R un anillo y $a \in R$. Decimos que a es *nilpotente* si existe $n \geq 1$ tal que $a^n = 0$. Escribimos

$$\mathrm{Nil}(R) = \{a \in R | a \text{ nilpotente}\}.$$

Proposición 2.4.33. *Sean k un cuerpo y $\iota : k \to R$ una k-álgebra tal que $\iota(k) \subset Z(R)$ y $0 < \dim_k R < \infty$. Entonces R es local si y sólo si* $\mathrm{Idem}(R) = \{0, 1\}$. *En ese caso $R \setminus R^* = \mathrm{Nil}(R)$.*

Demostración. Por el Ejercicio 2.4.32, si R es local, $\mathrm{Idem}(R) = \{0, 1\}$. Recíprocamente, supongamos que $\mathrm{Idem}(R) = \{0, 1\}$. Como $\iota(k) \subset Z(R)$, para cada $a \in R$ la función $L_a : R \to R$, $L_a(x) = ax$ es k-lineal. Entonces $L : R \to \mathrm{End}_k(A)$ es un monomorfismo de k-álgebras. Sean $\mathfrak{M} = R \setminus R^*$ y $a \in \mathfrak{M}$. La sucesión de ideales a derecha $I_n = a^n R = (L_a)^n R$ es decreciente, y cada uno es un subespacio k-lineal de R. Como $\dim_k R < \infty$, existe m tal que para todo n, $I_m = I_{m+n}$. Si $I_m = 0$, $a^m = 0$. Supongamos que $I_m \neq 0$, y sea $K_m = \mathrm{Ker}(L_{a^m})$. Notemos que K_m es un ideal a derecha de R. Como $a^m I_m = I_{2m} = I_m$, $K_m \cap I_m = 0$. Pero por el teorema de la dimensión, $\dim_k K_m + \dim_k I_m = \dim_k R$, luego $R = I_m \bigoplus K_m$

y por tanto existen $p \in I_m$ y $q \in K_m$ tales que $1 = p + q$. Entonces $p = p^2 + qp$, lo que implica que $p - p^2 \in I_m \cap K_m = 0$. Luego $p \in \mathrm{Idem}(R)$, y por tanto $p = 0, 1$. Si $p = 0$, $1 \in K_m$ y por tanto $a^m = 0$. Si $p = 1$, $K_m = 0$ y por tanto $a^m \in R^*$, lo que implica que $a \in R^*$, que es una contradicción. Hemos probado que $\mathfrak{M} := R \setminus R^* = \mathrm{Nil}(R)$. Resta ver que $\mathfrak{M}$ es un ideal. Sean $x \in \mathfrak{M} \setminus \{0\}$ y $n \geq 1$ tal que $x^n = 0$ y $x^{n-1} \neq 0$. Si $a \in R$ entonces $x^{n-1}(xa) = 0 = (ax)x^{n-1}$; luego ni xa ni ax pueden ser inversibles. Por tanto $\mathfrak{M}$ es cerrado por multiplicación a izquierda y a derecha. En particular, si $\lambda \in R^*$ y $x \in \mathfrak{M}$, existe $n \geq 1$ tal que $(\lambda^{-1}x)^n = 0$, y por tanto

$$\begin{aligned}(\lambda + x)(\sum_{i=0}^{n-1}(\lambda^{-1}x)^i)\lambda^{-1} &= \lambda(1 + \lambda^{-1}x)\left((\sum_{i=0}^{n-1}(\lambda^{-1}x)^i)\right)\lambda^{-1} \\ &= \lambda\lambda^{-1} = 1.\end{aligned}$$

Así, $\lambda + x$ es inversible a derecha y por tanto no puede ser nilpotente, de modo que es inversible. Sean ahora $y, z \in \mathfrak{M}$; queremos probar que $\lambda = y + z \in \mathfrak{M}$. Supongamos que no; entonces $\lambda \in R^*$ y por lo que acabamos de ver, $y = \lambda - z$ es inversible, que es una contradicción. Esto termina la demostración de que $\mathfrak{M}$ es un ideal y la de la proposición. □

Capítulo 3

Módulos

3.1. Módulos y morfismos

Sea R un anillo. Un *R-módulo (a izquierda)* consiste de un grupo abeliano M y una operación

$$\cdot : R \times M \to M$$

tal que las siguientes identidades se satisfacen $\forall\ m, n \in M$ y $a, b \in R$:

$$1 \cdot m = m, \quad a \cdot (b \cdot m) = (ab) \cdot m, \quad (a+b) \cdot m = a \cdot m + b \cdot m, \quad a \cdot (m+n) = a \cdot m + a \cdot n. \tag{3.1.1}$$

Las identidades de arriba pueden resumirse diciendo que la aplicación

$$\rho : R \to \mathrm{map}(M, M), \ \ \rho(a)(m) = a \cdot m \tag{3.1.2}$$

manda R en $\mathcal{E} = \mathrm{End}_{\mathbb{Z}}(M)$ y que su correstricción a $\mathcal{E}$ es morfismo de anillos. En otras palabras dar una estructura de R-módulo a izquierda en un grupo abeliano M equivale a dar un morfismo de anillos

$$\rho : R \to \mathrm{End}_{\mathbb{Z}}(M).$$

El *anulador* del módulo M es el ideal $\mathrm{Ann}_R(M) = \mathrm{Ker}(\rho) \lhd R$. Decimos que M es *fiel* si $\mathrm{Ann}_R(M) = 0$.

Un *submódulo* de un R-módulo M es un subgrupo abeliano N tal que $R \cdot N \subset N$.

Un *R-módulo a derecha* es un R^{op}-módulo a izquierda.

Observación 3.1.3. Por lo dicho arriba un R-módulo a derecha es un grupo abeliano M con un morfismo de anillos $\rho : R^{\mathrm{op}} \to \mathrm{End}_{\mathbb{Z}}(M)$. La condición de que ρ mande el producto en el producto nos dice que

$$\rho(ba) = \rho(a \cdot_{\mathrm{op}} b) = \rho(a)\rho(b). \tag{3.1.4}$$

En términos de la multiplicación asociada $\cdot : R \times M = R^{\mathrm{op}} \times M \to M$, esto se traduce en que para todo $a, b \in R$ y $m \in M$

$$(ba) \cdot m = a \cdot (b \cdot m).$$

Esta condición luce más natural si la expresamos en términos de la función

$$\cdot : M \times R \to M, \ \ m \cdot a = \rho(a)(m).$$

Tenemos

$$\begin{aligned} m \cdot (ab) =& (ab) \cdot m = b \cdot (a \cdot m) \\ =& (m \cdot a) \cdot b. \end{aligned}$$

Ejemplos 3.1.5. i) El anillo R, equipado con la multiplicación a izquierda por elementos de R es un módulo a izquierda fiel. En particular, R^{op} es un R^{op} módulo a izquierda fiel, es decir, R es un R módulo a derecha (fiel) con la multiplicación a derecha. Cuando queremos enfatizar que consideramos a R como módulo a izquierda o a derecha escribimos ${}_R R$ y R_R respectivamente. Los submódulos de ${}_R R$ son los ideales a izquierda de R; los de R_R son los ideales a derecha.

ii) Sean M un R-módulo y X un conjunto. El conjunto M^X de todas las funciones $X \to M$, con la suma puntual y la multiplicación puntual por elementos de R, es un R-módulo. El subconjunto $M^{(X)} \subset M^X$ de todas las funciones de soporte finito es un submódulo.

iii) Se sigue de los dos ítems anteriores y del Ejercicio 2.3.6 que los ideales a izquierda de $M_n R$ están en correspondencia biunívoca con los R-submódulos de R^n.

iv) Dar una estructura de $\mathbb{Z}$-módulo en un grupo M es lo mismo que dar un morfismo de anillos $\mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$. Dado que hay un único tal morfismo, se sigue que un $\mathbb{Z}$-módulo es lo mismo que un grupo abeliano.

v) Un módulo sobre un cuerpo k es lo mismo que un k-espacio vectorial. En virtud de la Proposición 2.2.11 un $k[x]$-módulo consiste de un k-espacio vectorial $\mathbb{V}$ y una transformación k-lineal $T : \mathbb{V} \to \mathbb{V}$. El anulador de este módulo, en tanto ideal de $k[x]$, es o bien 0 (e.g. cuando $\mathbb{V} = k[x]$ y $T = L_x$), o bien tiene un único generador mónico (e.g. si $\dim_k \mathbb{V} < \infty$), que se llama el *polinomio minimal* de T. Por la misma proposición, si $n \geq 2$, un $k[x_1, \ldots, x_n]$-módulo consiste de un k-e.v. $\mathbb{V}$ y n transformaciones lineales $T_1, \ldots, T_n : \mathbb{V} \to \mathbb{V}$ tales que para todo i, j, $T_i T_j = T_j T_i$. Por el Ejercicio 2.2.15 un $k\{x_1, \ldots, x_n\}$-módulo consiste de un k-e.v. $\mathbb{V}$ y n transformaciones lineales $T_1, \ldots, T_n : \mathbb{V} \to \mathbb{V}$.

vi) Sean $n \geq 2$, k un cuerpo y $L_n = L_n(k)$ la k-álgebra de Leavitt. Se sigue del Ejercicio 2.2.15 y del Teorema 2.4.7 que un L_n-módulo consiste de un espacio vectorial $\mathbb{V}$ y $2n$ transformaciones lineales $S_1, \ldots, S_n, T_1, \ldots, T_n \in \mathrm{End}_k(\mathbb{V})$ tales que $T_i S_j = \delta_{i,j} \mathrm{id}_{\mathbb{V}}$ y $\sum_{i=1}^n S_i T_i = \mathrm{id}_{\mathbb{V}}$.

vii) Sean $\phi : R \to S$ un morfismo de anillos y N un S-módulo. Sea $\rho : S \to \mathrm{End}_{\mathbb{Z}}(N)$, $\rho(s)(n) = s \cdot n$. Entonces $\rho \circ \phi : R \to \mathrm{End}_{\mathbb{Z}}(N)$ es morfismo de anillos, y por tanto nos da una estructura de R-módulo en N, definida por

$$a \cdot_\phi n = \phi(a) n.$$

Escribimos ${}_\phi N$ por N equipado con esta estructura de R-módulo.

viii) Sean R un anillo, $a \in Z(R)$ y $\mathrm{ev}_a : R[x] \to R$, $\mathrm{ev}_a(f) = f(a)$ la evaluación en a. Supongamos que R es conmutativo, de modo que ev_a es morfismo de anillos. Sea ${}_a R = {}_{\mathrm{ev}_a} R$; entonces $\mathrm{Ann}_R({}_a R) = R[x](x - a)$.

ix) Sean k un cuerpo y $\iota : k \to Z(R) \subset R$ una k-álgebra. Sean M un R-módulo y $\mathbb{V} = {}_\iota M$. Entonces la imagen de $\rho : R \to \mathrm{End}_{\mathbb{Z}}(M)$, $\rho(a)(m) = am$ cae en $\mathrm{End}_k(\mathbb{V}) \subset \mathrm{End}_{\mathbb{Z}}(M)$. Abusando notación llamaremos ρ también a la correstricción de ρ a $\mathrm{End}_k(\mathbb{V})$. Un submódulo de $\mathbb{V}$ es un subespacio $\mathbb{W}$ tal que $\rho(a)(\mathbb{W}) \subset \mathbb{W}$ para todo $a \in R$. Si $\dim_k \mathbb{V} = n$ y $\dim_k \mathbb{W} = m$ esto significa que si $\mathcal{B}$ es una base de $\mathbb{V}$ que contiene a una base de $\mathbb{W}$, entonces para cada $a \in R$, existen $X_a \in M_m k$, $Y_a \in M_{m\times(n-m)}k$ y $Z_a \in M_{n-m}k$ tales que la matriz con respecto a $\mathcal{B}$ de transformación lineal $\rho(a)$ tiene la forma

$$[\rho(a)]_{\mathcal{B}} = \left[\begin{array}{c|c} X_a & Y_a \\ \hline 0 & Z_a \end{array}\right]$$

Notemos además que $\mathbb{V}$ también es un $S = \rho(R)$ módulo, y que $\mathbb{W}$ es un R-submódulo si y sólo si es un S-submódulo.

Observación 3.1.6. Sean M un R-módulo a izquierda y $x \in M$. Sea

$$\mathrm{Ann}_R(x) = \{a \in R : ax = 0\}.$$

Notemos que $Rx \subset M$ es un submódulo a izquierda y que

$$\mathrm{Ann}_R(Rx) = \bigcap_{y \in Rx} \mathrm{Ann}_R(y) \subset \mathrm{Ann}_R(x). \tag{3.1.7}$$

Si R es conmutativo, vale la igualdad en (3.1.7), pero si R no es conmutativo, la inclusión puede ser estricta. Por ejemplo, si R es un anillo y $n \geq 1$, entonces para todo $1 \leq k \leq n$,

$$(M_n R)E_{1,1} = M_n(R)E_{k,1} = I_1 = \{A \in M_n R : A_{i,j} = 0 \,\forall j \neq 1\}.$$

Por otro lado, si $n \geq 2$,

$$0 = \mathrm{Ann}_{M_n R}(I_1) \subsetneq \mathrm{Ann}_{M_n R}(E_{k,1}) = \{A : A_{i,k} = 0 \,\forall i\}.$$

Ejercicio 3.1.8. Sean R un anillo, M un R-módulo, $a \in R$ y $m \in M$. Probar las siguientes identidades entre elementos de M:

$$a \cdot 0 = 0 = 0 \cdot m.$$

Sean R un anillo, M y N R-módulos y $f : M \to N$ una función. Decimos que f es *morfismo de R-módulos* –o que es un morfismo *R-lineal*– si f es morfismo de grupos abelianos y $f(ax) = af(x)$ para todo $a \in R$ y $x \in M$. Un morfismo R-lineal es monomorfismo, epimorfismo o isomorfismo si es inyectivo, suryectivo o biyectivo. La función inversa de un isomorfismo es nuevamente un morfismo R-lineal.

Ejercicio 3.1.9. Si M y N son R-módulos isomorfos, entonces $\mathrm{Ann}_R(M) = \mathrm{Ann}_R(N)$. En particular, si R es conmutativo, los $R[x]$-módulos ${}_a R$ ($a \in Z(R)$) del Ejemplo 3.1.5 viii) son no isomorfos 2 a 2.

Sean R un anillo y M y N R-módulos. Escribimos

$$\hom_R(M, N) = \{f : M \to N | f \text{ morfismo de } R\text{-módulos }\}$$
$$\mathrm{End}_R(M) = \hom_R(M, M), \quad \mathrm{Aut}_R(M) = \{f \in \mathrm{End}_R(M) : f \text{ iso}\}.$$

La suma puntual de dos morfismos de R-módulos es de nuevo un morfismo de R-módulos y dota al conjunto $\hom_R(M,N)$ de una estructura de grupo abeliano. La composición de dos morfismos R-lineales es un morfismo R-lineal. Si P es otro R-módulo, la composición da una aplicación

$$\circ : \hom_R(N,P) \times \hom_R(M,N) \to \hom_R(M,P), \tag{3.1.10}$$

y esta aplicación es *bilineal*, es decir que si $f_1, f_2 \in \hom_R(N,P)$ y $g_1, g_2 \in \hom_R(M,N)$,

$$(f_1+f_2)\circ g_1 = f_1\circ g_1 + f_2 \circ g_1 \text{ y } f_1 \circ (g_1+g_2) = f_1\circ g_1 + f_1 \circ g_2. \tag{3.1.11}$$

En particular, el grupo $\mathrm{End}_R(N)$ junto con la composición de morfismos es un anillo, y $\hom_R(M,N)$ es un $\mathrm{End}_R(N)$-módulo a izquierda y un $\mathrm{End}_R(M)$-módulo a derecha. Si $a \in R$ y M es un R módulo, la aplicación $L_a : M \to M$, $L_a(x) = ax$ es morfismo de grupos abelianos; si además $a \in Z(R)$, L_a es también R-lineal. La aplicación $L : Z(R) \to \mathrm{End}_R(M)$, $a \mapsto L_a$ es morfismo de anillos, y por tanto podemos ver a $\hom_R(M,N)$ como $Z(R)$-módulo a través de L, como en el Ejemplo 3.1.5 vii). La aplicación (3.1.10) es $Z(R)$-bilineal, es decir, además de (3.1.11), safisface también que para todo $z \in Z(R)$,

$$(z\cdot f)\circ g = f \circ (z\cdot g) = z\cdot (f\circ g). \tag{3.1.12}$$

Ejemplo 3.1.13. Sean R un anillo y $\mathcal{M}$ un monoide. Un $R[\mathcal{M}]$-módulo consiste de un R-módulo M y un morfismo de monoides $\mathcal{M} \to (\mathrm{End}_R(M), \circ)$. En particular, si G es un grupo, un $R[G]$-módulo es un R-módulo equipado con una acción de G por automorfismos R-lineales. Si $\rho : R[G] \to \mathrm{End}_{\mathbb{Z}}(M)$ y $\mu : R[G] \to \mathrm{End}_{\mathbb{Z}}(N)$ son $R[G]$-módulos, un morfismo $\phi : M \to N$ de grupos abelianos es $R[G]$-lineal si y sólo si es R-lineal y tal que para todo $g \in G$, $\phi \circ \rho(g) = \mu(g)\circ\phi$. En particular, un automorfismo $R[G]$-lineal de M es un automorfismo R-lineal ϕ tal que para todo $g \in G$, $\phi\circ\rho(g)\circ\phi^{-1} = \rho(g)$.

Sean M un grupo abeliano y R y S anillos. Una estructura de (R,S)-bimódulo en M consiste de una estructura de R módulo a izquierda $\rho : R \to \mathrm{End}_{\mathbb{Z}}(M)$ y una estructura S-módulo a derecha $\mu : S^{\mathrm{op}} \to \mathrm{End}_{\mathbb{Z}}(M)$ tales que $\rho(a)\mu(b) = \mu(b)\rho(a)$ para todo $a \in R$ y $b \in S$. En otras palabras

$$(a\cdot x)\cdot b = a\cdot(x\cdot b) \quad (\forall a \in R,\ \ b \in S,\ \ x \in M).$$

Aún otra manera de expresar esto es decir que $\mathrm{Im}(\rho) \subset \mathrm{End}_{S^{\mathrm{op}}}(M)$ y/o que $\mathrm{Im}(\mu) \subset \mathrm{End}_R(M)$.

Ejemplo 3.1.14. Sean M, N R-módulos. Entonces la composición de morfismos hace de $\hom_R(M,N)$ un $(\mathrm{End}_R(N), \mathrm{End}_R(M))$-bimódulo. Supongamos que N es (R,S)-bimódulo y sean $\rho : R \to \mathrm{End}_{S^{\mathrm{op}}}(N)$ y $\mu : S^{\mathrm{op}} \to \mathrm{End}_R(N)$ los morfismos de anillos que dan las acciones a izquierda y a derecha de R y S en N. Entonces como en el Ejemplo 3.1.5 vii), podemos ver a $\hom_R(M,N)$ como S-módulo a derecha a través de μ. La correspondiente multiplicación es

$$\hom_R(M,N)\times S \to \hom_R(M,N), \quad (f\cdot s)(m) = f(m)s.$$

Análogamente, si P es un S-módulo a derecha, $\hom_{S^{\mathrm{op}}}(P,N)$ es un R-módulo a izquierda a través del morfismo ρ.

Ejercicio 3.1.15. Sean R y S anillos y M un (R,S)-bimódulo, con acciones a izquierda y derecha dadas por morfismos $\rho : R \to \mathrm{End}_{\mathbb{Z}}(M)$ y $\mu : S^{\mathrm{op}} \to \mathrm{End}_{\mathbb{Z}}(M)$. Sean N un R-módulo a izquierda y P un S-módulo a derecha. Probar que $\hom_R(M,N)$ es un S-módulo a izquierda vía μ y que $\hom_S(M,P)$ es un R-módulo a derecha vía ρ.

Ejemplo 3.1.16. Sea M un R-módulo a izquierda. Como R es un (R,R)-bimódulo,
$\hom_R(R,M)$ es un R-módulo a izquierda. La aplicación

$$\mathrm{ev}_1 : \hom_R(R,M) \to M, \quad \mathrm{ev}_1(f) = f(1)$$

es un isomorfismo de módulos. Su inversa manda un elemento $m \in M$ al morfismo $a \mapsto a \cdot m$.

Ejemplo 3.1.17. En el caso particular $M = {}_RR$, el Ejemplo 3.1.16 nos da un isomorfismo de R-módulos a izquierda $\mathrm{End}_R({}_RR) \xrightarrow{\sim} {}_RR$ cuya inversa μ manda un elemento a de R a la multiplicación a derecha por a, a la que, por obvias razones, nos abstenemos de llamar R_a. Observemos que μ es un morfismo de anillos $R^{\mathrm{op}} \to \mathrm{End}_R({}_RR)$. Por otro lado, la aplicación $L : R \to \mathrm{End}_R(R_R)$, $L_a(x) = ax$ es un isomorfismo de anillos. Esto hace que para ciertos propósitos, sea más cómodo trabajar con módulos a derecha que con módulos a izquierda.

Ejemplo 3.1.18. Sea M un R-módulo; el *dual* de M es $M^* = \hom_R(M,R)$. Por el Ejemplo 3.1.14, M^* es un R-módulo a derecha, y $(M^*)^*$ es un R-módulo a izquierda. La función

$$\varepsilon : M \to (M^*)^*, \quad \varepsilon(m)(\phi) = \phi(m)$$

es morfismo de R-módulos.

3.2. Correspondencia entre R-módulos y M_nR-módulos

Sean R un anillo, $n \geq 2$, M un R-módulo. Si $A \in M_nR$ y $x \in M^n$, está definido el producto

$$A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_j A_{1,j}x_j \\ \vdots \\ \sum_j A_{n,j}x_j \end{bmatrix}.$$

Este producto hace de M^n un M_nR-módulo que denotaremos $F(M)$. Si $\phi : M \to N$ es un morfismo de R-módulos, definimos

$$F(\phi) : F(M) \to F(N), \quad F(\phi)(x_1,\ldots,x_n) = (\phi(x_1),\ldots,\phi(x_n)).$$

Notemos que $F(\phi)$ es morfismo de M_nR-módulos. Recíprocamente, si P es un M_nR-módulo y $\Delta : R \to M_nR$ es el morfismo diagonal de (2.1.7), entonces $G(P) = E_{1,1}P \subset {}_\Delta P$ es un R-submódulo, y todo morfismo de M_nR-módulos $\psi : P \to Q$ se restringe a un morfismo de R-módulos $G(\psi) : G(P) \to G(Q)$.

Teorema 3.2.1. *Sean R, n, M, N, P, Q, ϕ y ψ como arriba. Sean*

$$\alpha_M : G(F(M)) \to M, \ \ \alpha_M(E_{1,1}x) = x_1,$$
$$\beta_P : F(G(P)) \to P, \ \ \beta_P(E_{1,1}y_1, \dots, E_{1,1}y_n) = \sum_{i=1}^{n} E_{i,1}y_i$$

Entonces

i) α_M y β_P son isomorfismos, de R-módulos y de M_nR-módulos, respectivamente.

ii) Los siguientes diagramas conmutan

$$\begin{array}{ccc} G(F(M)) & \xrightarrow{\alpha_M} & M \\ \downarrow{\scriptstyle G(F(\phi))} & & \downarrow{\scriptstyle \phi} \\ G(F(N)) & \xrightarrow{\alpha_N} & N \end{array} \qquad \begin{array}{ccc} F(G(P)) & \xrightarrow{\beta_P} & P \\ \downarrow{\scriptstyle F(G(\psi))} & & \downarrow{\scriptstyle \psi} \\ F(G(Q)) & \xrightarrow{\beta_Q} & Q \end{array}$$

iii) Las funciones

$$F : \hom_R(M, N) \to \hom_{M_nR}(F(M), F(N)) \ y$$
$$G : \hom_{M_nR}(P, Q) \to \hom_R(G(P), G(Q))$$

son isomorfismos de grupos. Además tanto F como G preservan la composición de morfismos y satisfacen $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$ y $G(\mathrm{id}_P) = \mathrm{id}_{G(P)}$.

Demostración. Si $x \in M^n$, entonces $E_{1,1}x = (x_1, 0, \dots, 0)$. Luego $G(F(M)) = M \oplus \bigoplus_{i=1}^{n-1} 0$ y α es la proyección sobre la primera coordenada, que es claramente un isomorfismo. Es claro que β_P es morfismo de grupos; veamos que es M_nR-lineal. Sean $A \in M_nR$; entonces

$$\begin{aligned} A \cdot \beta_P(E_{1,1}y_1, \dots, E_{1,1}y_n) =& (\sum_{i,j} A_{i,j}E_{i,j}) \cdot (\sum_{l} E_{l,1}y_l) \\ =& \sum_{i,l} A_{i,l}E_{i,1}y_l = \sum_{i} E_{i,1} \sum_{l} A_{i,l}E_{1,1}y_l \\ =& \beta_P(\sum_{1,l} A_{1,l}E_{1,1}y_l, \dots, \sum_{n,l} A_{n,l}E_{1,1}y_l) \\ =& \beta_P(A \cdot (E_{1,1}y_1, \dots, E_{1,1}y_n)). \end{aligned}$$

Sea $\gamma_P : P \to F(G(P))$, $\gamma_P(y) = (E_{1,1}y, \dots, E_{1,n}y)$. Tenemos

$$\beta_P(\gamma_P(y)) = \beta_P(E_{1,1}y, \dots, E_{1,n}y) = \sum_{i=1}^{n} E_{i,1}E_{1,i}y = (\sum_{i=1}^{n} E_{i,i})y = y.$$

y

$$\begin{aligned} \gamma_P(\beta_P(y_1, \dots, y_n)) =& \gamma_P(E_{1,1}y_1 + \cdots + E_{n,1}y_n) \\ =& (E_{1,1}E_{1,1}y_1, \dots, E_{1,n}E_{n,1}y_n) = (y_1, \dots, y_n). \end{aligned}$$

Esto prueba la parte i) del teorema. Es claro que el primer diagrama de la parte ii) conmuta. Para chequear la conmutatividad del segundo, basta ver que ambas composiciones coinciden en cada sumando de $F(G(P))$. El i-ésimo sumando es $E_{1,1}P$, y las composiciones mandan $E_{1,1}y$ en $\psi(E_{i,1}y)$ y $E_{i,1}\psi(y)$ respectivamente, que son iguales porque ψ es morfismo de M_nR-módulos. Esto prueba la parte ii) del teorema. La parte iii) es inmediata de la definición de las funciones F y G. □

3.3. Morfismos de módulos y cocientes

Proposición 3.3.1. *Sean R un anillo y $f : M \to N$ un morfismo de R-módulos. Entonces las biyecciones inversas de la Proposición 1.4.24 preservan submódulos. En particular,* $\mathrm{Im}(f)$ *y* $\mathrm{Ker}(f)$ *son submódulos, y $T \mapsto f^{-1}(T)$ y $S \mapsto f(S)$ son biyecciones inversas entre los conjuntos de submódulos de* $\mathrm{Im}(f)$ *y de submódulos de M que contienen a* $\mathrm{Ker}(f)$.

Demostración. Inmediata de la Proposición 1.4.24 usando la identidad $f(ax) = af(x)$ $(a \in R,\ x \in M)$ y el Ejercicio 3.1.8. □

Lema 3.3.2. *Sean R un anillo, M un R-módulo y $\pi : M \to G$ un morfismo suryectivo de grupos abelianos. Si* $\mathrm{Ker}(f) \subset M$ *es un submódulo, entonces existe una única estructura de R-módulo que hace de G un R-módulo y de π un morfismo R-lineal.*

Demostración. La suryectividad de π junto con la fórmula

$$a\pi(x) = \pi(ax) \tag{3.3.3}$$

nos dicen que existe a lo sumo una estructura de R-módulo en el grupo G. Además si $\pi(x) = \pi(y)$, entonces $x - y \in \mathrm{Ker}(\pi)$ y por tanto $ax - ay \in \mathrm{Ker}(\pi)$, es decir que $\pi(ax) = \pi(ay)$. Por tanto (3.3.3) da una función bien definida $R \times G \to G$. Resta ver que se satisfacen las identidades (3.1.1); esto se sigue de que las mismas identidades son válidas en M. □

Teorema 3.3.4. *Sean R un anillo, M un R-módulo, $S \subset M$ un submódulo y $\pi : M \to M/S$ la proyección. Sea $f : M \to N$ un morfismo de R-módulos tal que* $\mathrm{Ker}(f) \supset S$. *Entonces*

i) Existe un único morfismo R-lineal $\bar{f} : M/S \to N$ tal que $\bar{f} \circ \pi = f$.

ii) El morfismo f induce un isomorfismo $M/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$.

Demostración. Para probar i), hay que ver que el morfismo de grupos $\bar{f} : M/S \to N$ del Teorema 1.6.10 conmuta con la acción de R. Esto se sigue de la identidad $\bar{f} \circ \pi = f$ y de que f es R-lineal. Probemos ii). Sabemos del Teorema 1.6.10 que la correstricción del morfismo $\bar{f} : M/\mathrm{Ker}(f) \to N$ es un isomorfismo de grupos $M/\mathrm{Ker}(f) \to \mathrm{Im}(f)$; por i) este isomorfismo es R-lineal. □

Teorema 3.3.5. *Sean R un anillo, M un R-módulo y $S, T \subset M$ submódulos. Entonces el isomorfismo del Teorema 1.6.15 es isomorfismo de módulos*

$$S/S \cap T \xrightarrow{\sim} (S + T)/T.$$

Demostración. La proyección al cociente $\pi : M \to M/T$ restringida a S es un morfismo con núcleo $S \cap T$ e imagen $\pi(S)$; la restricción de π a $S + T$ tiene la misma imagen y su núcleo es T. Luego aplicando la parte i) del Teorema 3.3.4 se obtiene el isomorfismo deseado. □

3.4. Hom_R es exacto a izquierda

Sean M, N y P R-módulos y sea $f : M \to N$ un morfismo R-lineal. Sean

$$\hom_R(P, f) : \hom_R(P, M) \to \hom_R(P, N), \quad \alpha \mapsto f \circ \alpha$$
$$\hom_R(f, P) : \hom_R(N, P) \to \hom_R(M, P), \quad \beta \mapsto \beta \circ f$$

Para aliviar notación, cuando R y P están claros del contexto, escribimos $f_* = \hom_R(P, f)$ y $f^* = \hom_R(f, P)$. Notemos que

$$(\mathrm{id}_M)_* = \mathrm{id}_{\mathrm{End}_R(M)} = (\mathrm{id}_M)^*. \tag{3.4.1}$$

Además si L es otro R-módulo y $g \in \hom_R(N, L)$, tenemos

$$(g \circ f)_* = g_* \circ f_*, \quad (g \circ f)^* = f^* \circ g^*. \tag{3.4.2}$$

Ejercicio 3.4.3. Sean $f : M \to N$ y P como arriba. Probar que f_* y f^* son morfismos de $Z(R)$-módulos.

Ejemplo 3.4.4. Sean k un cuerpo y $f : \mathbb{V} \to \mathbb{W}$ una transformación k-lineal de k-espacios vectoriales. Notemos que el morfismo $f^* : \mathbb{W}^* = \hom_k(\mathbb{W}, k) \to \mathbb{V}^*$ definido arriba no es otra cosa que la transformación lineal transpuesta f^t de álgebra lineal. En general, si R es un anillo cualquiera y $f : M \to N$ un morfismo de R-módulos a izquierda, llamamos *transpuesta* de f al morfismo de R-módulos a derecha $f^* : N^* = \hom_R(N, {}_R R) \to M^*$, al que a menudo denotaremos f^t.

Una sucesión $\{f_n : M_n \to M_{n+1} : n \in \mathbb{Z}\}$ de morfismos de R-módulos se dice *exacta* si para todo $n \in \mathbb{Z}$ se tiene $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0 \tag{3.4.5}$$

Lema 3.4.6. *Sean* (3.4.5) *una sucesión exacta de R-módulos y sea N un R-módulo. Entonces las siguientes sucesiones de morfismos de $Z(R)$-módulos son exactas*

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

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

Demostración. Como $p \circ i = 0$, tenemos $i^* \circ p^* = 0$ y $p_* \circ i_* = 0$, por (3.4.2), luego $\mathrm{Im}(p^*) \subset \mathrm{Ker}(i^*)$ e $\mathrm{Im}(i_*) \subset \mathrm{Ker}(p_*)$. Un elemento $f \in \hom_R(N, M)$ está en $\mathrm{Ker}(p_*)$ si y sólo si $\mathrm{Im}(f) \subset \mathrm{Ker}(p) = \mathrm{Im}(i)$. Como i es inyectiva por hipótesis, su correstricción es un isomorfismo $i' : M' \xrightarrow{\sim} \mathrm{Im}(i)$; sea $j = (i')^{-1}$. Entonces $i_*(jf) = f$; en particular, $f \in \mathrm{Im}(i_*)$. Luego $\mathrm{Ker}(p_*) = \mathrm{Im}(i_*)$. Un elemento de $\hom_R(N, M')$ está en $\mathrm{Ker}(i_*)$ si y sólo si su composición con i es 0. Como i es inyectiva, esto implica que el elemento en cuestión es 0. Hemos probado la exactitud de la primera sucesión. Sea ahora $g \in \hom_R(M, N)$; entonces $g \in \mathrm{Ker}(i^*)$ si y sólo si $g(\mathrm{Im}(i)) = 0$. Dado que, por hipótesis, $\mathrm{Im}(i) = \mathrm{Ker}(p)$ y p es suryectiva, se sigue del Teorema 3.3.4 que existe un único morfismo $\bar{g} \in \hom_R(M'', N)$ tal que $p^*(\bar{g}) = \bar{g} \circ p = g$. Esto se aplica, en particular, cuando $g = 0$ y demuestra que p^* es inyectivo. □

Observación 3.4.7. Siguiendo la demostración del Lema 3.4.6, vemos que la suryectividad de p en (3.4.5) no es necesaria para la exactitud de la primera sucesión del lema, y que la inyectividad de i no es necesaria para la exactitud de la segunda. Notemos también que, a pesar de que las hipótesis del lema piden tanto que i sea inyectiva como que p sea suryectiva, no se afirma ni que p_* ni que i^* sean suryectivas, y en general no lo son, como muestran los Ejemplos 3.4.8. Por supuesto, si p tiene inversa a derecha, p_* también la tiene, por (3.4.1) y (3.4.2), y por tanto es suryectiva. Del mismo modo si i tiene inversa a izquierda, i_* tiene inversa a derecha, y por tanto es suryectiva también.

Ejemplos 3.4.8. Sea $n \in \mathbb{N}_{\geq 2}$; consideremos la sucesión exacta de grupos abelianos

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0. \tag{3.4.9}$$

Aplicando $\hom_{\mathbb{Z}}(-,\mathbb{Z})$ obtenemos la sucesión exacta

$$0 \to 0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z}$$

Vemos así que aunque la muliplicación por n es un morfismo inyectivo, su transpuesta no es suryectiva. Por otro lado, si aplicamos $\hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, -)$ a (3.4.9) obtenemos la sucesión exacta

$$0 \to 0 \to 0 \to \mathbb{Z}/n\mathbb{Z}$$

Vemos así que aunque la proyección al cociente $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es suryectiva, $\pi_* = \hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \pi)$ no lo es.

3.5. Suma y producto directos

Sean R un anillo, I un conjunto y $\{M_i : i \in I\}$ una familia de R-módulos. El *producto directo* de la familia $\{M_i : i \in I\}$ es el producto cartesiano $\prod_{i\in I} M_i$ equipado con las operaciones coordenada a coordenada, es decir, si $a \in R$ y $x, y \in \prod_{i\in I} M_i$,

$$(ax)_i = ax_i, \quad (x+y)_i = x_i + y_i.$$

El *soporte* de un elemento $x \in \prod_{i\in I} M_i$ es

$$\operatorname{sop}(x) = \{i \in I : x_i \neq 0\}.$$

La *suma directa* de la familia $\{M_i : i \in I\}$ es el R-submódulo

$$\prod_{i\in I} M_i \supset \bigoplus_{i\in I} M_i = \{x : |\operatorname{sop}(x)| < \infty\}.$$

Para cada $j \in I$ sean

$$\pi_j : \prod_{i\in I} M_i \to M_j, \quad \pi_j(x) = x_j$$
$$\iota_j : M_j \to \bigoplus_{i\in I} M_i, \quad (\iota_j(y))_i = \delta_{i,j} y.$$

Notemos que si M es un R-módulo, entonces

$$\prod_{i\in I} M = M^I \supset M^{(I)} = \bigoplus_{i\in I} M.$$

Proposición 3.5.1. *Sean R un anillo, N un R módulo y $\{M_i : i \in I\}$ una familia de R-módulos. Entonces para cada familia de morfismos de R-módulos $\{f_i : N \to M_i | i \in I\}$ existe un único morfismo de R-módulos $f : N \to \prod_{i\in I} M_i$ tal que para todo $i \in I$, $\pi_i \circ f = f_i$.*

Demostración. La función $f : N \to \prod_{i\in I} M_i$, $f(x)_i = f_i(x)$ es la única tal que $\pi_i \circ f = f_i$ para todo i. Dado que las operaciones en el producto directo se calculan coordenada a coordenada y que los f_i son morfismos R-lineales, f también lo es. □

Si $\{M_i : i \in I\}$ una familia de submódulos de un R-módulo M, la *suma* de los M_i es la imagen $\Sigma_{i\in I} M_i$ del morfismo canónico $\sigma : \bigoplus_{i\in I} M_i \to M$. Así, $\sum_{i\in I} M_i$ consiste de todas las sumas $\sum_{i\in F} m_i$ con $F \subset I$ finito y $m_i \in I$ para todo $i \in F$. Notemos que $\sum_{i\in I} M_i$ es el menor submódulo de M que contiene simultáneamente a todos los M_i. Cuando σ es un isomorfismo, escribimos $\bigoplus_{i\in I} M_i = \sum_{i\in I} M_i$.

Corolario 3.5.2. *La función*

$$\hom_R(N, \prod_{i\in I} M_i) \to \prod_{i\in I} \hom_R(N, M_i), \quad f \mapsto (\pi_i \circ f)_{i\in I}.$$

es un isomorfismo de $\mathrm{End}_R(N)$*-módulos.*

Demostración. La biyectividad de la función del corolario es simplemente otra manera de formular la Proposición 3.5.1. Si $g \in \mathrm{End}_R(N)$, la función envía $f \circ g$ en $(\pi_i \circ f \circ g)_{i\in I} = (g \cdot (\pi_i \circ f))_{i\in I} = g \cdot (\pi_i \circ f)_{i\in I}$ y es por tanto $\mathrm{End}_R(N)$-lineal. □

Corolario 3.5.3. *Sean R un anillo y $\{N_i \subset M_i : i \in I\}$ una familia de submódulos. Hay isomorfismos canónicos*

$$(\prod_{i\in I} M_i)/(\prod_{i\in I} N_i) \cong \prod_{i\in I} M_i/N_i$$
$$(\bigoplus_{i\in I} M_i)/(\bigoplus_{i\in I} N_i) \cong \bigoplus_{i\in I} M_i/N_i.$$

Demostración. Para cada $i \in I$, sea $p_i : M_i \to M_i/N_i$ la proyección. Entonces $f_j = p_j \circ \pi_j : \prod_{i\in I} M_i \to M_j/N_j$ $(j \in I)$ es una familia de morfismos. Por la Proposición 3.5.1 existe un único morfismo $f : \prod_{i\in I} M_i \to \prod_{i\in I} M_i/N_i$ tal que para cada $i \in I$, $\pi_i \circ f = f_i$. El morfismo f es suryectivo porque cada f_i lo es. Un elemento $x \in \prod_{i\in I} M_i$ está en $\mathrm{Ker}(f)$ si y sólo si $\forall i \in I$, $x_i = \pi_i(x) \in \mathrm{Ker}(p_i) = N_i$. Luego $\mathrm{Ker}(f) = \prod_{i\in I} N_i$, y el primer isomorfismo del corolario se sigue del Teorema 3.3.4. Para probar el segundo isomorfismo, consideremos la restricción g de f a $\bigoplus_{i\in I} M_i$. Es claro que $\mathrm{Im}(g) = \bigoplus_{i\in I} M_i/N_i$. Además

$$\mathrm{Ker}(g) = \mathrm{Ker}(f) \cap (\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} N_i.$$

El segundo isomorfismo se sigue ahora usando nuevamente el Teorema 3.3.4. □

Ejercicio 3.5.4. Sean I y J conjuntos y sea $\{M_{i,j} : (i,j) \in I \times J\}$ una familia de R-módulos. Probar que hay un isomorfismo canónico $\prod_{(i,j)\in I\times J} M_{i,j} \cong \prod_{i\in I} \prod_{j\in J} M_{i,j}$.

Lema 3.5.5. *Sean N un R-módulo e I un conjunto. La función*

$$\sigma : N^{(I)} \to N, \sigma(x) = \sum_{i \in I} x_i$$

es un morfismo R-lineal.

Demostración. La suma está bien definida pues cada elemento de $N^{(I)}$ tiene soporte finito. Luego σ es una función bien definida; que además es un morfismo R-lineal es inmediato. □

Proposición 3.5.6. *Sean R un anillo, N un R-módulo y $\{M_i : i \in I\}$ una familia de R-módulos. Entonces para cada familia de morfismos de R-módulos $\{f_i : M_i \to N | i \in I\}$ existe un único morfismo de R-módulos $f : \bigoplus_{i \in I} M_i \to N$ tal que para todo $j \in I$, $f \circ \iota_j = f_j$.*

Demostración. Notemos que si $m \in \bigoplus_{i \in I} M_i$ entonces

$$m = \sum_{i \in \text{sop}(m)} \iota_i(\pi_i(m)) = \sum_{i \in I} \iota_i(\pi_i(m))$$

Por tanto si f es un morfismo tal que para todo $j \in I$, $f \circ \iota_j = f_j$, entonces necesariamente

$$f(m) = \sum_{i \in I} f_i(\pi_i(m))). \tag{3.5.7}$$

Esto prueba que existe a lo sumo un morfismo que satisface las condiciones de la proposición. Resta ver que la fórmula (3.5.7) define un morfismo de R-módulos. Dado que π_i y f_i son morfismos R-lineales, $f_i \circ \pi_i$ también lo es. Luego por la Proposición 3.5.1, la familia $(f_i \circ \pi_i)_{i \in I}$ define un morfismo $\bar{f} : \bigoplus_{i \in I} M_i \to N^I$, $\bar{f}(m)_i = f_i(\pi_i(m))$. Como además para cada $m \in \bigoplus_{i \in I} M_i$ hay sólo un número finito de j tales que $f_j(\pi_j(m)) \neq 0$, la imagen de $\bar{f}$ cae dentro de $N^{(I)}$. La función f es morfismo R-lineal porque es la composición de la composición del morfismo σ del Lema 3.5.5 con la correstricción del morfismo $\bar{f}$ a $N^{(I)}$. □

Corolario 3.5.8. *La función*

$$\hom_R(\bigoplus_{i \in I} M_i, N) \to \prod_{i \in I} \hom_R(M_i, N), \quad f \mapsto (f \circ \iota_j)_{j \in I}$$

es un isomorfismo $\text{End}_R(N)$*-lineal.*

Demostración. La biyectividad de la función del corolario es otra forma de expresar el enunciado de la Proposición 3.5.6. Para cada $j \in I$, la función $f \mapsto f \circ \iota_j$ es morfismo de $\text{End}_R(N)$-módulos a izquierda. Luego la función del corolario también lo es, por la Proposición 3.5.1. □

Ejemplo 3.5.9. Sean M un R-módulo y X un conjunto. Por el Corolario 3.5.8 y el Ejemplo 3.1.16, la función

$$\text{ev} : \hom_R({}_R R^{(X)}, M) \to M^X, \quad \text{ev}(f)_x = f(\chi_x)$$

es un isomorfismo de $Z(R)$-módulos. De hecho por el Ejercicio 3.1.15,

$\hom_R({}_RR^{(X)}, M)$ es un R-módulo a izquierda y si $a \in R$ y $f \in \hom_R({}_RR^{(X)}, M)$, entonces

$$\operatorname{ev}(af)_x = f(\chi_x a) f(a\chi_x) = af(\chi_x) = a \operatorname{ev}(f)_x$$

Luego ev es un isomorfismo de R-módulos a izquierda.

Corolario 3.5.10. *Sean $\{M_j : j \in J\}$ y $\{N_i : i \in I\}$ familias de R-módulos. Entonces la aplicación*

$$\hom_R(\bigoplus_{j\in J} M_j, \prod_{i\in I} N_i) \to \prod_{(i,j)\in I\times J} \hom_R(M_j, N_i),$$
$$f \mapsto (\pi_i \circ f \circ \iota_j)_{(i,j)\in I\times J}$$

es un isomorfismo de $Z(R)$-módulos.

Demostración. Se sigue de los Corolarios 3.5.2 y 3.5.8, usando el Ejercicio 3.5.4. □

Ejemplo 3.5.11. Sean $P_1, \dots, P_n$ y $Q_1, \dots, Q_m$ R-módulos.
Sea $f \in \hom_R(\bigoplus_{j=1}^n P_j, \bigoplus_{i=1}^m Q_i)$. Por el Corolario 3.5.10, podemos identificar a f con la matriz

$$[f] = (f_{i,j})_{1\le i\le m, 1\le j\le n}, \quad f_{i,j} = \pi_i \circ f \circ \iota_j \in \hom_R(P_j, Q_i)$$

Si $S_1, \dots, S_l$ son R-módulos y $g \in \hom_R(\bigoplus_{i=1}^m Q_i, \bigoplus_{k=1}^l S_k)$, entonces para cada $1 \le k \le l$ y cada $1 \le j \le n$,

$$\begin{aligned}(g \circ f)_{k,j} =& p_k \circ g \circ f \circ \iota_j = p_k \circ \sum g \circ \mathrm{id}_Q \circ f \circ \iota_j \\ =& p_k \circ g \circ (\sum_i \iota_i p_i) \circ f \circ \iota_j = \sum_i g_{k,i} \circ f_{i,j}.\end{aligned}$$

En otras palabras, la matriz $[g \circ f]$ es el producto matricial de $[g]$ y $[f]$.

Ejemplo 3.5.12. Consideremos el caso particular del Ejemplo 3.5.11 en que todos los P_j, Q_i y S_k son iguales a R_R. Por el Ejemplo 3.1.17, la multiplicación a izquierda induce un morfismo $L : R \xrightarrow{\sim} \operatorname{End}_R(R_R)$. Luego $[f] \in M_{m\times n}R$, $[g] \in M_{l\times m}R$ y $[g \circ f] \in M_{l\times n}R$ es el producto usual de matrices. En particular, si identificamos $R_R^n = \hom_R(R_R, R_R^n)$, $[x]$ es un vector columna y $[f(x)] = [f][x]$. Si en cambio tomamos todos los P_j, Q_i y S_k iguales a ${}_RR$, entonces la multiplicación a derecha da un isomorfismo $\mu : R^{\mathrm{op}} \xrightarrow{\sim} \operatorname{End}_R({}_RR)$ y por tanto un isomorfismo $\hom_R({}_RR^n, {}_RR^m) \xrightarrow{\sim} M_{m\times n}R^{\mathrm{op}}$. Componiendo este isomorfismo con la transposición de matrices, obtenemos un isomorfismo $\hom_R({}_RR^n, {}_RR^m) \xrightarrow{\sim} M_{n\times m}R$. Un morfismo $f : R^n \to R^m$ de R-módulos a izquierda corresponde así a una matriz $[f] \in M_{n\times m}R$; el valor $f(x) \in R^m$ se obtiene multiplicando el vector fila $[x]$ por la matriz $[f]$. La composición $g \circ f$ corresponde al producto de matrices $[f][g]$.

Observación 3.5.13. Sean $\{M_i : i \in I\}$ y N como en el Corolario 3.5.8. Para cada $j \in I$, tenemos un morfismo de $Z(R)$-módulos

$$(\iota_j)_* : \hom_R(N, M_j) \to \hom_R(N, \bigoplus_{i\in I} M_i).$$

Luego por la Proposición 3.5.6, tenemos un morfismo de $\mathrm{End}_R(N)$-módulos

$$\iota : \bigoplus_{i\in I} \hom_R(N, M_i) \to \hom_R(N, \bigoplus_{i\in I} M_i), \iota(f)(n)_i = f_i(n). \tag{3.5.14}$$

Notemos que ι es inyectiva. Sin embargo no es suryectiva en general. Por ejemplo vimos ya que si k es un cuerpo y $\mathbb{V} = k^{(\mathbb{N})}$ entonces

$$\mathrm{End}_k(\mathbb{V}) = \{A \in M_{\mathbb{N}\times\mathbb{N}}k : (\forall j \in \mathbb{N}) \,|\, \mathrm{sop}(A_{*,j})| < \infty\}$$

Por otro lado

$$\bigoplus_{n\in\mathbb{N}} \hom_k(\mathbb{V}, k) = \{A \in M_{\mathbb{N}\times\mathbb{N}}k : (\exists N)(\forall j \in \mathbb{N})|\, \mathrm{sop}(A_{*,j})| \leq N\}.$$

Ejemplo 3.5.15. Sean R un anillo y $e \in R$ un idempotente, i.e. un elemento tal que $e^2 = e$. Entonces $(1-e)^2 = 1-e$ y las inclusiones $eR \subset R_R \supset (1-e)R$ inducen un morfismo $\alpha : eR \oplus (1-e)R \to R_R$. Es claro que α es suryectivo. Además si $(ea, (1-e)b) \in \mathrm{Ker}(\alpha)$ entonces $ea + (1-e)b = 0$ lo que, multiplicando por e y por $1-e$ y usando que $e(1-e) = 0$, nos da que $ea = (1-e)b = 0$. Luego α es un isomorfismo y por tanto, en vista del Corolario 3.5.3, tenemos que $R_R/(1-e)R \cong eR$. Se sigue entonces del Teorema 3.3.4 y del Ejemplo 3.1.16 que si M es un R módulo, entonces

$$\begin{aligned}\hom_R(eR, M) =& \hom_R(R/(1-e)R, M) = \{\phi \in \hom_R(R, M) | \phi((1-e)R) = 0\} \\ &\xrightarrow[\mathrm{ev}_1]{\sim} \{m \in M : m(1-e) = 0\} = Me.\end{aligned}$$

En particular, si $f \in R$,

$$\hom_R(eR, fR) \cong fRe. \tag{3.5.16}$$

Ejercicio 3.5.17. Sean R un anillo y $e, f, g \in R$ elementos idempotentes.

i) Probar que el isomorfismo (3.5.16) transforma la composición de morfismos en el producto de elementos, de modo que si $\alpha : eR \to fR$ y $\beta : fR \to gR$ corresponden a fxe y a gyf entonces $\beta\alpha$ corresponde a $gyfxe$.

ii) Probar que $eR \cong fR$ si y sólo si existen $x, y \in R$ tales que se satisfacen las identidades siguientes

$$x = fxe, \;\; y = eyf, \;\; yx = e, \;\; xy = f.$$

iii) Probar que si $z, w \in R$ satisfacen $wz = e$ y $zw = f$, entonces $x = fze$ y $y = ewf$ satisfacen las condiciones de ii).

Si existen x y y como en ii) (o equivalentemente, z y w como en iii)), decimos que e y f son *Murray-von Neumann equivalentes*, o simplemente *equivalentes*.

Lema 3.5.18. *Sean M un R-módulo y $M_1 \subset M \supset M_2$ submódulos. Sea $\jmath : M_1 \oplus M_2 \to M$ el morfismo inducido por las inclusiones. Son equivalentes*

i) $\jmath$ es un isomorfismo.

ii) Existe $e \in \mathrm{End}_R M$ idempotente tal que $\mathrm{Im}(e) = M_1$ y $\mathrm{Ker}(e) = M_2$.

Demostración. El morfismo $\jmath$ es un isomorfismo si y sólo si todo elemento $m \in M$ se escribe en forma única como $m = m_1 + m_2$ con $m_i \in M_i$. En ese caso, $e : M \to M$, $e(m) = m_1$ es un endomorfismo idempotente que satisface las condiciones de ii). Recíprocamente, si $e \in \mathrm{End}_R(M)$ es un idempotente que satisface ii) y $m \in M$, entonces

$$m = em + (\mathrm{id}_M - e)m, \quad em \in M_1 \text{ y } (\mathrm{id}_M - e)m \in M_2. \tag{3.5.19}$$

Además, $ex = x$ si y sólo si $x \in M_1$ y $ex = 0$ si y sólo si $(\mathrm{id}_M - e)x = x$. Por tanto si $m = m_1 + m_2$ con $m_i \in M_i$, $em = m_1$ y $(\mathrm{id}_M - e)m_2 = m_2$. Esto prueba que la escritura (3.5.19) es única, y por tanto $\jmath$ es un isomorfismo. □

Lema 3.5.20. *Sea* (3.4.5) *una sucesión exacta de R-módulos. Son equivalentes*

i) Existe $j \in \hom_R(M'', M)$ *tal que* $p \circ j = \mathrm{id}_{M''}$.

ii) Existe $q \in \hom_R(M, M')$ *tal que* $q \circ i = \mathrm{id}_{M'}$.

iii) Existe un isomorfismo $\phi : M' \oplus M'' \xrightarrow{\sim} M$ *tal que* $\forall m' \in M', m'' \in M''$, $\phi(m', 0) = i(m')$ *y* $p(\phi(m', m'')) = m''$.

Demostración. Sea j como en i). Sea $e = jp \in \mathrm{End}_R(M)$; por definición, $\mathrm{Im}(e) \subset \mathrm{Im}(j)$. Notemos además que que $ej = jpj = j$ y por tanto $\mathrm{Im}(e) = \mathrm{Im}(j)$. Además, como j es inyectiva, $0 = e(x) = j(p(x)) \iff p(x) = 0 \iff x \in \mathrm{Im}(i)$. Luego $\mathrm{Ker}(e) = \mathrm{Im}(i)$ y por el Lema 3.5.18,

$$M = \mathrm{Im}(i) \oplus \mathrm{Im}(j). \tag{3.5.21}$$

Como i es inyectiva, su correstricción a $\mathrm{Im}(i)$ es un isomorfismo; sea $i' : \mathrm{Im}(i) \to M'$ la inversa y pongamos $q = \imath' \circ (\mathrm{id}_M - e)$. Dado que $e \circ i = 0$, tenemos $(\mathrm{id}_M - e) \circ i = i$, y por tanto $q \circ i = \imath' i = \mathrm{id}_{M'}$. Hemos probado que $i) \Rightarrow ii)$. Además, como $i : M' \to \mathrm{Im}(i)$ y $j : M'' \to j(M'')$ son isomorfismos y $pj = \mathrm{id}_{M''}$, la identidad (3.5.18) muestra que $\phi : M' \oplus M'' \to M$, $\phi(m', m'') = i(m') + j(m'')$ es un isomorfismo. Luego i)⇒iii). Supongamos que vale iii); sean $\psi = \phi^{-1}$, $\pi : M' \oplus M'' \to M'$ la proyección y $q = \pi\psi$. Entonces para todo $m' \in M'$, $q(i(m')) = pi(m', 0) = m'$. Luego iii)⇒ ii). Si ahora q es como en ii), sea $f = iq$. Entonces $fi = i$ y $pf = 0$, lo que implica que $\mathrm{Im}(f) = \mathrm{Im}(i)$. Por otro lado como i es inyectiva, $\mathrm{Ker}(f) = \mathrm{Ker}(iq) = \mathrm{Ker}(q)$. Dado que $f^2 = f$, tenemos que $M = \mathrm{Im}(i) \oplus \mathrm{Ker}(q)$, por el Lema 3.5.18. Además $\mathrm{Ker}(\mathrm{id}_M - f) = \mathrm{Im}(f) = \mathrm{Im}(i)$, luego por el Teorema 3.3.4, existe un único morfismo $j : M'' \to M$ tal que $jp = \mathrm{id}_M - f$. Pero dado que $\mathrm{Im}(f) = \mathrm{Im}(i) = \mathrm{Ker}(p)$, tenemos que $pjp = p$, lo que, dado que p es suryectiva, prueba que $pj = \mathrm{id}_{M''}$. Luego ii)⇒i), lo que termina la demostración. □

Decimos que (3.4.5) *se parte* o *se escinde* si se satisfacen las condiciones equivalentes del Lema 3.5.20. En virtud del Lema 3.4.6 y de la Observación 3.4.7, las sucesiones exactas cortas que se parten permanecen exactas luego de aplicar $\hom_R(P, -)$ o $\hom_R(-, P)$ para cualquier R-módulo P.

Ejercicio 3.5.22. Sea (3.4.5) una sucesión exacta de R-módulos. Probar que son equivalentes:

i) (3.4.5) se parte.

ii) $\hom_R(N, p)$ es suryectiva para todo R-módulo N.

iii) $\hom_R(i, N)$ es suryectiva para todo R-módulo N.

Sea $f : M \to N$ un morfismo de R-módulos. Decimos que f es una *retracción* si existe un morfismo de R-módulos $g : N \to M$ tal que $fg = \mathrm{id}_N$. Decimos que f es una *sección* si existe un morfismo de R-módulos $h : N \to M$ tal que $hf = \mathrm{id}_M$. Decimos que M es un *sumando directo* (o un *retracto*) de N si existe una sección de M en N o equivalentemente, si existe una retracción de N en M.

Ejercicio 3.5.23. Sea $f : M \to N$ un morfismo de R-módulos.

i) Si f es retracción, entonces $M \cong \mathrm{Ker}(f) \oplus N$.

ii) Si f es sección, entonces $N \cong M \oplus N/\mathrm{Im}(f)$.

Ejemplo 3.5.24. Sean k un cuerpo, $\mathbb{V}$ un k-espacio vectorial y $\mathbb{V}_1 \subset \mathbb{V}$ un subespacio. Sea $T \in \mathrm{End}_k(\mathbb{V})$; consideremos a $\mathbb{V}$ como $k[x]$-módulo como en el Ejemplo 3.1.5 v). Entonces $\mathbb{V}_1 \subset \mathbb{V}$ es un $k[x]$ submódulo si y sólo si $T(\mathbb{V}_1) \subset \mathbb{V}_1$ y es un sumando directo si y sólo si existe un subespacio $\mathbb{V}_2 \subset \mathbb{V}$ tal que $\mathbb{V} = \mathbb{V}_1 \oplus \mathbb{V}_2$ y $T(\mathbb{V}_2) \subset \mathbb{V}_2$. Si $\mathbb{V}_1 \subset \mathbb{V}$ es un $k[x]$-submódulo y $\mathbb{V}_2$ es un subespacio (pero no necesariamente un $k[x]$-submódulo) tal que $\mathbb{V} = \mathbb{V}_1 \oplus \mathbb{V}_2$ y $\mathfrak{B}_i$ es una base de $\mathbb{V}_i$, entonces la matriz de T con respecto a la base $\mathfrak{B} = \mathfrak{B}_1 \cup \mathfrak{B}_2$ tiene la forma de bloques

$$[T]_{\mathfrak{B}} = \left[\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right].$$

Que $\mathbb{V}_2 \subset \mathbb{V}$ también sea un submódulo significa que $B = 0$. Del mismo modo, si $k \to Z(R) \to R$ es una k-álgebra y $\rho : R \to \mathrm{End}_k(\mathbb{V})$ es una estructura R-módulo en $\mathbb{V}$, que $\mathbb{V}_1$ y $\mathbb{V}_2$ sean ambos submódulos significa que para todo $a \in R$, en la matriz $[\rho(a)]_{\mathfrak{B}}$ del Ejemplo 3.1.5 ix), se tiene $Y_a = 0$.

3.6. Módulos libres, sistemas de generadores

Sean M un R-módulo y $X \subset M$ un subconjunto. Para cada $x \in X$ sea $h_x : {}_RR \to M$, $h_x(a) = ax$. Por la Proposición 3.5.6 existe un único morfismo de módulos $h = h_X : R^{(X)} \to M$ tal que para todo $x \in X$, $h(\chi_x) = x$. Decimos que X es *sistema de generadores* de M si h es suryectivo, que es *linealmente independiente* si h es inyectivo y que es una *base* si h es biyectivo. Un módulo se dice *libre* si admite una base. Un módulo es *finitamente generado* si tiene un sistema de generadores finito, o, equivalentemente, si para algún $n \geq 0$ existe un morfismo suryectivo $R^n \to M$.

Ejemplos 3.6.1. Sea R un anillo. El módulo 0 es libre, con base $\emptyset$; en efecto, $0 \cong R^{\emptyset}$. Si $X \neq \emptyset$, el cardinal de $R^{(X)}$ es mayor o igual que el de R. En particular, si R es infinito y M es un R-módulo de cardinal finito, entonces M no puede ser libre. En particular, ningún grupo abeliano finito no nulo es un $\mathbb{Z}$-módulo libre. Por otro lado, cualquier anillo es libre como módulo sobre sí mismo; en particular $\mathbb{Z}/n\mathbb{Z}$ es un $\mathbb{Z}/n\mathbb{Z}$-módulo libre. Si G es un grupo finito de orden n, entonces $nG = 0$ y por tanto G es un $\mathbb{Z}/n\mathbb{Z}$-módulo que puede o no ser libre como tal, pero que definitivamente no lo es como $\mathbb{Z}$-módulo. Por otro lado, el grupo $\mathbb{Q}$ tiene el mismo cardinal que $\mathbb{Z}$ y si $n \in \mathbb{Z}$ y $x \in \mathbb{Q}$ son

tales que $nx = 0$ entonces $n = 0$ o $x = 0$. Sin embargo, $\mathbb{Q}$ no es libre como $\mathbb{Z}$-módulo. En efecto, todo módulo libre no nulo L es isomorfo a $\mathbb{Z}^{(X)}$ para algún conjunto no vacío X y por tanto admite un morfismo suryectivo $L \to \mathbb{Z}$ (e.g. cualquiera de las proyecciones coordenadas π_x). Dado que $\hom_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$, deducimos que $\mathbb{Q}$ no es libre.

Observación 3.6.2. Todo R-módulo admite un sistema de generadores. En efecto, si M es un R-módulo, entonces $\pi : {}_RR^{(M)} \to M$, $\pi(\phi) = \sum_{m \in M} \phi(m)$ es un morfismo R-lineal tal que $\pi(\chi_m) = m$. En particular, π es suryectivo; en otras palabras, M es un sistema de generadores de M.

Proposición 3.6.3. *Sean $\{M_i : i \in I\}$ una familia de R-módulos y N un R-módulo. Supongamos que N es finitamente generado. Entonces la aplicación* (3.5.14) *es un isomorfismo de $\mathrm{End}_R(N)$-módulos.*

Demostración. Sólo debemos probar que el morfismo ι de (3.5.14) es suryectivo. Sea $f \in \hom_R(N, \bigoplus_{i \in I} M_i)$; para cada $i \in I$, sea $f_i = \pi_i \circ f$. Sean $X \subset N$ un sistema finito de generadores y $I \supset J = \bigcup_{x \in X} \mathrm{sop}(f(x))$. Si $i \in I \setminus J$, entonces $\pi_i \circ f(x) = 0$ para todo $x \in X$. Como h_X es suryectivo, esto implica que si $i \notin J$, entonces $\pi_i \circ f = 0$ (e.g. por el Lema 3.4.6). Luego $f = \sum_{j \in J} \iota_j \circ f_j$ es la imagen por ι del elemento $(f_i)_{i \in I} \in \bigoplus_{i \in I} \hom_R(N, M_i)$. □

Corolario 3.6.4. *Sean $\{M_i : i \in I\}$ una familia de R-módulos y $M = \bigoplus_{i \in I} M_i$. Son equivalentes*

i) M es finitamente generado.

ii) Existe $F \subset I$ finito tal que $j \in F \Rightarrow M_j$ es finitamente generado y $j \notin F \Rightarrow M_j = 0$.

Demostración. . El morfismo identidad $\mathrm{id}_M \in \mathrm{End}_R(M) = \prod_{i,j \in I} \hom_R(M_i, M_j)$ es una matriz de morfismos cuyo coeficiente (i, j) es $\delta_{i,j} \mathrm{id}_{M_i}$. Si M es finitamente generado, entonces por la Proposición 3.6.3, esa matriz tiene soporte finito. Luego existe F finito como en ii). Además cada M_i es finitamente generado pues es un cociente de M, que es finitamente generado por hipótesis. Esto prueba que i)⇒ii). Recíprocamente, si ii) se satisface, entonces $M \cong \bigoplus_{i \in F} M_i$ y para cada $i \in F$ hay un epimorfismo $p_i : {}_RR^{n_i} \to M_i$. Luego para $n = \sum_{i \in F} n_i$, $p = \bigoplus_{i \in F} p_i : R^n = \bigoplus_{i \in F} R^{n_i} \to M$ es un epimorfismo, y por tanto M es finitamente generado. □

Decimos que un anillo R tiene *noción de rango* si para $n, m \geq 1$, $R^n_R \cong R^m_R$ implica que $n = m$. En virtud del Ejemplo 3.5.12, R tiene noción de rango si y sólo si si $A \in M_{m \times n}R$ y $B \in M_{n \times m}R$ son tales que $AB = I_m$ y $BA = I_n$, entonces $m = n$. Esta condición es equivalente –otra vez por el Ejemplo 3.5.12– a que ${}_RR^n \cong {}_RR^m$ implica que $n = m$.

Ejemplos 3.6.5.

i) Todo cuerpo tiene noción de rango. Veremos más adelante que esto se aplica más generalmente a todo anillo de división.

ii) Sean k un cuerpo, $n \geq 2$ y $L_n(k)$ la k-álgebra de Leavitt. Se sigue de las ecuaciones 2.4.14 y 2.4.15 que $L_n(k)$ no tiene noción de rango.

Lema 3.6.6. *Sea $\phi : R \to S$ un morfismo de anillos. Si S tiene noción de rango entonces R también la tiene.*

Demostración. Supongamos que R no tiene noción de rango. Entonces existen $n \neq m \in \mathbb{N}$, $A \in M_{m\times n}R$ y $B \in M_{n\times m}R$ tales que $AB = I_m$ y $BA = I_n$. Sean $\phi(A) \in M_{m\times n}S$ y $\phi(B) \in M_{n\times n}S$ las matrices que resultan de aplicar ϕ coeficiente a coeficiente a las matrices A y B. Entonces $\phi(A)\phi(B) = \phi(AB) = I_m$, y $\phi(B)\phi(A) = I_n$, por lo que S no tiene noción de rango. □

Ejemplos 3.6.7.

i) Si R admite un morfismo en un cuerpo (o más generalmente en un anillo de división), entonces R tiene noción de rango, por el Lema 3.6.6. En particular todo anillo conmutativo tiene noción de rango. En efecto, por el Teorema 2.4.27 R tiene un ideal maximal $\mathfrak{M}$ y por la Proposición 2.4.17, $R/\mathfrak{M}$ es un cuerpo.

ii) Sean k un cuerpo y $\mathbb{V} = k^{(\mathbb{N})}$. Vimos en el Ejemplo 2.4.13 que existe un morfismo de anillos $\rho : L_n(k) \to \mathrm{End}_k(\mathbb{V})$. Luego $\mathrm{End}_k(\mathbb{V})$ no tiene noción de rango, por el Ejemplo 3.6.5 y el Lema 3.6.6.

Teorema 3.6.8. *Sean R un anillo y X, Y conjuntos tales que ${}_RR^{(X)} \cong {}_RR^{(Y)}$. Si X es infinito, entonces $|X| = |Y|$.*

Demostración. Sean $L = {}_RR^{(X)}$, $L' = {}_RR^{(Y)}$ y $\phi : L \to L'$ el isomorfismo del enunciado. Veamos que Y es infinito. Si no, $X \supset F = \bigcup_{y\in Y} \mathrm{sop}(\phi^{-1}(\chi_y))$ es finito, y por tanto existe $x \in X \setminus F$. Pero entonces χ_x no es combinación lineal de los $\phi^{-1}(\chi_y)$; esto es una contradicción, ya que ϕ^{-1} es un isomorfismo y los χ_y generan L'. Entonces Y es infinito. Sea $\mathcal{F}$ el conjunto de todos los subconjuntos finitos de Y; como Y es infinito, $|\mathcal{F}| = |Y|$. Sea $f : X \to \mathcal{F}$, $f(x) = \mathrm{sop}(\phi(\chi_x))$. Por el razonamiento de antes aplicado con X e Y intercambiados, vemos que el subconjunto $Y \supset \bigcup_{x\in X} f(x)$ no puede ser finito, de lo que se sigue que $\mathrm{Im}(f)$ es infinito. En particular,

$$|\mathrm{Im}(f) \times \mathbb{N}| = |\mathrm{Im}(f)| \leq |\mathcal{F}| = |Y| \tag{3.6.9}$$

Además si $F \in \mathrm{Im}(f)$ entonces para $T = \sum_{y\in F} R\chi_y$,

$$\phi^{-1}(T) = \sum_{y\in F} R\phi^{-1}(\chi_y) \subset \sum_{x\in\bigcup_{y\in T}\mathrm{sop}(\phi^{-1}(\chi_y))} R\chi_x$$

Luego

$$f^{-1}(\{F\}) = \{x \in X : \phi(\chi_x) \in T\} \subset \bigcup_{y\in T} \mathrm{sop}(\phi^{-1}(\chi_y))$$

es finito. Se sigue que

$$|X| = |\coprod_{F\in\mathrm{Im}(f)} f^{-1}\{F\}| \leq |\coprod_{F\in\mathrm{Im}(f)} \mathbb{N}| = |\mathrm{Im}(f) \times \mathbb{N}| \tag{3.6.10}$$

De (3.6.9) y (3.6.10) se sigue que $|X| \leq |Y|$. Intercambiando los roles de Y y X, obtenemos $|Y| \leq |X|$. Luego $|X| = |Y|$. □

3.7. Módulos sobre un producto de anillos

Sean $n \geq 1$ y $R_1, \ldots, R_n$ anillos. El grupo abeliano $R = \bigoplus_{i=1}^n R_i$ con el producto coordenada a coodenada es un anillo. Para cada $1 \leq i \leq n$, sea

$e_i \in R$, $(e_i)_j = \delta_{i,j}$. Notemos que

$$e_i \in Z(R),\ e_i e_j = \delta_{i,j} e_i,\ 1 = \sum_{i=1}^{n} e_i.$$

Sea M un R-módulo; como $e_i \in Z(R)$, $e_i M \subset M$ es un R-submódulo. Como $e_i e_j = \delta_{i,j} e_i$, $e_i m_j = \delta_{i,j} m_i$ para todo $m_i \in e_i M$. Sea $\sigma : \bigoplus_{i=1}^{n} e_i M \to M$ la aplicación canónica. Como $\sum_{i=1}^{n} e_i = 1$, σ es suryectiva. Además si $(m_1, \ldots, m_n) \in \mathrm{Ker}(\sigma)$,

$$0 = m_1 + \cdots + m_n \Rightarrow (\forall i),\ 0 = e_i(m_1 + \cdots + m_n) = m_i.$$

Luego σ es un isomorfismo, y por tanto $M = \bigoplus_{i=1}^{n} e_i M$. Notemos además que $(1 - e_i)e_i M = 0$ y por tanto $(1 - e_i)R$ está en el núcleo del morfismo de anillos $\rho_i : R \to \mathrm{End}_{\mathbb{Z}}(e_i M)$. Luego ρ_i induce un morfismo $R_i \cong R/(1-e)R \to \mathrm{End}_{\mathbb{Z}}(e_i M)$. En particular, $e_i M$ es un R_i-módulo. Por otra parte si $f : M \to N$ es un morfismo de R-módulos entonces $f(e_i M) = e_i f(M) \subset e_i$, y el morfismo inducido $f : e_i M \to e_i N$ es R_i-lineal. Luego para cada R-módulo M podemos asociar una n-upla

$$F(M) = (F(M)_1, \ldots, F(M)_n),\ F(M)_i = e_i M,$$

cuya i-ésima coordenada es un R_i-módulo y cada morfismo $f : M \to N$ induce una n-upla

$$F(f) = \left(f_{|e_1 M}, \ldots, f_{|e_n M}\right), f_{e_i M} \in \hom_{R_i}(e_i M, e_i N).$$

Recíprocamente, si $(M_1, \ldots, M_n)$ es una n-upla tal que cada M_i es un R_i-módulo, entonces podemos ver también a cada M_i como R-módulo vía la proyección $\pi_i : R \to R_i$ y formar su suma directa

$$G(M_1, \ldots, M_n) = \bigoplus_{i=1}^{n} {}_{\pi_i} M_i$$

Si $(N_1, \ldots, N_n)$ es otra n-upla tal que para cada i, N_i es un R_i-módulo y $f_i \in \hom_{R_i}(M_i, N_i)$, entonces $f_i \in \hom_R({}_{\pi_i} M, {}_{\pi_i} N)$ y

$$G(f_1, \ldots, f_n) = \bigoplus_{i=1}^{n} f_i \in \hom_R(G(M), G(N))$$

Proposición 3.7.1. *Sean $R_1, \ldots, R_n$ anillos, $R = \bigoplus_{i=1}^{n} R_i$, $\phi \in \hom_R(M, N)$ y $\psi_i \in \hom_{R_i}(M_i, N_i)$, $i = 1, \ldots, n$. Sean F y G como arriba. Entonces*

$$F(G(M_1, \ldots, M_n))_i = M_i\ (\forall 1 \leq i \leq n)\ y$$

$$\sigma_M : G(F(M)) \to M, \sigma(e_1 m_1, \ldots, e_n m_n) = \sum_{i=1}^{n} e_i m_i$$

es un isomorfismo. Además $F(G(f_1,\dots,f_n))_i = f_i$ $\forall 1 \leq i \leq n$ *y el siguiente diagrama conmuta.*

$$\begin{array}{ccc} G(F(M)) & \xrightarrow{\sigma_M} & M \\ \downarrow{\scriptstyle G(F(f))} & & \downarrow{\scriptstyle f} \\ G(F(N)) & \xrightarrow{\sigma_N} & N \end{array}$$

Demostración. Ejercicio. □

3.8. Módulos proyectivos e inyectivos

Sean R un anillo y M un R-módulo. Decimos que M es *proyectivo* si $\hom_R(M,-)$ preserva epimorfismos y que M es *inyectivo* si $\hom_R(-,M)$ manda monomorfismos en epimorfismos. En términos de diagramas, M es proyectivo si y sólo si para todo epimorfismo $p : N \to N''$ y todo morfismo $f : M \to N''$ existe un morfismo $\bar{f} : M \to N$ de modo que el siguiente diagrama conmuta

$$\begin{array}{ccc} & & M \\ & \swarrow^{\bar{f}} & \downarrow{\scriptstyle f} \\ N & \xrightarrow[p]{} & N'' \end{array} \tag{3.8.1}$$

Por otro lado M es inyectivo si y sólo si para todo monomorfismo $i : N' \to N$ y todo morfismo $g : N' \to M$ existe un morfismo $\bar{g} : N \to M$ de modo que el siguiente diagrama conmuta

$$\begin{array}{ccc} & & M \\ & \nearrow^{\bar{g}} & \uparrow{\scriptstyle g} \\ N & \xleftarrow{i} & N' \end{array} \tag{3.8.2}$$

Ejemplo 3.8.3. Todo R módulo libre es proyectivo. En efecto, si X es un conjunto y $f : M \twoheadrightarrow M''$ es un epimorfismo de R-módulos, entonces $f^X : M^X \to (M'')^X$, $f^X(\phi)_x = f(\phi_x)$ es un epimorfismo. Por el Ejemplo 3.5.9, esto implica que $\hom_R(R^{(X)},-)$ preserva epimorfismos.

Proposición 3.8.4. *Sean R un anillo y P un R-módulo. Son equivalentes*

i) P es proyectivo.

ii) Todo epimorfismo de R-módulos $M \to P$ es una retracción.

iii) Existen R-módulos Q y L tales que L es libre y $P \oplus Q \cong L$.

Demostración. Supongamos que P satisface i) y sea $p : M \to P$ es un epimorfismo. Aplicando (3.8.1) a $f = \mathrm{id}_P$, obtenemos que p es una retracción. Luego i)⇒ii). Se sigue de la Observación 3.6.2 que ii)⇒iii). Supongamos que P satisface iii). Sean $i : P \to L$ la composición de la inclusión $P \to P \oplus Q$ y el isomorfismo $P \oplus Q \cong L$ y $\pi : L \to P$ la composición del isomorfismo inverso $L \to P \oplus Q$ con la proyección $P \oplus Q \to P$. Notemos que $\pi \circ i = \mathrm{id}_P$. Sean $p : M \twoheadrightarrow M''$ un epimorfismo de R-módulos y $f \in \hom_R(P, M'')$. Por el Ejemplo 3.8.3 existe $g : L \to M$ tal que $pg = f\pi$. Entonces $\bar{f} = g \circ i$ satisface $p \circ \bar{f} = f \circ \pi \circ i = f$. Luego iii)⇒i). □

Ejemplo 3.8.5. Sea P un R-módulo. Por definición P es finitamente generado si y sólo si existen un R-módulo libre finitamente generado L y un morfismo suryectivo $\pi : L \to P$. Si P es proyectivo, entonces $P \oplus \mathrm{Ker}(\pi) \cong L$, por el Ejercicio 3.5.23. Luego por la Proposición 3.8.4, P es proyectivo y finitamente generado si y sólo si existe Q tal que $L = P \oplus Q$ es libre finitamente generado. Por el Lema 3.5.18 esto equivale a que exista $e \in \mathrm{Idem}(\mathrm{End}_R(L))$ tal que $\mathrm{Im}(e) = P$.

Sean R un anillo y $n \geq 1$. En lo que sigue, escribiremos

$$\mathrm{Idem}_n(R) = \mathrm{Idem}(M_n R).$$

Ejercicio 3.8.6. Sean R un anillo, $n, m \geq 1$ $e \in \mathrm{Idem}_n R$ y $f \in \mathrm{Idem}_m R$. Probar que los R-módulos a derecha eR^n y fR^m son isomorfos si y sólo si existen $A \in M_{m\times n}R$ y $B \in M_{n\times m}R$ tales que $fA = A = Ae$, $eB = Bf = B$, $AB = f$ y $BA = e$. Sugerencia: utilizar el Teorema 3.2.1 y el isomorfismo (3.5.16).

Ejercicio 3.8.7. Sea Q un R-módulo. Probar que son equivalentes

i) Q es inyectivo.

ii) Todo monomorfismo de R-módulos $Q \to M$ es una sección.

Ejercicio 3.8.8. Sea Q un R-módulo y sean Q_0, Q_1 submódulos tales que $Q = Q_0 \bigoplus Q_1$. Entonces Q es inyectivo si y sólo si Q_0 y Q_1 lo son.

Teorema 3.8.9. *Sean R un anillo y Q un R-módulo a izquierda. Son equivalentes*

i) Q es inyectivo.

ii) Para todo ideal a izquierda $\mathfrak{A} \subset R$ y todo morfismo de R-módulos $f : \mathfrak{A} \to Q$ existe $x \in Q$ tal que para todo $a \in \mathfrak{A}$, $f(a) = ax$.

Demostración. Por el Ejemplo 3.1.16, dar un elemento $x \in Q$ equivale a dar un morfismo de R-módulos $g : {}_RR \to Q$. La condición ii) equivale a pedir que todo $f \in \hom_R(\mathfrak{A}, Q)$ se extienda a un morfismo $h : {}_RR \to Q$. Por definición, Q es inyectivo si y sólo si toda vez $f : M' \to Q$ es un morfismo de R-módulos y $j : M' \subset M$ es un monomorfismo de R-módulos, entonces existe un morfismo $h : M \to Q$ de modo que $h \circ j = f$. Por tanto i)⇒ii). Recíprocamente, supongamos que que Q satisface ii). Sean $f : M' \to Q$ y $j : M' \to M$ morfismos de módulos, con j inyectivo; queremos probar que existe $h : M \to Q$ tal que $h \circ j = f$. Sea X el conjunto formado por todos los pares (N, g) donde $j(M') \subset N \subset M$ es un submódulo y $g : N \to Q$ es un morfismo R-lineal tal que $g \circ j = f$. Si (N_1, g_1) y $(N_2, g_2) \in X$, ponemos $(N_1, g_1) \leq (N_2, g_2)$ si $N_1 \subset N_2$ y $(g_2)_{|N_1} = g_1$. Notemos que $\leq$ es un orden parcial en X. Si $C \subset X$ es una cadena y $P = \bigcup_{(N,g)\in C} N$, entonces existe una única función $h : P \to Q$, tal que para todo $(N, g) \in C$, $h_{|N} = g$; es un ejericio verificar que h es un morfismo R-lineal. Luego por Zorn, X tiene un elemento maximal $(\mathfrak{M}, h)$. Queremos ver que $\mathfrak{M} = M$. Sean $x \in M \setminus \mathfrak{M}$ y $\mathfrak{N} = Rx + \mathfrak{M}$. Sea $I = \{a \in R : ax \in \mathcal{M}\}$; notemos que I es un ideal a izquierda. Además, por definición,

$$Rx \cap \mathfrak{M} = Ix.$$

Luego el morfismo

$$\mathfrak{M} \oplus Rx \to \mathfrak{N}, \quad (m, ax) \mapsto m - ax \tag{3.8.10}$$

es suryectivo con núcleo $\{(ax, ax)|a \in I\}$. Si $I = 0$, $\mathfrak{N} = Rx \oplus \mathfrak{M}$. Sea $p : \mathfrak{N} \to \mathfrak{M}$ la proyección, entonces $(\mathfrak{M}, h) \leq (\mathfrak{N}, h \circ p) \in X$, luego por maximalidad de $(\mathfrak{M}, h)$, $\mathfrak{N} = \mathfrak{M}$ y por tanto $x = 0$. Supongamos entonces que $I \neq 0$. Entonces por ii) aplicado al morfismo $I \to Q$, $a \mapsto h(ax)$, existe $q \in Q$ tal que para todo $a \in I$, $aq = h(ax)$. El morfismo $\xi : \mathfrak{M} \oplus Rx \to Q$, $\xi(m, bx) = h(m) - bq$ satisface $\xi(ax, ax) = 0$ para todo $a \in I$. Luego por el Teorema 3.3.4 aplicado al morfismo (3.8.10), existe un único morfismo $\bar{\xi} : \mathfrak{N} \to Q$ tal que $\bar{\xi}_{|\mathfrak{M}} = h$ y $\bar{\xi}(x) = q$. Pero entonces $(\mathfrak{N}, \bar{\xi}) \in X$, luego $x \in \mathfrak{M}$. □

Corolario 3.8.11. *Sean R un anillo conmutativo y Q un R-módulo. Consideremos los dos enunciados siguientes.*

i) Q es inyectivo.

ii) Para todo $x \in Q$ y todo $a \in R \setminus \{0\}$, existe $y \in Q$ tal que $x = ay$.

Si R es un dominio, entonces i)⇒ii). Si además R es principal, vale también que ii)⇒i).

Demostración. Sea $L_a : R \to R$ la multiplicación a izquierda por $a \in R$. En virtud del Ejemplo 3.1.16, la condición ii) equivale a decir que para todo morfismo $f : R \to Q$ y todo $a \in R \setminus \{0\}$, existe $g : R \to Q$ tal que $g \circ L_a = f$. Si R es un dominio y $a \neq 0$, L_a es inyectivo. Luego se sigue de la definición de módulo inyectivo que i)⇒ii). Notemos además que si R es dominio, $L_a : R \to aR$ es un isomorfismo. Por tanto pedir que Q satisfaga la condición ii) equivale a pedir que satisfaga la condición ii) del Teorema 3.8.9 para todo ideal principal $\mathfrak{A}$. Si R es principal, esos son todos los ideales, luego en ese caso ii)⇒i), por el Teorema 3.8.9. □

Un módulo Q sobre un dominio conmutativo R se dice *divisible* si satisface la condición ii) del Corolario 3.8.11.

Corolario 3.8.12. *Sean R un dominio principal, y $\{Q_i : i \in I\}$ una familia de R-módulos inyectivos. Entonces $\bigoplus_{i \in I} Q_i$ es inyectivo.*

Demostración. Se sigue del Corolario 3.8.11 y de que la condición ii) de dicho corolario se preserva por sumas directas. □

Corolario 3.8.13. *Sean R un dominio conmutativo y Q un R-módulo. Si $Q \neq 0$ es inyectivo, entonces* $\mathrm{Ann}_R\, Q = 0$.

Demostración. Supongamos que $\mathrm{Ann}_R\, Q$ contiene un elemento $d \neq 0$. Sea $x \in Q$; por el Corolario 3.8.11, existe $y \in Q$ tal que $x = dy = 0$. Luego $Q = 0$, que es una contradicción. □

Ejemplos 3.8.14.

i) Sean R un anillo conmutativo $f : Q \to M$ un epimorfismo de R-módulos. Notemos que si Q satisface la condición ii) del Corolario 3.8.11, M también la satisface. Si además R es un dominio principal, Q y M son inyectivos, por el Teorema. Así, por ejemplo, $\mathbb{Q}$, y más en general, cualquier $\mathbb{Q}$-espacio vectorial, es un $\mathbb{Z}$-módulo inyectivo, lo mismo que cualquier cociente de un $\mathbb{Q}$-espacio vectorial por un subgrupo. En particular, $\mathbb{Q}/\mathbb{Z} \cong G_\infty$ es inyectivo.

ii) Veamos que si p es primo, entonces $G_{p^\infty} = \bigcup_{n\geq 1} G_{p^n}$ es un $\mathbb{Z}$-módulo inyectivo. En efecto, sean $\omega \in G_{p^\infty}$, $p^n = \text{ord}(\omega)$, $m = p^r h$ con $r \geq 0$ y $(p : h) = 1$. Sea $\eta \in \mathbb{C}^*$ tal que $\eta^{p^r} = \omega$; entonces $\eta \in G_{p^{r+n}}$. Como $(p : h) = 1$, el endomorfismo de $G_{p^{r+n}}$ que manda $x \mapsto x^h$ es un automorfismo. En particular existe $\xi \in G_{p^{r+n}}$ tal que $\xi^h = \eta$ y por tanto $\xi^m = \omega$.

iii) Los $\mathbb{Z}$-módulos $\mathbb{R}_{>0}$, S^1 y $\mathbb{C}^*$ satisfacen la condición ii) del Corolario 3.8.11, y por tanto son inyectivos.

iv) Sea k un cuerpo. Por el Ejemplo 2.3.11, $k[x]$ es un dominio principal. Por el Corolario 3.8.11, el anillo $k(x) = \{f/g : f, g \in k[x], g \neq 0\}$ es un $k[x]$-módulo inyectivo y por el primer ejemplo de arriba, también lo es $k(x)/k[x]$.

3.9. Módulos simples, módulos indescomponibles

Sean R un anillo y M un R módulo. Decimos que M es *simple* si tiene exactamente dos submódulos; 0 y M. Decimos que un submódulo $S \subset M$ es *complementado* si existe un submódulo T tal que $S \oplus T = M$. Por ejemplo, 0 y M son complementados. Decimos que M es *indescomponible* si tiene exactamente dos submódulos complementados.

Observación 3.9.1. Un módulo a izquierda M sobre un anillo R es simple si y sólo si $M \neq 0$ y $Rm = M$ para todo $m \in M \setminus \{0\}$.

Ejemplos 3.9.2.

i) Un grupo abeliano es simple si y sólo si es isomorfo a $\mathbb{Z}/p\mathbb{Z}$ para algún primo p. Un grupo cíclico C de orden n es descomponible si y sólo si n se puede escribir como $n = n_1 n_2$ con $n_1, n_2 \geq 2$ y $(n_1 : n_2) = 1$. Luego C es indescomponible si y sólo si n una potencia de un primo.

ii) Sean $\mathbb{V} \neq 0$ un $\mathbb{C}$-espacio vectorial de dimensión finita y $T : \mathbb{V} \to \mathbb{V}$ es un endomorfismo $\mathbb{C}$-lineal. Consideremos a $\mathbb{V}$ como $k[x]$-espacio vectorial como en el Ejemplo 3.1.5 v). Entonces T tiene un autovector, v, y $kv \subset \mathbb{V}$ es un $k[x]$-submódulo no nulo. Se sigue que $\mathbb{V}$ es un $k[x]$-módulo simple si y sólo si $\dim_{\mathbb{C}} \mathbb{V} = 1$. Sea $\mathfrak{B} \subset \mathbb{V}$ una base tal que la matrix $A = [T]_{\mathfrak{B}}$ sea de Jordan. Entonces $\mathbb{V}$ es indescomponible si y sólo si A consiste de un solo bloque de Jordan

iii) Sea R un anillo. Entonces por la Observación 3.9.1, ${}_R R$ es simple si y sólo si todo elemento no nulo de R tiene inversa a izquierda y esto ocurre si y sólo si R es un anillo de división.

iv) Sean k un cuerpo, G un grupo y $n \geq 1$. Por el Ejemplo 3.1.13, dar una estructura de $k[G]$ módulo en k^n equivale a dar un morfismo de grupos $\rho : G \to \text{GL}_n(k)$. Con esta estructura, $k[G]$ es simple si y sólo si no hay subespacios $S \notin \{0, k^n\}$ que sean estables simultáneamente por todas las transformaciones $\rho(g)$ ($g \in G$). Esto sucede, por ejemplo, si $n = 1$. Las estructuras de $k[G]$-módulo en k corresponden a los morfismos $G \to \text{GL}_1(k) = k^*$, o lo que es lo mismo, a los morfismos $G_{\text{ab}} = G/[G, G] \to k^*$. Por lo visto en el Ejemplo 3.1.13, si $\rho, \mu \in \hom(G, k^*)$ entonces las estructuras de $k[G]$ módulo en k inducidas por ρ y μ son isomorfas si y sólo si $\rho = \mu$.

Sean R un anillo, M un R-módulo y $N \subsetneq M$ un submódulo. Decimos que N es *maximal* si N y M son los únicos submódulos de M que lo contienen.

Lema 3.9.3. *Sean R un anillo M un R-módulo y $N \subsetneq M$ un R-submódulo propio. Entonces M/N es simple si y sólo si N es maximal.*

Demostración. Inmediata de la definición de módulo simple y la Proposición 3.3.1. □

Corolario 3.9.4. *Un R-módulo a izquierda M es simple si y sólo si existen un ideal a izquierda maximal $\mathfrak{M} \subset R$ y un isomorfismo de R-módulos ${}_RR/\mathfrak{M} \cong M$.*

Demostración. Si $M \cong {}_RR/\mathfrak{M}$, M es simple por el Lema 3.9.3. Si M es simple, entonces es cíclico, por la Observación 3.9.1. Si $Rx = M$, entonces $\varepsilon_x : {}_RR \to M$, $a \mapsto ax$ es un morfismo suryectivo. Luego $M \cong {}_RR/\mathrm{Ker}(\varepsilon_x)$ y $\mathrm{Ker}(\varepsilon_x)$ es maximal, de nuevo por el Lema 3.9.3. □

Observación 3.9.5. La demostración del Corolario (3.9.4) nos dice que si M es simple, entonces para cada $x \in M \setminus 0$, el ideal a izquierda $\mathrm{Ann}_R(x)$ es maximal. Por lo visto en la Observación 3.1.6, si R es conmutativo, $\mathrm{Ann}_R(x) = \mathrm{Ann}_R(M)$. En general, $\mathrm{Ann}_R(M) = \bigcap_{y \in M} \mathrm{Ann}_R(y) \subset \mathrm{Ann}_R(x)$ y la inclusión puede ser estricta. Por ejemplo si $n \geq 1$ y D es de división el ideal a izquierda $I_1 \subset M_nD$ de la Observación 3.1.6 es simple (e.g. por el Teorema 3.2.1) y $\mathrm{Ann}_{M_nD}(I_1) = 0$ no es maximal si $n \geq 2$.

Observación 3.9.6. Sea R un dominio conmutativo, Q un R-módulo inyectivo e $I = \mathrm{Ann}_R(Q)$. Por el Corolario 3.8.13, $I = 0$. Si además Q es simple, entonces I es maximal, por el Corolario 3.9.4 y la Observación 3.9.5, y por tanto R es un cuerpo. En otras palabras si R es un dominio conmutativo que no es un cuerpo, entonces ningún R-módulo inyectivo puede ser simple.

Ejemplo 3.9.7. Sean R un dominio principal y M un R-módulo. Entonces por el Corolario 3.9.4 y el Ejemplo 2.4.18, M es simple si y sólo si existe $f \in R$ irreducible tal que $M \cong R/fR$.

Proposición 3.9.8. *Sean R un anillo y $M \neq 0$ un módulo finitamente generado y $S \subsetneq M$ un submódulo. Entonces M tiene un submódulo maximal N tal que $N \supset S$.*

Demostración. $\{x_1, \ldots, x_n\} \subset M$ un sistema de generadores finito. Por el Lema de Zorn, basta ver que si $\mathcal{C}$ es una cadena de submódulos propios de M que contienen a S entonces $L = \bigcup_{K \in \mathcal{C}} K \neq M$. Supongamos que $L = M$. Entonces $x_1, \ldots, x_n \in L$, y por tanto para cada $1 \leq i \leq n$ existe $K_i \in \mathcal{C}$ tal que $x_i \in K_i$; luego $L_0 = \bigcup_{i=1}^n K_i \in \mathcal{C}$ y es un submódulo que contiene a $\sum_{i=1}^n Rx_i = M$, lo que es absurdo, ya que $M \notin \mathcal{C}$. □

Corolario 3.9.9. *Existen un módulo simple S y un epimorfismo $f : M \twoheadrightarrow S$.*

Demostración. Se sigue de la Proposición 3.9.8 y del Lema 3.9.3 □

Observación 3.9.10. Decimos que un R-módulo es *noetheriano* si toda cadena de submódulos tiene un elemento máximo y que es *artiniano* si toda cadena de submódulos tiene un elemento mínimo. Un módulo tiene *longitud finita* si es a la vez noetheriano y artiniano. Notemos que un módulo noetheriano es necesariamente finitamente generado. Por ejemplo si k es un cuerpo,

$k \to Z(R) \subset R$ es una k-álgebra y M es un R-módulo tal que $\dim_k M < \infty$, entonces M tiene longitud finita. Si R es un anillo y M es un R-módulo de longitud finita, aplicando el corolario 3.9.9 iteradamente, obtenemos una cadena finita de submódulos $0 \subset M_n \subset M_{n-1} \subset \cdots \subset M_1 \subset M_0 = M$ tal que $S_i = M_i/M_{i+1}$ es simple para todo i. Si bien la cadena anterior no es única, el teorema de Jordan-Hölder ([1, Proposition 4.2.16]) dice que si $\{M'_i : 0 \leq i \leq n'\}$ es otra cadena con $S'_i = M'_i/M'_{i+1}$ simple, entonces $n' = n$ y existe una permutación $\sigma \in \mathbb{S}_n$ tal que para todo i $S_{\sigma(i)} \cong S'_i$. En forma similar, si M es de longitud finita, aplicando reiteradamente la definición de módulo descomponible, obtenemos una familia finita de módulos indescomponibles $I_1, \ldots, I_m$ tales que $M = I_1 \oplus \cdots \oplus I_m$. El teorema de Krull-Schmidt ([2, Sección 3.4]) nos dice que si $I'_1, \ldots, I'_{m'}$ es otra familia de submódulos indescomponibles tal que $M = I'_1 \oplus \cdots \oplus I'_{m'}$ entonces $m = m'$ y existe una permutación $\tau \in \mathbb{S}_m$ tal que para todo i, $M_{\sigma(i)} \cong M'_i$.

Lema 3.9.11. *[Lema de Schur] Sean R un anillo y $f : M \to N$ un morfismo de R módulos. Supongamos que M y N son simples. Si $f \neq 0$, entonces f es un isomorfismo.*

Demostración. Sean $K = \operatorname{Ker}(f)$ y $L = \operatorname{Im}(f)$. Entonces $f = 0 \iff K = M \iff L = 0$. Dado que M y N tienen exactamente dos submódulos cada uno, si $f \neq 0$, K tiene que ser 0 y L tiene que ser N. Luego f es un isomorfismo. □

Corolario 3.9.12. *Si M es simple, entonces $\operatorname{End}_R(M)$ es un anillo de división.*

Lema 3.9.13. *Sean R un anillo y M un R-módulo. Entonces M es indescomponible si y sólo si $\operatorname{Idem}(\operatorname{End}_R(M)) = \{0, 1\}$.*

Demostración. Inmediato del Lema 3.5.18. □

Observación 3.9.14. Se sigue del Lema 3.9.13 y de la Proposición 2.4.33 que si k es un cuerpo, $k \to Z(R) \to R$ es una k-álgebra y M es un R-módulo tal que $\dim_k M < \infty$, entonces M es indescomponible si y sólo si $\operatorname{End}_R M$ es local, y en ese caso, todo endomorfismo de M es o bien nilpotente o bien biyectivo.

3.10. Módulos semisimples

Lema 3.10.1. *Sean R un anillo, M un R-módulo y $\{S_i : i \in I\}$ una familia no vacía de submódulos simples de M tales que $\sum_{i \in I} S_i = M$. Entonces existe $J \subset I$ tal que $\bigoplus_{j \in J} S_j = M$.*

Demostración. Sea $X = \{K \subset I : \sum_{k \in K} S_k = \bigoplus_{k \in K} S_k\}$. Notemos que $\{i\} \in X$ para todo $i \in I$. En particular, $X \neq \emptyset$. Notemos que X está parcialmente ordenado por inclusión. Es un ejercicio verificar que la unión de una cadena de elementos de X está en X. Luego por Zorn, X tiene un elemento maximal J. Sea $N = \bigoplus_{j \in J} S_j$; queremos ver que $N = M$. Si no, tiene que existir $i \in I$ tal que S_i no está contenido en N; en particular, $i \notin J$. Como S_i es simple, se sigue que $N \cap S_i = 0$, y por tanto $S_i + N = S_i \oplus N$, por que que $J \cup \{i\} \in X$, absurdo. □

Proposición 3.10.2. *Sean R un anillo y M un R-módulo. Son equivalentes:*

i) Existe una familia $\{S_i : i \in I\}$ *de submódulos simples de* M *tal que* $\sum_{i\in I} S_i = M$.

ii) Existe una familia $\{S_j : j \in J\}$ *de submódulos simples de* M *tal que* $\bigoplus_{j\in J} S_j = M$.

iii) Para todo submódulo $N \subset M$ *existe un submódulo* $P \subset M$ *tal que* $N \oplus P = M$.

Demostración. Por el Lema 3.10.1, i)⇒ii). Es claro que ii)⇒i). Supongamos que ii) se satisface y sea $N \subset M$ un submódulo. Queremos probar iii); si $N \subsetneq M$, tomamos $P = 0$. Si no, sea $\pi : M \to Q = M/N$ la proyección; para cada i, la restricción de π a S_i es o bien 0, en cuyo caso $S_i \subset N$ o bien inyectiva (en cuyo caso $S_i \cap N = 0$). Sea $K = \{i \in I : S_i \cap N = 0\}$; como $N \subsetneq M$, $K \neq \emptyset$ y $Q = \sum_{k\in K} \pi(S_k)$. Por el Lema 3.10.1, existe $J \subset K$ tal que $Q = \bigoplus_{j\in J} \pi(S_j)$. Luego π restringido a $P = \bigoplus_{j\in J} S_j$ es un isomorfismo; sea f_1 su inversa; componiendo f_1 con la inclusión $P \subset M$, obtenemos un morfismo $f : Q \to M$ tal que $\pi f = \mathrm{id}_Q$. Luego $M = N \oplus P$, por Lema 3.5.20 (ver (3.5.21)). Luego ii)⇒iii). Resta probar que iii)⇒i). Sea M_0 la suma de todos los submódulos simples de M. Si iii) se satisface, existe N tal que $M_0 \oplus N = M$. Supongamos que $N \neq 0$; sea $0 \neq x \in N$. Por la Proposición 3.9.8, Rx posee un submódulo maximal $\mathfrak{M} \subset Rx$. Por iii) existe un submódulo $P \subset M$ tal que $\mathfrak{M} \oplus P = M$. Si $a \in R$ entonces $ax = \mathfrak{m} + p$ con $\mathfrak{m} \in \mathfrak{M}$, $p \in S := P \cap Rx$. Se sigue que $Rx = \mathfrak{M} \oplus S$, y por tanto $S \cong Rx/\mathfrak{M}$ es simple. Hemos probado que si $N \neq 0$ entonces contiene un submódulo simple; pero $N \cap M_0 = 0$ y M_0 contiene a todos los submódulos simples de M, luego $N = 0$ y $M = M_0$ satisface i). □

Decimos que un módulo M es *semisimple* si cumple las condiciones equivalentes de la Proposición 3.10.2.

Observación 3.10.3. Por definición, todo módulo simple es no nulo. Sin embargo el módulo 0 es semisimple, ya que es la suma de la familia vacía de módulos simples.

Corolario 3.10.4. *Si* M *es semisimple y* $N \subset M$ *es un submódulo, entonces* N *y* M/N *son semisimples, y la sucesión exacta*

$$0 \to N \to M \to M/N \to 0$$

se parte.

Demostración. Si $M = \sum_{i\in I} S_i$ con S_i simple y $\pi : M \to M/N$ es la proyección, $M/N = \sum_{i\in I} \pi(S_i)$. Como S_i es simple, $p(S_i)$ es simple o nulo. Luego M/N satisface la condición i) de la Proposición 3.10.2 y por tanto es semisimple. Además, como M satisface iii), existe un submódulo $P \subset M$ tal que $M = N \oplus P$. Luego $N \cong M/P$ es semisimple. □

Sea R un anillo y sea

$$\mathrm{Simp}(R) = \{{}_R R/\mathfrak{M} : \mathfrak{M} \text{ maximal}\}.$$

Sea $\cong$ la relación de isomorfismo entre R-módulos a izquierda y $\mathrm{Simp}(R)/\cong$ el conjunto cociente. Un *conjunto de representantes de* R*-módulos a izquierda simples* de R es un subconjunto $\mathcal{S} \subset \mathrm{Simp}(R)$ tal que la proyección al cociente induce una biyección $\mathcal{S} \to \mathrm{Simp}(R)/\cong$. Por el Corolario 3.9.4 para cada R-módulo a izquierda simple S existe un único ideal a izquierda maximal $\mathfrak{M} \subset R$ tal que $R/\mathfrak{M} \in \mathcal{S}$ y $S \cong R/\mathfrak{M}$.

Teorema 3.10.5. *Sean R un anillo, $\mathcal{S}$ un conjunto de representantes de R-módulos simples y M un R-módulo semisimple. Entonces para cada $S \in \mathcal{S}$ existe un conjunto $I(S)$ tal que $M \cong \bigoplus_{S\in\mathcal{S}} S^{I(S)}$. Si $M \cong \bigoplus_{S\in\mathcal{S}} S^{J(S)}$ entonces $|J(S)| = |I(S)|$ $\forall S \in \mathcal{S}$.*

Demostración. Como M es semisimple, existen un conjunto I y una familia de submódulos simples $S_i \subset M$ $i \in I$ tal que $M = \bigoplus_{i\in I} S_i$. Para cada $i \in I$ existe un único $f(S_i) \in \mathcal{S}$ tal que $S_i \cong f(S_i)$. Para cada $S \in \mathcal{S}$, sea $I(S) = f^{-1}(\{S\})$. Entonces

$$M = \bigoplus_{S\in S} \bigoplus_{i\in I(S)} S_i \cong \bigoplus_{S\in\mathcal{S}} S^{(I(S))}.$$

Notemos que, por el Lema de Schur (3.9.11) para cada $S \in \mathcal{S}$, $D(S) = \mathrm{End}_R(S)$ es un anillo de división; usando además la Proposición 3.6.3, tenemos un isomorfismo de $D(S)$-módulos

$$\hom_R(S, M) \cong D(S)^{I(S)}.$$

Del mismo modo, si $M \cong \bigoplus_{S\in\mathcal{S}} S^{(J(S))}$, tenemos que para cada $S \in \mathcal{S}$, $\hom_R(S, M) \cong D(S)^{(J(S))}$ como $D(S)$-módulos. Luego los $D(S)$-módulos $D(S)^{I(S)}$ y $D(S)^{J(S)}$ son isomorfos. Por el Teorema 3.6.8, $I(S)$ es infinito si y sólo si $J(S)$ lo es, y en ese caso $|I(S)| = |J(S)|$. Sea $D = D(S)$ y supongamos que $|I(S)| = n$ y $|J(S)| = m$; tenemos que ver que si $D^n \cong D^m$ entonces $n = m$. Por simetría, basta probar que si $\mathcal{B} = \{v_1, \ldots, v_m\} \subset D^n$ es una base, entonces $m \leq n$. Sea $\mathcal{E} = \{e_1, \ldots, e_n\}$ la base canónica de D^n; escribimos $v_m = \sum_{i=1}^n a_i e_i$. Sea j tal que $a_j \neq 0$; entonces $e_j = a_j^{-1} v_m - \sum_{i\neq j} a_j^{-1} a_i e_i$. Luego $\{e_1, \ldots, e_{j-1}, v_m, e_j, \ldots, e_n\}$ es un sistema de generadores de D^n. En particular, podemos escribir $v_{m-1} = bv_m + \sum_{i\neq j} b_i e_i$, y hay algún $k \neq j$ tal que $b_k \neq 0$, pues de lo contrario $\mathcal{B}$ no sería l.i. Como antes, multiplicando por b_k^{-1} y pasando de miembro obtenemos que los e_l con $l \notin \{j, k\}$ junto con v_m y v_{m-1}, forman un sistema de generadores de D^n. Iterando este proceso, llegamos a que $m \leq n$, ya que de lo contrario $\mathcal{B}$ no sería l.i. □

3.11. Anillos semisimples

Un anillo R se dice *semisimple* a derecha si R_R es semisimple y se dice semisimple a izquierda si ${}_R R$ lo es.

Teorema 3.11.1. *[Artin-Wedderburn] Sea R un anillo. Son equivalentes*

i) R es semisimple a derecha.

ii) Todo R-módulo a derecha es semisimple.

iii) Todo R-módulo a derecha es proyectivo.

iv) Todo R-módulo a derecha es inyectivo.

v) Toda sucesión exacta corta (3.4.5) de R-módulos a derecha se parte.

vi) Existen $r \geq 1$, $n_1, \ldots, n_r \geq 1$ y $D_1, \ldots, D_r$ anillos de división y un isomorfismo de anillos $R \cong \bigoplus_{i=1}^r M_{n_i} D_i$.

vii) R es semisimple a izquierda.

Demostración. i) $\iff$ ii): La dirección $\Leftarrow$ es clara. Veamos $\Rightarrow$; como R_R es semisimple, cada R-módulo a derecha libre lo es. Por la Observación 3.6.2 todo R-módulo a derecha es cociente de un libre a derecha, luego es semisimple por el Corolario 3.10.4.

ii) $\iff$ v) Inmediato del Corolario 3.10.4.

iii) $\iff$ iv) $\iff$ v) Inmediato del Ejercicio 3.5.22.

i)$\Rightarrow$vi) Por el Corolario 3.6.4 y el Teorema 3.10.5, existen finitos $S_1, \dots, S_r$ no isomorfos 2 a 2 y $n_1, \dots, n_r$ tales que $R_R = \bigoplus_{i=1}^r S_i^{n_i}$. Por el Ejemplo 3.1.17 y el Lema de Schur 3.9.11, $D_i = \operatorname{End}_R(S_i)$ es un anillo de división y hay un isomorfismo de anillos $R \cong \operatorname{End}_R(R_R) \cong \bigoplus_{i=1}^r M_{n_i} D_i$.

vi)$\Rightarrow$ i) Sea $S = \bigoplus_{i=1}^r M_{n_i} D_i$; basta ver que S cumple i). Por la Proposición 3.7.1 dar un S-módulo a derecha equivale a dar una r-upla $(M_1, \dots, M_r)$ con M_i un $M_{n_i} D_i$-módulo a derecha para cada i. Por el Teorema 3.2.1, todo $M_{n_i} D_i$-módulo es suma directa de copias de $T_i = (D_i)_{D_i}^{1 \times n_i}$, y éste es un $M_{n_i} D_i$-módulo a derecha simple. Luego todo S-módulo a derecha es suma directa de copias de $T_1, \dots, T_n$; en particular, S es semisimple a derecha.

vi) $\iff$ vii) Observemos que, por el Ejemplo 2.3.2 $R^{\mathrm{op}} \cong \bigoplus_{i=1}^r M_{n_i}(D_i^{\mathrm{op}})$. Además D_i^{op} es un anillo de división. Vemos así que vi) $\iff$ vii) se sigue de vi)$\Rightarrow$i) aplicado a R^{op}. □

Corolario 3.11.2. *Sea R un anillo semisimple. Entonces R es simple en el sentido de la Sección 2.3 si y sólo si existen un anillo de división D y $n \geq 1$ tales que $R \cong M_n D$.*

Demostración. Se sigue de vi) del Teorema 3.11.1 y del hecho de que si $A_1, \dots, A_r$ son anillos, entonces $A_i \lhd \bigoplus_{i=1}^r A_i$. □

Observación 3.11.3. Vemos en la demostración del Teorema 3.11.1 que si $R_R = S_1^{n_1} \oplus \cdots \oplus S_r^{n_i}$ con $n_1, \dots, n_r \geq 1$, $S_1, \dots, S_r$ simples y $S_i \ncong S_j$ si $i \neq j$, entonces $\{S_1, \dots, S_r\}$ es un conjunto completo de representantes de R-módulos a derecha simples y que si $D_i = \operatorname{End}_R(S_i)$, entonces $R \cong \bigoplus_{i=1}^r M_{n_i} D_i$. En particular un anillo semisimple tiene un número finito r de clases de isomorfismo de módulos simples, y más aún, por el Ejercicio 2.1.6, su centro es un producto de r cuerpos.

Proposición 3.11.4. *Sean k un cuerpo y $\iota : k \to Z(D) \subset D$ una k-álgebra que es anillo de división y tal que $\dim_k D < \infty$. Si k es algebraicamente cerrado, entonces $\dim_k D = 1$. En particular, $\iota(k) = Z(D) = D$.*

Demostración. Para cada $a \in D$ sea $L_a \in \operatorname{End}_k(D)$, $L_a(x) = ax$. Sea $f = \chi_a \in k[x]$ el polinomio característico de L_a. Notemos que $d = \dim_k D = \operatorname{gr}(f)$. Como k es algebraicamente cerrado, f se factoriza linealmente en $k[x]$ como $f = \prod_{i=1}^r (x - \lambda_i)^{\alpha_i}$ con $\alpha_i > 0$ para todo i y $d = \sum_{i=1}^r \alpha_i$. Pero para cada i, $L_a - \lambda_i \operatorname{id}_D = L_{a - \iota(\lambda_i)}$ tiene núcleo no trivial. Luego tiene que ser $1 = r$ y $a = \iota(\lambda_1)$; en particular $\iota(k) = D$ y por tanto $d = 1$. □

Proposición 3.11.5. *Sean k un cuerpo algebraicamente cerrado y $k \to Z(R) \subset R$ una k-álgebra de dimensión finita. Entonces R es semisimple si y sólo si existe un isomorfismo de k-álgebras $R \cong \bigoplus_{i=1}^r M_{n_i} k$. En ese caso R tiene exactamente $r = \dim_k Z(R)$ clases de isomorfismo de módulos simples.*

Demostración. Se sigue de la parte i) $\iff$ vi) del Teorema 3.11.1, la Proposición 3.11.4 y el Ejercicio 2.1.6. □

Teorema 3.11.6. *[Maschke] Sean k un cuerpo y G un grupo finito tal que $|G|$ es inversible en k. Entonces $k[G]$ es semisimple.*

Demostración. Probaremos que $k[G]$ cumple la condición ii) del Teorema 3.11.1. Para ello basta ver que todo $k[G]$-módulo M cumple la condición iii) de la Proposición 3.10.2. Sea $N \subset M$ un $k[G]$-módulo; como k es semisimple, existe $\pi \in \mathrm{End}_k M$ idempotente tal que $\mathrm{Im}(\pi) = N$. Sea $\rho : k[G] \to \mathrm{End}_k(M)$, $\rho(a)(m) = a \cdot m$. Para cada $g \in G$, $\rho(g) \in \mathrm{Aut}_k(M)$, y $\mathrm{ad}(\rho(g)) \in \mathrm{Aut}_k(\mathrm{End}_k(M))$. El morfismo $\mu : G \to \mathrm{Aut}_k(\mathrm{End}_k(M))$, $g \mapsto \mathrm{ad}(\rho(g))$ induce una estructura de $k[G]$-módulo en $\mathrm{End}_k(M)$, tal que si $g \in G$ y $f \in \mathrm{End}_k(M)$, $(g \cdot f)(m) = g(f(g^{-1}m))$. Notemos que un endomorfismo k-lineal $f : M \to M$ es $k[G]$-lineal si y sólo si $g \cdot f = f$ para todo $g \in G$. Sea $q \in \mathrm{Idem}(k[G])$ como en el Ejemplo 2.1.15, entonces $q^2 = q$ y $gq = q$ $\forall g \in G$. Luego $q \cdot f \in \mathrm{End}_{k[G]}(M)$ para todo $f \in \mathrm{End}_k(k[G])$. En particular, $e = q \cdot \pi$ es $k[G]$-lineal. Además si $m \in M$,

$$e(m) = (1/|G|) \sum_{g \in G} g(\pi(g^{-1}m)) \in k[G]N = N.$$

Luego $\mathrm{Im}(e) \subset N$. Por otro lado, si $m \in N$, $g^{-1}m \in N$ y por tanto $g\pi(g^{-1}m) = g(g^{-1}m) = m$, de lo que se sigue que $e(m) = m$. Esto prueba que e es idempotente y que $\mathrm{Im}(e) = N$; luego $M = N \oplus \mathrm{Ker}(e)$ y $\mathrm{Ker}(e)$ es un $k[G]$-submódulo pues e es $k[G]$-lineal. □

En la proposición siguiente, relacionamos el centro de $k[G]$ con las clases de conjugación de G, definidas en el Ejemplo 1.7.10.

Proposición 3.11.7. *Sean k un anillo conmutativo y G un grupo finito. Sean $C_1, \dots, C_r$ las clases de conjugación de G. Sea $v_i = \sum_{g \in C_i} g \in k[G]$. Entonces $Z(k[G]) = \bigoplus_{i=1}^r kv_i$.*

Demostración. Notemos que como $\mathrm{sop}(v_i) = C_i$ y $C_i \cap C_j = \emptyset$ para $i \neq j$, $\{v_1, \dots, v_r\}$ es l.i., y por tanto $Z := \sum_{i=1}^r kv_i = \bigoplus_{i=1}^r kv_i$. Además un elemento $x = \sum_{h \in G} \lambda_h h$ está en $Z(k[G])$ si y sólo si conmuta con todos los elementos de G, o lo que es lo mismo, si y sólo si $gxg^{-1} = x$ para todo $g \in G$. Pero

$$\sum_{h \in G} \lambda_h ghg^{-1} = \sum_{h \in G} \lambda_{g^{-1}hg} h$$

Luego $gxg^{-1} = x$ para todo $g \in G$ si y sólo si $\lambda_{ghg^{-1}} = \lambda_h$ para todo $g, h \in G$, y esto equivale a que $x \in Z$. Luego $Z = Z(k[G])$, como queríamos demostrar. □

Corolario 3.11.8. *Sea k un cuerpo algebraicamente cerrado y G un grupo finito tal que $|G|$ es inversible en k. Entonces el número de clases de isomorfismo de $k[G]$-módulos simples es igual al número de clases de conjugación de G.*

Ejemplo 3.11.9. Sea G un grupo finito. Si G es abeliano, entonces tiene $|G|$ clases de conjugación y $\mathbb{C}[G]$ es conmutativo. Luego $\mathbb{C}[G] \cong \mathbb{C}^{|G|}$. Bajo este isomorfismo, las $|G|$ clases de módulos simples están representadas por las $|G|$ proyecciones coordenadas $\mathbb{C}^{|G|} \to \mathbb{C}$. Como vimos en el Ejemplo 3.9.2 iv), para G no necesariamente conmutativo, las clases de isomorfismo de $\mathbb{C}[G]$-módulos de dimensión 1 sobre $\mathbb{C}$ corresponden a los morfismos $G_{\mathrm{ab}} \to \mathbb{C}^*$,

o lo que es lo mismo, a $\mathbb{C}[G_{\text{ab}}]$-módulos de dimensión 1. Es decir que, por lo que acabamos de ver, el número de tales módulos es $|G_{\text{ab}}|$. Por otro lado, sabemos del Ejemplo 3.9.2 iv) que los módulos correspondientes a dos morfimos $\rho, \mu : G_{\text{ab}} \to \mathbb{C}^*$ son isomorfos si y sólo si son iguales. Luego $|G_{\text{ab}}| = |\hom_{\mathbb{Z}}(G_{\text{ab}}, \mathbb{C}^*)|$. Notemos además, que como G es finito, la imagen de cualquier morfismo $G_{\text{ab}} \to \mathbb{C}^*$ cae en G_∞, luego también se tiene $|\hom_{\mathbb{Z}}(G_{\text{ab}}, G_\infty)| = |G_{\text{ab}}|$.

Ejemplo 3.11.10. Sea $D_4 = \{R^j S^k : 0 \leq j \leq 3,\ 0 \leq k \leq 1\}$ el grupo diedral. Las clases de conjugación de D_4 son 5: $\{1\}$, $\{R^2\}$, $\{S, R^2S\}$, $\{R, R^3\}$, $\{SR, SR^3\}$. Luego las clases de isomorfismo de $\mathbb{C}[D_4]$-módulos simples son 5, por el Corolario 3.11.8. En virtud del Ejemplo 3.11.9 y dado que $(D_4)_{\text{ab}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, 4 de aquéllas 5 clases corresponden a módulos de dimensión 1 sobre $\mathbb{C}$. Por otra parte, la inclusión $D_4 \subset O_2 \subset U_2 \subset \mathrm{GL}_2(\mathbb{C})$ nos da un $\mathbb{C}[D_4]$-módulo M de dimensión 2. Veamos que M es simple, y por tanto completa una lista de representantes de $\mathbb{C}[D_4]$-módulos simples. Si no lo fuera, habría un subespacio de dimensión 1 de $\mathbb{C}^2$ estable simultáneamente por R y S, es decir, un autovector común a ambos. Recordemos que

$$R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Las 2 rectas estables por R son $\mathbb{C}(i, 1)$ y $\mathbb{C}(-i, 1)$; las estables por S son $\mathbb{C}(1, 1)$ y $\mathbb{C}(1, -1)$. Luego R y S no tienen autovectores comunes, y por tanto M es simple.

Capítulo 4

Dominios principales

En este capítulo R será frecuentemente un dominio de ideales principales, que abreviaremos DIP.

4.1. Módulos libres, torsión

Teorema 4.1.1. *Sean R un DIP, $n \geq 1$, L un R-módulo libre de rango n y $M \subset L$ un R-submódulo. Entonces M es libre de rango $\leq n$.*

Demostración. Sea $\mathfrak{B} = \{x_1, \ldots, x_n\}$ base de L y sean $L_i = \langle x_1, \ldots, x_i \rangle$ y $M_i = M \cap L_i$. Notemos que $M_n = M$. Tenemos $M_1 \subset Rx_1$; sea $\phi : Rx_1 \xrightarrow{\sim} R$, $\phi(ax_1) = a$; como R es DIP, existe $f \in R$ tal que $\phi(M_1) = fR$. Luego M_1 es libre de rango ≤ 1. Supongamos inductivamente que $n \geq i > 1$ y que M_{i-1} es libre de rango $\leq i-1$. Consideremos la i-ésima función coordenada $\phi : L \to R$, $\phi(\sum_{j=1}^{n} a_j x_j) = a_i$. Sea $I = \phi(M_i)$; como ϕ es morfismo de módulos, $I \lhd R$. Como R es DIP, hay $f \in R$ tal que $I = fR$, luego I es libre de rango ≤ 1 y por tanto proyectivo. Entonces la sucesión exacta

$$0 \to M_{i-1} \to M_i \to I \to 0$$

se parte, luego $M_i \cong M_{i-1} \oplus I$ es libre de rango $\leq i - 1 + 1 = i$. □

Observación 4.1.2. Recordemos que un módulo M sobre un anillo R se dice noetheriano si todo submódulo de M es finitamente generado, o equivalentemente si toda cadena de submódulos tiene un elemento máximo. Un anillo R se dice noetheriano (a izquierda) si todo R-módulo (a izquierda) finitamente generado es noetheriano. Si

$$0 \to M' \to M \to M''' \to 0$$

es una sucesión exacta de R-módulos, entonces M es noetheriano si y sólo si M' y M'' lo son. En particular la suma directa de finitos R-módulos noetherianos es de nuevo noetheriano. Dado que cada cociente de un módulo noetheriano es noetheriano y que todo módulo finitamente generado es cociente de un módulo libre finitamente generado, se sigue que R es noetheriano a izquierda si y sólo si ${}_R R$ es noetheriano. En particular, un DIP es un anillo noetheriano.

Sean R un anillo, M un R-módulo a izquierda y $x \in M$. El *anulador* de x es

$$\mathrm{Ann}_R(x) = \{a \in R : ax = 0\}$$

Notemos que $\mathrm{Ann}_R(x) \subset R$ es un ideal a izquierda. Decimos que x es *de torsión* si $\mathrm{Ann}_R(x) \neq 0$. Supongamos ahora que R es un dominio conmutativo. En este caso definimos la *torsión* de M como

$$\mathrm{tors}(M) = \{x \in M | \, \mathrm{Ann}_R(x) \neq 0\}.$$

Es claro que $0 \in \mathrm{tors}(M)$. Como R es conmutativo, si $x \in M$ y $c \in R$, $\mathrm{Ann}_R(cx) \supset \mathrm{Ann}_R(x)$. Luego $\mathrm{tors}(M)$ es cerrado bajo producto por elementos de R. Como además R es dominio, si $x, y \in \mathrm{tors}(M)$ y $a \in \mathrm{Ann}_R(x)$, $b \in \mathrm{Ann}_R(y)$ son no nulos, entonces $0 \neq ab \in \mathrm{Ann}_R(x+y)$, luego $\mathrm{tors}(M)$ también es cerrado por sumas. Luego $\mathrm{tors}(M)$ es un R-submódulo de M.

Decimos que M es *de torsión* si $\mathrm{tors}(M) = M$ y que es *libre de torsión* si $\mathrm{tors}(M) = 0$.

Observación 4.1.3. Sean R un dominio conmutativo, M un R-módulo y $\{x_i : i \in I\} \subset M$ un sistema de generadores. Un elemento $a \in R$ está en $\mathrm{Ann}_R(M)$ si y sólo si $ax_i = 0$ para todo $i \in I$. Por tanto

$$\mathrm{Ann}_R(M) = \bigcap_{i \in I} \mathrm{Ann}_R(x_i).$$

En particular,

$$\mathrm{Ann}_R(x) = \mathrm{Ann}_R(Rx).$$

Lema 4.1.4. *Sean R un dominio conmutativo y M un módulo finitamente generado. Entonces M es de torsión si y sólo si $\mathrm{Ann}_R(M) \neq 0$.*

Demostración. Como $\mathrm{Ann}_R(M) \subset \mathrm{Ann}_R(x)$ para todo $x \in M$, si el anulador es no nulo, M es de torsión. Recíprocamente, supongamos que M es de torsión. Sea $\{x_1, \ldots, x_n\}$ un sistema de generadores de M. Para cada $1 \leq i \leq n$, sea $0 \neq a_i \in \mathrm{Ann}_R(x_i)$; entonces $0 \neq a = a_1 \cdots a_n \in \bigcap_{i=1}^n \mathrm{Ann}_R(x_i) = \mathrm{Ann}_R(M)$. □

Ejercicio 4.1.5. Sean R un dominio conmutativo y $\{M_i : i \in I\}$ una familia de R-módulos.

i) Probar que $\mathrm{tors}(\bigoplus_{i \in I} M_i) = \bigoplus_{i \in I} \mathrm{tors}(M_i)$.

ii) Sea $p > 0$ un número primo. Probar que el grupo abeliano $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ no es de torsión.

Lema 4.1.6. *Sean R un dominio conmutativo y M un R-módulo. Entonces*

$$M_{\mathrm{tf}} := M/\,\mathrm{tors}(M)$$

es libre de torsión.

Demostración. Sea $\pi : M \to M_{\mathrm{tf}}$ la proyección. Sea $y \in M_{\mathrm{tf}}$; como π es suryectiva existe $x \in M$ tal que $y = \pi(x)$. El elemento y es de torsión si y sólo si existe $a \in R \setminus \{0\}$ tal que $0 = \pi(ax)$, es decir, hay $a \in R \setminus \{0\}$ tal que $ax \in \mathrm{tors}(M)$. Pero entonces hay $b \in R \setminus \{0\}$ tal que $0 = b(ax) = (ba)x$; luego $0 \neq ba \in \mathrm{Ann}_R(x)$ y por tanto $x \in \mathrm{tors}(M)$, lo que implica que $y = 0$. □

Teorema 4.1.7. *Sean R un DIP y M un R-módulo finitamente generado. Entonces M es libre de torsión si y sólo si M es libre.*

Demostración. Como R es dominio, $\operatorname{tors}(R) = 0$ y por tanto cualquier R módulo libre es libre de torsión por el Ejercicio 4.1.5. Supongamos ahora que M es finitamente generado y libre de torsión. Sea $Y = \{y_1, \dots, y_n\} \subset M$ un sistema finito de generadores. Entonces el conjunto $\mathfrak{Y}$ de todos los subconjuntos l.i. de Y es no vacío (pues $\emptyset \in \mathfrak{Y}$), y como Y es finito, $\mathfrak{Y}$ tiene un elemento maximal $\mathfrak{B}$. Sea $N = \langle \mathfrak{B} \rangle$; si $N = M$, M es libre. Supongamos que no; entonces $\mathfrak{B} \subsetneq Y$. Sin pérdida de la generalidad, $\mathfrak{B} = \{y_1, \dots, y_m\}$ para algún $1 \leq m < n$. Para cada $m < i \leq n$, $\mathfrak{B} \cup \{y_i\}$ es l.d. y por tanto existe $a_i \in R \setminus \{0\}$ tal que $a_i y_i \in N$. Sea $a = \prod_{i=m+1}^{n} a_i$; entonces $aM \subset N$ es libre por el Teorema 4.1.1. Como M es libre de torsión y $a \neq 0$, $M \to aM$, $x \mapsto ax$ es un isomorfismo. Luego M es libre. □

Observación 4.1.8. La demostración del Teorema 4.1.7 muestra que si M es libre de torsión y $Y = \{y_1, \dots, y_n\} \subset M$ es un sistema de generadores, entonces M es libre y su rango es igual al número de elementos de cualquier subconjunto l.i. maximal de Y. En particular, este número no depende del subconjunto l.i. maximal de Y elegido. Lo que no prueba la demostración es que un tal subconjunto de Y sea una base de M. Por ejemplo, $Y = \{6, 10, 15\}$ es un sistema de generadores de $\mathbb{Z}$; cada uno de sus elementos forma un subconjunto l.i. maximal, pero ninguno de ellos genera todo $\mathbb{Z}$.

Corolario 4.1.9. *Si R es un DIP y M es un R-módulo finitamente generado, entonces existe $n \geq 0$ tal que $M \cong \operatorname{tors}(M) \oplus R^n$.*

Demostración. Por el Teorema 4.1.7, M_{tf} es libre y finitamente generado. Luego existe $n \geq 0$ tal que $M_{\text{tf}} \cong R^n$, y por tanto $M \cong \operatorname{tors}(M) \oplus R^n$. □

Ejercicio 4.1.10. Sean R un dominio conmutativo, M_1, M_2 módulos de torsión y $n_1, n_2 \geq 1$. Probar que $M_1 \oplus R^{n_1} \cong M_2 \oplus R^{n_2}$ si y sólo si $M_1 \cong M_2$ y $n_1 = n_2$.

4.2. Factorización en dominios principales

Sean R un dominio conmutativo y $a \in R \setminus (R^* \cup \{0\})$. Una *factorización irreducible* de a consiste de enteros $r \geq 1$, $n_1, \dots, n_r \geq 1$ y elementos $u \in R^*$ y $p_1, \dots, p_r \in R$ irreducibles tales que $p_i R \neq p_j R$ si $i \neq j$ y de modo que

$$a = u p_1^{n_1} \cdots p_r^{n_r}.$$

Decimos que otra factorización irreducible $a = v q_1^{m_1} \cdots q_s^{m_s}$ es *equivalente* a la anterior si $s = r$ y existe una permutación $\sigma \in \mathfrak{S}_r$ tal que para todo i, $q_i = p_{\sigma(i)}$ y $m_i = n_{\sigma(i)}$.

Observación 4.2.1. Sean R un dominio, $v \in R^*$, $f_1, \dots, f_n$ elementos irreducibles y $a = v f_1 \cdots f_n$. Veamos a posee una factorización irreducible. Sea $P \subset \{f_1, \dots, f_n\}$ suconjunto maximal entre los que verifican que si $p, q \in P$ entonces $Rp \neq Rq$. Sea $r = |P|$; sin pérdida de la generalidad, podemos suponer que $P = \{f_1, \dots, f_r\}$. Si $1 \leq i \leq n$, $f_i = u_i f_{\alpha(i)}$ para un único $1 \leq \alpha(i) \leq r$. Para cada $1 \leq i \leq r$, sea $n_i = |\alpha^{-1}\{i\}|$; sea $u = v \cdot \prod_{i=1}^{n} u_i$. Entonces $a = u f_1^{n_1} \cdots f_r^{n_r}$ es una factorización irreducible de a.

Proposición 4.2.2. *Sean R un dominio conmutativo noetheriano y $a \in R \setminus (\{0\} \cup R^*)$. Entonces a admite una factorización irreducible.*

Demostración. Por la Observación 4.2.1 basta ver que todo elemento $a \in S = R \setminus (\{0\} \cup R^*)$ se factoriza como producto de irreducibles. Sea $F \subset S$ el subconjunto de todos los elementos que admiten una tal factorización. Notemos que

$$a, b \in F \Rightarrow ab \in F. \tag{4.2.3}$$

Supongamos $F \neq S$. Sea $a \in S \setminus F$. Entonces a no es irreducible, y por tanto existe una factorización $a = a_1 b_1$ con $a_1, a_2 \in S$. Por (4.2.3) alguno de a_1 o b_1 no está en F; si pérdida de generalidad podemos suponer $a_1 \notin F$. Luego podemos factorizarlo como $a_1 = a_2 b_2$ con $a_2, b_2 \in S$ y $a_2 \notin F$; procediendo de esta forma obtenemos una sucesión de elementos $a_1, a_2, \ldots$ tales que para todo i, $a_i R \subsetneq a_{i+1} R \subsetneq R$. Esto contradice la hipótesis de que R es noetheriano; por tanto $F = S$, lo que termina la demostración. □

Un dominio noetheriano R se dice *de factorización única* (DFU) si todo $a \in R \setminus (R^* \cup \{0\})$ admite una única factorización irreducible a menos de equivalencia.

Teorema 4.2.4. *Sea R un DIP. Entonces R es DFU.*

Demostración. Como por la Observación 4.1.2 R es noetheriano, todo elemento de $S = R \setminus (\{0\} \cup R^*)$ admite una factorización irreducible, por la Proposición 4.2.2. Sea, para cada $n \geq 1$, $S_n \subset S$ el subconjunto de todos los elementos que admiten una factorización irreducible $a = u p_1^{n_1} \cdots p_r^{n_r}$ con $n = \sum_{i=1}^r n_i$; por la observación anterior, $S = \bigcup_{n \geq 1} S_n$. Probaremos por inducción en n que el teorema es válido para todos los elementos de S_n. Por el Ejemplo 2.4.18 un elemento $f \in R$ es irreducible si y sólo si el ideal fR es maximal; en particular fR es primo. Luego $f \backslash gh$ implica que $f \backslash g$ o $f \backslash h$. Se sigue que el teorema es cierto para los elementos de S_1. Para el paso inductivo, supongamos $n > 1$ y que el teorema es cierto para los elementos de S_{n-1}. Sea $a \in S_n$, $a = u p_1^{n_1} \cdots p_r^{n_r}$ una factorización irreducible con $\sum_{i=1}^r n_i = n$ y sea

$$a = v q_1^{m_1} \cdots v q_s^{m_s} \tag{4.2.5}$$

otra factorización irreducible. Como p_r es irreducible y divide a a, existe i tal que $p_r \backslash q_i$. Como $p_r R$ es maximal, $p_r R = q_i R$ y por tanto hay $w \in R^*$ tal que $q_i = w p_r$. Entonces $a = p_r b$ con $b = u p_1^{n_1} \cdots p_r^{n_r - 1} \in S_{n-1}$ y $b = vw q_1^{m_1} \cdots q_i^{m_i - 1} \cdots q_s^{m_s}$. Por hipótesis inductiva, estas dos factorizaciones de b son equivalentes; se sigue que las dos factorizaciones de a son equivalentes. □

Proposición 4.2.6. *Sean R un DIP y $0 \subsetneq I \subsetneq R$ un ideal. Entonces existen $r \geq 1$, $n_1, \ldots, n_r \geq 1$ y $\mathfrak{m}_1, \ldots, \mathfrak{m}_r \in \max(R)$ tales que $I = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r}$ con r único y los pares $(\mathfrak{m}_i, n_i)$ únicos salvo una permutación $\sigma \in \mathbb{S}_r$.*

Demostración. Si $fR = I$, y $f = u p_1^{n_1} \cdots p_r^{n_r}$ es una factorización irreducible, entonces $\mathfrak{m}_i = p_i R$ es maximal e $I = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r}$. Por otro lado, dado que dos generadores de un mismo ideal principal no nulo difieren en una unidad, cualquier otra descomposición de I como producto de potencias de ideales

maximales sin repeticiones y con todos los exponentes positivos, produce una descomposición irreducible de f. Luego la descomposición de I es única pues por el Teorema 4.2.4, la de f lo es. □

Ejercicio 4.2.7. i) Sea R un DFU y sean $a, b \in R$ tales que $a^2 = b^3$. Probar que existe $c \in R$ tal que $c^2 = b$ y $c^3 = a$.

ii) Sean k un cuerpo y $R = k \oplus \bigoplus_{n\geq 2} kt^n \subset k[t]$. Probar que R no es DFU.

4.3. Teorema de descomposición primaria para módulos de torsión

Sea R un anillo conmutativo y sea

$$\max(R) = \{\mathfrak{m} \lhd R : \mathfrak{m} \text{ maximal}\}$$

el conjunto de todos los ideales maximales de R. Supongamos ahora que R es un DIP; entonces $\max(R) = \{fR : f \text{ irreducible}\}$. Sean M un R-módulo, $x \in \text{tors}(M)$ y $\mathfrak{m} \in \max(R)$. Decimos que x es de $\mathfrak{m}$-*torsión* (o que es $\mathfrak{m}$-*primario*) si existe $n \geq 0$ tal que $\text{Ann}_R(x) = \mathfrak{m}^n$.

Lema 4.3.1. *Sean R un DIP, $f \in R$ irreducible, $\mathfrak{m} = fR$, M un R-módulo y $x \in M$. Son equivalentes*

i) x es de $\mathfrak{m}$-torsión.

ii) Existe $n \geq 1$ tal que $f^n x = 0$.

Demostración. Si x es de $\mathfrak{m}$-torsión, existe $n \geq 0$ tal que $\mathfrak{m}^n = \text{Ann}_R(x)$; como $f^n \in \mathfrak{m}^n$, $f^n x = 0$. Recíprocamente, supongamos que $f^n x = 0$; entonces $f^n \in \text{Ann}_R(Rx)$ y por tanto Rx es un $R/f^n R = R/\mathfrak{m}^n$-módulo. Por tanto $I = \text{Ann}_R(x) = \text{Ann}_R(Rx) \supset \mathfrak{m}^n$. Sea g tal que $I = gR$. Entonces $g \backslash f^n$, lo que por el Teorema 4.2.4, implica que $g = uf^m$ con $m \leq n$. Luego $\text{Ann}_R(x) = f^m R$. □

Corolario 4.3.2. *El subconjunto*

$$M \supset M[\mathfrak{m}] = \{x \in \text{tors}(M) : x \text{ de } \mathfrak{m} - \text{torsión}\}$$

es un R-submódulo.

Demostración. Sea f como en el Lema 4.3.1. Si $x, y \in \text{tors}(M)[\mathfrak{m}]$ entonces existen $n, m \geq 1$ tales que $f^n x = f^m y = 0$. Luego $f^{\text{máx}\{n,m\}}(x + y) = 0$ y $f^n(ax) = 0$ para todo $a \in x$. Luego ax y $x + y \in M[\mathfrak{m}]$, por el lema. □

Lema 4.3.3. *Sean R DIP, $\mathfrak{m} \in \max(R)$ y M un R-módulo de $\mathfrak{m}$-torsión finitamente generado. Entonces existe $n \geq 0$ tal que $\text{Ann}_R(M) = \mathfrak{m}^n$.*

Demostración. Si $M = 0$, $\text{Ann}_R(M) = R = \mathfrak{m}^0$. Supongamos $M \neq 0$ y sea $\{x_1, \ldots, x_r\} \subset M$ un sistema de generadores con $x_i \neq 0$ para todo i. Entonces para cada i, existe $n_i \geq 1$ tal que $\text{Ann}_R(x_i) = \mathfrak{m}^{n_i}$; sea $n = \text{máx}\{n_i : 1 \leq i \leq r\}$. Por la Observación 4.1.3,

$$\text{Ann}_R(M) = \bigcap_{i=1}^{r} \text{Ann}_R(x_i) = \bigcap_{i=1}^{r} \mathfrak{m}^{n_i} = \mathfrak{m}^n.$$

□

Lema 4.3.4. *Sean R un DIP, $\mathfrak{m} \in \max(R)$ y M un R-módulo de $\mathfrak{m}$-torsión. Sea $a \in R$ y sea $L_a : M \to M$, $L_a(x) = ax$. Si $a \in R \setminus \mathfrak{m}$, L_a es un isomorfismo.*

Demostración. Sea $f \in R$ irreducible tal que $\mathfrak{m} = fR$. Si $x \in M$ entonces $\mathrm{Ann}_R(x) = f^n R$ para algún n. Como $a \notin fR$ y $\mathfrak{m}$ es el único ideal maximal que contiene a f^n, $\langle a, f^n \rangle = R$. Luego existen $b, c \in R$ tales que $1 = ab + f^n c$, y por tanto $x = abx = L_a(bx)$. Luego L_a es suryectiva; además $L_a(x) = 0$ implica $0 = bL_a(x) = L_a(bx) = x$. Por tanto L_a es un isomorfismo. □

Corolario 4.3.5. *Sean R un DIP, M un R-módulo y $\mathfrak{m} \in \max(R)$. Si $M[\mathfrak{m}] \neq 0$ entonces $\mathfrak{m} \supset \mathrm{Ann}_R(M)$.*

Demostración. Supongamos que $\mathfrak{m} \not\supset \mathrm{Ann}_R(M)$. Entonces hay $a \in \mathrm{Ann}_R(M) \setminus \mathfrak{m}$; como $a \in \mathrm{Ann}_R(M)$, $L_a = 0$. Por el Lema 4.3.4, L_a restringido a $M[\mathfrak{m}]$, es un isomorfismo. Por tanto 0 es un isomorfismo sobre $M[\mathfrak{m}]$, de lo que se sigue que $M[\mathfrak{m}] = 0$. □

Ejercicio 4.3.6. Sean R un DIP, $n \geq 1$, e $I_1, \ldots, I_n \lhd R$ ideales tales que si $i \neq j$, $I_i + I_j = R$. Probar que $\bigcap_{j=1}^n I_j = I_1 \cdots I_n$.

Teorema 4.3.7 (Descomposición primaria)**.** *Sean R un DIP y M un R-módulo de torsión. Entonces*

$$M = \bigoplus_{\mathfrak{m} \in \max(R)} M[\mathfrak{m}].$$

Demostración. Sea $N = \sum_{\mathfrak{m} \in \max(R)} M[\mathfrak{m}]$. Sean $q_1, \ldots, q_s$ irreducibles tales que $q_i R \neq q_j R$ si $i \neq j$ y $y = \sum_{i=1}^s y_i$ con $\mathrm{Ann}_R(y_i) = q_i^{m_i} R$. Entonces para cada $1 \leq i \leq s$, la multiplicación por $h_i = \prod_{j \neq i} q_j^{m_j}$ es biyectiva en $M[q_i R]$ (por Lema 4.3.4) y nula en $M[q_j R]$ si $j \neq i$. Además, como $q_i R \neq q_j R$, se sigue que $\langle h_1, \ldots, h_s \rangle = R$, y por tanto existen $a_1, \ldots, a_s \in R$ tales que $1 = \sum_{i=1}^s a_i h_i$. Luego $h_i y = h_i y_i$ y $a_i h_i y = y_i$. Se sigue que $y = 0$ si y sólo si cada $y_i = 0$. Por tanto $N = \bigoplus_{\mathfrak{m} \in \max(R)} M[\mathfrak{m}]$. Sea ahora $x \in M \setminus \{0\}$ y sea $f \in R$ tal que $\mathrm{Ann}_R(x) = fR$. Sea $f = u p_1^{n_1} \cdots p_r^{n_r}$ una factorización irreducible. Por la observación 4.1.3, tenemos un isomorfismo $R/fR \xrightarrow{\sim} Rx$ que manda $1 \mapsto x$. Por el Ejercicio 4.3.6 y el Teorema chino del resto, 2.4.23, hay un isomorfismo de anillos $R/fR \cong \bigoplus_{i=1}^r R/p_i^{n_i} R$. Luego tenemos un isomorfismo de R-módulos $\phi : \bigoplus_{i=1}^r R/p_i^{n_i} R \xrightarrow{\sim} Rx$ que manda la clase de $(1, \ldots, 1)$ en x. Para cada $1 \leq i \leq r$ sean $e_i = (0, \ldots, 1, \ldots, 0)$, con el 1 en el lugar i y $x_i = \phi(e_i)$. Entonces $x = \sum_{i=1}^r x_i$ y $p_i^{n_i} x_i = 0$; en particular x_i es de $p_i R$-torsión por el Lema 4.3.1 y por tanto $x \in N$. □

Ejemplo 4.3.8. Sean R un DIP, $I = fR \lhd R$ y $f = u p_1^{n_1} \cdots p_m^{n_m}$ una factorización irreducible. Entonces $\mathfrak{p}_i = p_i R \lhd R$ es maximal, $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_m^{n_m}$. Por el Teorema chino del resto 2.4.23, $R/I = \bigoplus_{i=1}^m R/\mathfrak{p}_i^{n_i}$. Luego si $\mathfrak{m} \in \max(R)$ entonces $(R/I)[\mathfrak{m}] \neq 0$ si y sólo si $\mathfrak{m} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ y $(R/I)[\mathfrak{p}_i] \cong R/\mathfrak{p}_i^{n_i}$. Más generalmente, si M es un módulo con $\mathrm{Ann}_R(M) = I$, entonces M es un R/I-módulo y por la Proposición 3.7.1, $M = \bigoplus_{i=1}^m M_i$, con M_i un $R/\mathfrak{p}_i^{n_i}$-módulo. En particular $\mathfrak{p}_i^{n_i} M_i = 0$ y por tanto $M_i \subset M[\mathfrak{p}_i]$. Por otro lado si $x = x_1 + \cdots + x_m$ con $x_i \in M_i$ y $a \in \mathfrak{p}_i \cap \mathrm{Ann}_R(x)$, entonces $a x_j = 0$ para todo j. Luego $x_j = 0$ para todo $j \neq i$, por Lema 4.3.4. En conclusión, $M_i = M[\mathfrak{p}_i]$, y por tanto $M[\mathfrak{m}] \neq 0 \iff \mathfrak{m} \supset I$.

Ejercicio 4.3.9. Sean R un DIP, $\mathfrak{m} \in \max(R)$, $n \geq 1$ y M un R-módulo con $\mathrm{Ann}_R(M) = \mathfrak{m}^n$. Probar que existe $x \in M$ tal que $\mathrm{Ann}_R(M) = \mathfrak{m}^n$.

4.4. Teorema de estructura para módulos finitamente generados

Lema 4.4.1. *Sean R un DIP, $\mathfrak{m} \in \max(R)$, $n \geq 1$ y M un R-módulo con $\mathrm{Ann}_R(M) = \mathfrak{m}^n$. Sean $x_1 \in M$ tal que $\mathrm{Ann}_R(x_1) = \mathfrak{m}^n$, y $\pi : M \to N = M/Rx_1$ la proyección.*

i) Si $y \in N$ entonces existe $x \in M$ tal que $\pi(x) = y$ y $\mathrm{Ann}_R(x) = \mathrm{Ann}_R(y)$.

ii) Si $x_2, \ldots, x_r \in M$ son tales que $\mathrm{Ann}_R(x_i) = \mathrm{Ann}_R(\pi(x_i))$ y $\sum_{i=2}^r R\pi(x_i) = \bigoplus_{i=2}^r R\pi(x_i)$, entonces $\sum_{i=1}^r Rx_i = \bigoplus_{i=1}^r Rx_i$. Si además $\bigoplus_{i=2}^r R\pi(x_i) = N$ entonces $\bigoplus_{i=1}^r Rx_i = M$.

Demostración. Sean $\mathfrak{m} = pR$, $l \geq 1$, $y \in N$ con $\mathrm{Ann}_R(y) = \mathfrak{m}^l$ y $x \in M$ tal que $\pi(x) = y$. Entonces $p^l x \in Rx_1$ y por tanto existen $s \leq n$ y $c \in R \setminus \mathfrak{m}$ tales que

$$p^l x = p^s c x_1.$$

Si $s = n$, $p^l x = 0$ y por tanto $\mathrm{Ann}_R(x) = \mathrm{Ann}_R(y)$. Si $s < n$, entonces $\mathrm{Ann}_R(p^s c x_1) = p^{n-s}R$ y por tanto $\mathrm{Ann}_R(x) = p^{l+n-s}R$. Dado que $\mathrm{Ann}_R(M) = p^n R$, resulta que $l + n - s \leq n$ y por tanto $l \leq s$. Sea

$$z = x - p^{s-l} c x_1$$

Entonces $\pi(z) = y$, de lo que se sigue que $\mathrm{Ann}_R(z) \subset \mathrm{Ann}_R(y)$; como además $p^l z = p^l x - p^s c x_1 = 0$, tenemos también $\mathrm{Ann}_R(z) \supset \mathrm{Ann}_R(y)$. Esto prueba la parte i) del lema. Sean $x_2, \ldots, x_r$ como en ii). Sea $P = \pi^{-1}(\bigoplus_{i=2}^n R\pi(x_i))$; notemos que si $\bigoplus_{i=2}^r R\pi(x_i) = N$, entonces $P = M$. Si $x \in P$, existen $a_2, \ldots, a_n$ tales que $\pi(x) = \sum_{i=2}^r a_i \pi(x_i)$, luego $x - \sum_{i=2}^r a_i x_i \in Rx_1$ y por tanto $x \in \sum_{i=1}^r Rx_i$. Si $a_1, \ldots, a_r \in R$ son tales que $0 = \sum_{i=1}^r a_i x_i$, entonces $\sum_{i=2}^r a_i \pi(x_i) = 0$ y por tanto para cada $2 \leq i \leq r$, $a_i \in \mathrm{Ann}_R(\pi(x_i)) = \mathrm{Ann}_R(x_i)$. Se sigue que $a_i x_i = 0$ para todo $1 \leq i \leq r$. Luego $P = \bigoplus_{i=1}^r Rx_i$. □

Teorema 4.4.2 (Teorema de estructura para módulos finitamente generados)**.** *Sean R un DIP y M un R-módulo finitamente generado. Entonces existen únicos $n, r \geq 0$ e ideales propios $0 \neq I_1 \subset \cdots \subset I_r \subsetneq R$ tales que $M \cong R^n \oplus \bigoplus_{j=1}^r R/I_j$.*

Demostración. Por el Corolario 4.1.9 existen $n \geq 0$ y N R-módulo de torsión tales que $M \cong R^n \oplus N$; por el Ejercicio 4.1.10, n es único y N es único salvo isomorfismo. Luego basta probar el teorema para módulos de torsión finitamente generados. Consideramos primero el caso en que existe $\mathfrak{m} \in \max(R)$ tal que M es de $\mathfrak{m}$-torsión. Por el Lema 4.3.3, existe $l \geq 0$ tal que $\mathrm{Ann}_R(M) = \mathfrak{m}^l$. Por el Ejercicio 4.3.9, existe $x_1 \in M$ tal que $\mathrm{Ann}_R(x_1) = \mathfrak{m}^l$; sean $M_1 = Rx_1$ y $\pi_1 : M \to M/M_1$ la proyección. Por el mismo ejercicio y el Lema 4.4.1 existe $x_2 \in M$ tal que $\mathrm{Ann}_R(x_2) = \mathrm{Ann}_R(\pi(x_2)) = \mathrm{Ann}_R(M/Rx_1)$. Aplicando el lema repetidamente obtenemos una sucesión creciente de submódulos $M_i = \langle x_1 \ldots x_i \rangle$ con $\mathrm{Ann}_R(x_i) = \mathrm{Ann}_R(M/M_{i-1})$. Dado que M es noetheriano, se sigue que existe un r tal que $M = M_r$. Sea $\pi_i : M \to M/M_i$ la proyección. Tenemos $M/M_{r-1} = R\pi_{r-1}(x_r)$; luego $M/M_{r-2} = R\pi_{r-2}(x_{r-1}) \oplus R\pi_{r-2}(x_r)$,

por el Lema 4.4.1. Aplicando repetidamente el Lema 4.4.1, vemos que $M = \bigoplus_{i=1}^{r} Rx_i$. Sea $I_j = \mathrm{Ann}_R(x_j)$. Por construcción, $I_1 \subset \cdots \subset I_r$ con $I_j = \mathfrak{m}^{l_j}$ y $M \cong \bigoplus_{j=1}^{r} R/I_j$. Veamos la unicidad de la sucesión $l = l_1 \geq \cdots \geq l_r$. Sea $k = R/\mathfrak{m}$ y sea $f \in R$ tal que $\mathfrak{m} = fR$. Para cada $i \geq 0$, la multiplicación for f^i induce un isomorfismo $k \xrightarrow{\sim} \mathfrak{m}^i/\mathfrak{m}^{i+1}$. Luego

$$\mathfrak{m}^i(R/\mathfrak{m}^j)/\mathfrak{m}^{i+1}(R/\mathfrak{m}^j) = (\mathfrak{m}^i + \mathfrak{m}^j)/(\mathfrak{m}^{i+1} + \mathfrak{m}^j) \cong \begin{cases} k & \text{si } j > i \\ 0 & \text{si no.} \end{cases}$$

Por tanto para cada $i \geq 0$,

$$\dim_k(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M) = |\{1 \leq j \leq r \,|\, l_j > i\}|$$

y entonces

$$|\{1 \leq j \leq r \,|\, l_j = i\}| = \dim_k(\mathfrak{m}^{i-1}M/\mathfrak{m}^i M) - \dim_k(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M).$$

En particular, $r = \dim_k(M/\mathfrak{m}M)$, y la sucesión $l_1 \geq \cdots \geq l_r \geq 1$ está completamente determinada por la clase de isomorfismo de M. Esto completa la demostración para el caso en que M es de $\mathfrak{m}$-torsión. Sea ahora M de torsión finitamente generado. Por el Teorema 4.3.7 y el Corolario 3.6.4, existen finitos maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ tales que $M_i := M[\mathfrak{m}_i] \neq 0$, y $M = \bigoplus_{i=1}^{s} M_i$. Por lo que acabamos de probar, para cada i existe una única sucesión $l_{i,1} \geq \cdots \geq l_{i,r_i} \geq 1$ tal que $M_i \cong \bigoplus_{j=1}^{r_i} R/\mathfrak{m}_i^{l_{i,j}}$. Sea $r = \max\{r_i : 1 \leq i \leq s\}$; para $r_i < r$ y $r \geq j > r_i$, sea $l_j = 0$. Para cada $1 \leq j \leq r$, sea $I_j = \mathfrak{m}_1^{l_{1,j}} \cdots \mathfrak{m}_s^{l_{s,j}}$. Entonces $I_1 \subset \cdots \subset I_r$ y por el Teorema chino del resto 2.4.23, $R/I_j = \bigoplus_{i=1}^{s} R/\mathfrak{m}_i^{l_{i,j}}$. Por tanto

$$M \cong \bigoplus_{j=1}^{r} R/I_j. \tag{4.4.3}$$

Resta probar la unicidad de la sucesión de ideales en la descomposición (4.4.3). Por el Ejemplo 4.3.8,

$$X = \{\mathfrak{m} \in \max(R) : (\exists j)\, I_j \subset \mathfrak{m}\} = \{\mathfrak{m} \in \max(R) : M[\mathfrak{m}] \neq 0\},$$

y si $\mathfrak{m} \in X$ y v_j es el exponente de $\mathfrak{m}$ en la descomposición de I_j de la Proposición 4.2.6 entonces $M[\mathfrak{m}] = \bigoplus_{j=1}^{r} R/\mathfrak{m}^{v_j}$. Luego la unicidad de la descomposición (4.4.3) se sigue de la del caso en que M es de $\mathfrak{m}$-torsión. □

Observación 4.4.4. También es posible formular el teorema pidiendo que la sucesión de ideales sea decreciente; más aún, si permitimos que los últimos ideales sean 0, podemos incluir los primeros n sumandos en la segunda suma directa. En efecto, si n, r e I_j son como en el teorema, definiendo $I'_j = I_{r-j+1}$, obtenemos una sucesión decreciente de ideales ; definiendo $I'_{r+1} = \cdots = I'_{r+n} = 0$ obtenemos $M \cong \bigoplus_{j=1}^{r+n} R/I'_j$. El número $n + r$ y la sucesión $R \supsetneq I'_1 \supset \cdots \supset I'_{r+n}$ son únicos también. Aún otra forma de formular el teorema de estructura es la del siguiente corolario.

Corolario 4.4.5. *Sean R y M como en el Teorema 4.4.2. Supongamos que $0 \neq M$ es de torsión. Entonces existen únicos $r \geq 1$, ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, $s \geq 1$ y vectores $0 \neq n_i = (n_{i,1}, \ldots, n_{i,s}) \in \mathbb{N}_0^s$ tales que para cada i, j, $n_{i,j} \geq n_{i,j+1}$ y*

$$M \cong \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} R/\mathfrak{m}_i^{n_{i,j}}.$$

Demostración. Por el Lema 4.1.4 y la Proposición 4.2.6, $0 \neq \operatorname{Ann}_R(M) = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r}$ con $\mathfrak{m}_i \in \max(R)$. Por el Ejemplo 4.3.8 $M[\mathfrak{m}] \neq 0 \iff \mathfrak{m} \in \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Aplicando el Teorema 4.4.2 a cada $M[\mathfrak{m}_i]$ se obtiene la descomposición del teorema. Dada una tal descomposición, por el argumento del Ejemplo 4.3.8 se sigue del Lema 4.3.4 que $M[\mathfrak{m}_i] \cong \bigoplus_{j=1}^{s} R/\mathfrak{m}_i^{n_{i,j}}$. La unicidad de la descomposición del corolario se sigue entonces del Teorema 4.4.2. □

Ejemplo 4.4.6. Sean k un cuerpo, $\mathbb{V}$ un k-espacio vectorial de dimensión finita, $T \in \operatorname{End}_k(\mathbb{V})$ y $m_T \in k[x]$ el polinomio minimal. Entonces $\mathbb{V}$, considerado como $k[x]$-módulo mediante $f(x) \cdot v = f(T)(v)$, es finitamente generado y de torsión, con $\operatorname{Ann}_{k[x]}(\mathbb{V}) = \langle m_T \rangle$. El Teorema 4.4.2 nos dice que $\mathbb{V} \cong \bigoplus_{i=1}^{r} k[x]/\langle f_i \rangle$, con f_i mónico, $\operatorname{gr}(f_i) > 0$ y $f_{i+1} \backslash f_i$ para todo i. Se sigue que existen subespacios T-estables $\mathbb{V}_1, \ldots, \mathbb{V}_r$ tales que $\mathbb{V} = \mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_r$ y tales que cada $\mathbb{V}_i$ tiene una base $\mathfrak{B}_i$ que corresponde a la base $\{1, x, \ldots, x^{\operatorname{gr}(f_i)-1}\}$ de $k[x]/\langle f_i \rangle$, de modo que T corresponde a la multiplicación por x. La matriz $[T_{|\mathbb{V}_i}]_{\mathfrak{B}_i} = C_{f_i}$ es la *matriz compañera* de f_i. Si f es un polinomio mónico de grado n y $f = x^n + \sum_{i=0}^{n-1} a_i x^i$,

$$C_f = \begin{bmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & -a_{n-1} \end{bmatrix}$$

Por definición, C_f es la matriz de la multiplicación por x en $k[x]/\langle f \rangle$ con respecto a la base $\{1, \ldots, x^{n-1}\}$. Si $f = (x - \lambda)^n$, la matriz de la multiplicación por x en la base $\{1, x - \lambda, \cdots, (x - \lambda)^{n-1}\}$ es el *bloque de Jordan*

$$J(\lambda, n) = \begin{bmatrix} \lambda & 0 & \ldots & 0 \\ 1 & \lambda & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \lambda \end{bmatrix}$$

Así, la descomposición del Corolario 4.4.5 es equivalente a la de la forma de Jordan de T.

4.5. Forma normal de Smith

Lema 4.5.1. *Sean R un DIP y $a, b \in R$. Sean $d \in R$ tal que $dR = aR + bR$, y $s, t \in R$ tales que $sa + tb = d$. Sean $a' = a/d$, $b' = b/d$. Entonces la matriz*

$$P = \begin{pmatrix} s & t \\ -b' & a' \end{pmatrix} \in \mathrm{GL}_2(R)$$

y se tiene

$$P \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ -tb' & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot P^t = \begin{pmatrix} d & 0 \\ 0 & a'b \end{pmatrix}.$$

Demostración. La matriz P es inversible porque $\det(P) = 1$. El resto se sigue por cálculo directo. □

Teorema 4.5.2 (Forma normal de Smith)**.** *Sean R un DIP, $n, m \geq 1$, y $0 \neq A \in R^{m \times n}$. Sea $r = \min\{n, m\}$. Entonces existen $P \in \mathrm{GL}_m(R)$, $Q \in \mathrm{GL}_n(R)$ tales que $PAQ = \mathrm{diag}(d_1, \ldots, d_r)$ es una matriz diagonal con $I_j = d_j R \supset I_{j+1}$ para todo j. Los ideales I_j son únicos; si $P' \in \mathrm{GL}_m(R)$ y $Q' \in \mathrm{GL}_n(R)$ son tales que $P'AQ' = \mathrm{diag}(d'_1, \ldots, d'_r)$ con $I'_j = d'_j R \supset I'_{j+1} R$ para todo j, entonces $I'_j = I_j$ para todo j.*

Demostración. Existencia: Sea

$$\delta : R \setminus \{0\} \to \mathbb{N}_0, \delta(a) = \begin{cases} 0 & \text{si } a \in R^* \\ \sum_{i=1}^r n_i & \text{si } a = u p_1^{n_1} \ldots p_r^{n_r} \text{ es FI.} \end{cases}$$

Sea j el índice de la primera columna no nula de A. Luego de multiplicar a izquierda por una matriz de permutación si es necesario, podemos suponer que $A_{1,j} \neq 0$. Más aún si alguno de los coeficientes de la columna j divide a todos los otros, podemos suponer que está en el lugar $(1, j)$. En ese caso, multiplicando a izquierda por una matriz elemental y sin cambiar las primeras $j - 1$ columnas ni la fila 1, llegamos a una matriz en la que el soporte de la columna j consiste sólo del 1. Notemos que el valor de $\delta(A_{1,j})$ no cambia en este proceso. Si ningún coeficiente divide a los demás, utilizando una matriz inversible como en el Lema 4.5.1, (intercalada en la matriz identidad) podemos reemplazar A por una matriz que difiere de A sólo en las filas 1 e i, cuya primera columna no nula es la columna j, que tiene un coeficiente no nulo en $A_{1,j}$ y 0 en el lugar (i, j). Observemos que el valor de $\delta(A_{1,j})$ disminuye en este proceso. Iterando este proceso llegamos a una matriz cuya primera columna no nula es la columna j, la cual tiene un solo coeficiente no nulo, que está en la posición $(1, j)$ y que divide a todos los coeficientes de la columna j de la matriz original. El valor de $\delta(A_{1,j})$ de esta matriz es estrictamente menor que en la matriz original. A continuación aplicamos el mismo procedimiento, multiplicando ahora a derecha por matrices inversibles, de modo de lograr una matriz cuya primera columna no nula sigue siendo la columna j, y donde la fila 1 está soportada en la columna j. Si el viejo $A_{1,j}$ dividía a todos los coeficientes de la fila 1, podemos hacerlo de forma tal que en la nueva matriz

el coeficiente $(1, j)$ sea el mismo, y que sea el único coeficiente no nulo tanto de la fila 1 como de la columna j. Si no, el soporte de la columna j de la nueva matriz puede incluir más filas, pero el nuevo coeficiente $(1, j)$ tiene δ estrictamente menor que el viejo. En este caso repetimos el proceso nuevamente, para que quede un solo coeficiente no nulo en la columna j y que esté en el lugar $(1, j)$, y sin cambiar las primeras $j - 1$ columnas, etc. Vemos que el valor de $\delta(A_{1,j})$ disminuye estrictamente hasta que se logra una matriz con las primeras $j - 1$ columnas nulas, y donde el único coeficiente no nulo tanto en la columna j como en la fila 1 está en el lugar $(1, j)$. Entonces si j' es la segunda columna no nula de esa matriz, aplicamos el procedimiento anterior sin cambiar la fila 1 ni las primeras $j' - 1$ columnas para lograr una nueva matriz donde el único coeficiente no nulo tanto de la fila 2 como de la columna j' esté en el lugar $(2, j')$. Siguiendo de este modo llegamos a una matriz de la forma $\sum_{i=1}^{s} a_i E_{i,j_i}$ con $j_1 < \cdots < j_s$ y $a_i \neq 0$ para todo $1 \leq i \leq s$. Multiplicando a derecha por una matriz de permutación, nos queda una matriz de esa misma forma pero con $j_i = i$ para todo $1 \leq i \leq s$. Si algún a_i no es divisible por a_1, multiplicando reiteradamente a izquierda y a derecha por matrices inversibles como en el Lema 4.5.1, podemos reemplazar a nuestra matriz por otra matriz diagonal donde el coeficiente $(1, 1)$ divide a todos los otros coeficientes. Si algún coeficiente diagonal no es divisible por el coeficiente $(2, 2)$, aplicamos el mismo proceso, sin cambiar el coeficiente $(1, 1)$, llegando a una matriz diagonal donde el coeficiente $(1, 1)$ divide a todos los demás y el coeficiente $(2, 2)$ divide a todos los coeficientes en (i, i) con $i > 2$. Iterando este procedimiento, llegamos a una matriz diagonal como indica el teorema.

Unicidad: Sea $M = \mathrm{Coker}(A) = R^m/\mathrm{Im}(A)$ y sean P, Q, $D = \mathrm{diag}(d_1, \ldots, d_r) = PAQ$ e I_j como en el teorema; si $m > n$, sea $s = m - r$ si no, sea $s = 0$. Tenemos un diagrama conmutativo de flechas sólidas con filas exactas

$$\begin{array}{ccccccc} R^n & \xrightarrow{A} & R^m & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle Q^{-1}} & & \downarrow{\scriptstyle P} & & \vdots{\scriptstyle f} & & \\ R^n & \xrightarrow[D]{} & R^m & \xrightarrow[\pi']{} & \mathrm{Coker}(D) & \longrightarrow & 0. \end{array}$$

La flecha punteada f existe porque la conmutatividad del diagrama nos dice que P manda la imagen de A en la imagen de D. Como $\pi' \circ P$ es suryectiva, f también lo es. Análogamente, como Q es inversible, $\mathrm{Im}(DQ^{-1}) = \mathrm{Im}(D)$ y como $DQ^{-1} = PA$, tenemos $\mathrm{Im}(D) = P(\mathrm{Im}(A))$. Dado que P es inversible, se sigue que $P(x) \in \mathrm{Ker}(\pi') = \mathrm{Im}(D)$ si y sólo si $x \in \mathrm{Im}(A) = \mathrm{Ker}(\pi)$. Por tanto f es un monomorfismo. En conclusión, f es un isomorfismo entre M y $\mathrm{Coker}(D) = R^s \oplus \bigoplus_{j=1}^{r} R/I_j$. Sea l el número de ideales $I_j = 0$ en esta descomposición. Por el Teorema 4.4.2 y el Lema 4.4.4, tanto $s + l$ como la sucesión de ideales propios no nulos en esta descomposición dependen sólo de la clase de isomorfismo de M; el número de j tales que $I_j = R$ depende de sólo de M y del tamaño de A. □

Corolario 4.5.3. *Sean $A, B \in M_n(R)$ matrices no nulas y sean $M = \mathrm{Coker}(A)$, $N = \mathrm{Coker}(B)$. Si $M \cong N$ entonces $\det(A)R = \det(B)R$.*

Demostración. Por el Teorema 4.5.2, existen $P, Q, G, H \in \mathrm{GL}_n(R)$ y $d, e \in R^n$ tales que $PAQ = \mathrm{diag}(d_1, \ldots, d_n)$ y $GBH = \mathrm{diag}(e_1, \ldots, e_n)$ con $d_i \backslash d_{i+1}$, $e_i \backslash e_{i+1}$ y $I_j = e_i R = d_i R$. Como $\det(P)$,$\det(Q)$,$\det(G)$ y $\det(H)$ son inversibles, se tiene

$$\det(A)R = d_1 \cdots d_n R = I_1 \cdots I_n = e_1 \cdots e_n R = \det(B)R.$$

□

Observación 4.5.4. El Corolario 4.5.3 dice que si $A \in M_n(\mathbb{Z})$, entonces el valor absoluto $|\det(A)|$ de su determinante, depende sólo de la clase de isomorfismo de $\mathrm{Coker}(A)$. Por otro lado, el ejemplo $A = [n]$, $B = [-n]$ muestra que dos matrices cuadradas enteras A y B pueden tener conúcleos isomorfos y determinantes de signo distinto.

4.6. Teorema de estructura para módulos inyectivos

Sean R un dominio conmutativo y $f \in R \setminus (R^* \cup \{0\})$. Sea K el cuerpo de cocientes de R (definido en el Ejercicio 10 de la Práctica 7) y sea

$$K \supset R[1/f] = \{x \in K : (\exists n \geq 1)\, f^n x \in R\} = \{a/f^n : a \in R,\, n \in \mathbb{N}_0\}.$$

Lema 4.6.1. *Hay un isomorfismo de R-álgebras $R[1/f] \cong R[x]/\langle xf - 1\rangle$.*

Demostración. Sea $\psi : R[x] \to K$ el morfismo de R-álgebras determinado por $\psi(x) = 1/f$. Entonces $\psi(ax^n) = a/f^n$, y por tanto $\mathrm{Im}(\psi) = R[1/f]$. Sea $q = \sum_{i=0}^{n} a_i x^i \in R[x]$ con $a_n \neq 0$. Entonces $q \in \mathrm{Ker}(\psi)$ si y sólo si $0 = q(1/f)$ si y sólo si el polinomio $x - 1/f$ divide a q en $K[x]$. Sea $p = \sum_{i=0}^{n-1} b_i x^i \in K[x]$

tal que $q = (x - 1/f)p$; sean $b_n = b_{-1} = 0$. Entonces

$$\begin{aligned}\sum_{i=0}^{n} a_i x^i &= \sum_{i=0}^{n-1} b_i x^i (x - 1/f) \\ &= \sum_{i=0}^{n-1} b_i x^{i+1} - \sum_{i=0}^{n-1} (b_i/f) x^i \\ &= \sum_{i=0}^{n} (b_{i-1} - b_i/f) x^i.\end{aligned}$$

Igualando coeficiente a coeficiente, obtenemos

$$a_i = b_{i-1} - b_i/f \Rightarrow b_i = f(b_{i-1} - a_i).$$

En particular $b_0 = -fa_0$ y obtenemos la fórmula recursiva

$$b_i = -\sum_{j=0}^{i} f^{i+1-j} a_j.$$

En particular, $c_i = -\sum_{j=0}^{i} f^{i-j} a_j \in R$, y $b_i = fc_i$. Luego $q = (fx-1)(\sum_{i=0}^{n-1} c_i x^i)$ es múltiplo de $fx - 1$ en $R[x]$. Por tanto $\mathrm{Ker}(\psi) = \langle fx - 1 \rangle$ y $R[1/f] \cong R[x]/(fx-1)R[x]$. □

Corolario 4.6.2. *Sean Q un R-módulo inyectivo, $n \geq 0$ y $q \in Q$. Entonces existe un morfismo de R-módulos $\psi : R[1/f] \to Q$ tal que $\psi(1/f^n) = q$.*

Demostración. Como Q es inyectivo, existe una sucesión $(q_m)_{m \geq 0}$ de elementos de Q con $q_0 = q$ y tal que para todo m, $fq_{m+1} = q_m$. Recordemos que $R[x]$ es un R-módulo libre con base $\{x^i : i \geq 0\}$. Sea $\hat{\psi} : R[x] \to Q$ el morfismo de R-módulos definido por

$$\hat{\psi}(x^i) = \begin{cases} f^{n-i} q_0 & \text{si } 0 \leq i \leq n \\ q_{i-n} & \text{si } i \geq n \end{cases}$$

Observemos que, para todo $i \geq 0$, $f\hat{\psi}(x^{i+1}) = \hat{\psi}(x^i)$. Luego $\hat{\psi}(fx^{i+1} - x^i) = 0$ para todo $i \geq 0$, y por tanto $\hat{\psi}((fx-1)R[x]) = 0$. Luego $\hat{\psi}$ induce un morfismo de R-módulos $\psi : R[1/f] \to Q$ con $\psi(1/f^n) = q$, por el Lema 4.6.1. □

Observemos que $R[1/f]$ es un R-submódulo de K que contiene a R como R-submódulo. Sean

$$R_{f^\infty} = R[1/f]/R \text{ y } \pi : R[1/f] \to R_{p^\infty}$$

la proyección.

Corolario 4.6.3. *Sean Q un R-módulo inyectivo, $n \geq 0$ y $q \in Q$. Supongamos que $f^n q = 0$. Entonces existe un morfismo de R-módulos $\bar{\psi} : R_{f^\infty} \to Q$ tal que $\bar{\psi}(\pi(1/f^n)) = q$.*

Demostración. Dado que $f^n q = 0$, el morfismo ψ del Corolario 4.6.2 pasa al cociente módulo R. □

Ejercicio 4.6.4.

i) R_{f^∞} es un R-módulo de torsión.

ii) Sea $n \geq 1$; entonces $R[1/f^n] = R[1/f]$ y $R_{(f^n)^\infty} = R_{f^\infty}$.

iii) Si $f \backslash g$ entonces $R[1/f] \subset R[1/g]$ y $R_{f^\infty} \subset R_{g^\infty}$.

Observación 4.6.5. Si $f \backslash g$ y $g \backslash f$ entonces $R[1/f] = R[1/g]$ y $R_{f^\infty} = R_{g^\infty}$, por el Ejercicio 4.6.4. Luego tanto $R[1/f]$ como R_{f^∞} dependen sólo del ideal fR.

Proposición 4.6.6. *Sean R un DIP, $f \in R \setminus (R^* \cup \{0\})$ y $f = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ una factorización irreducible.*

i) $R_{f^\infty} = \bigoplus_{i=1}^r R_{p_i^\infty}$ y $R_{p_i^\infty}$ es la componente p_iR-primaria de R_{f^∞}

ii) R_{f^∞} es un R-módulo inyectivo.

Demostración. Sea $\mathfrak{p}_i = p_iR$ $(1 \leq i \leq r)$. Notemos que para todo $x \in M = R_{f^\infty}$ existe $n \geq 0$ tal que $f^n x = 0$. Luego si $\mathfrak{m} \in \max(R) \supset \operatorname{Ann}_R(x)$ entonces $\mathfrak{m} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. En particular, $M[\mathfrak{m}] = 0$ para todo $\mathfrak{m} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Por lo que acabamos de ver y el Ejercicio 4.6.4, $R_{p_i^\infty} \subset M[\mathfrak{p}_i]$. Sean $\pi : R[1/f] \to M$ la proyección y $x \in R[1/f]$ tal que $\pi(x) \in M[\mathfrak{p}_i]$; entonces existe $n \geq 1$ tal que $p_i^n x = a \in R$. Luego $x = a/p_i^n \in R[1/p_i]$ y por tanto $\pi(x) \in R_{p_i^\infty}$. Esto prueba que $M[\mathfrak{p}_i] = R_{p_i^\infty}$ y termina la demostración de la parte i). Para la parte ii) basta ver que M es divisible, por el Corolario 3.8.11. Sea $a \in R \setminus \{0\}$ y sea $L_a : M \to M$, $L_a(x) = ax$. Debemos probar que L_a es suryectiva. Por el Lema 4.3.4, si $a \notin \mathfrak{p}_j$, la restricción de L_a a $M[\mathfrak{p}_j]$ es un isomorfismo. Luego basta ver que si $a \in \mathfrak{p}_i$, $L_a(R_{p_i^\infty}) = R_{p_i^\infty}$. Escribamos $a = p_i^n q$ con $n \geq 1$ y $p \not\backslash q$. Entonces $L_a = L_q \circ L_{p_i^n}$ y $L_q : R_{p_i^\infty} \to R_{p_i^\infty}$ es biyectiva por el Lema 4.3.4. Luego basta ver que $L_{p_i^n}(R_{p_i^\infty}) = R_{p_i^\infty}$. Sea $x \in R[1/p_i]$; entonces $y = x/p_i^n \in R[1/p_i]$ y $\pi(x) = p_i^n \pi(y) = L_{p_i^n}(\pi(y))$. Esto termina la demostración. □

Lema 4.6.7. *Sean R un DIP, $p \in R$ irreducible, $\mathfrak{p} = pR$ y $\pi : R[1/p] \to R_{p^\infty}$ la proyección.*

i) Para todo $x \in R[1/p] \setminus \{0\}$ existen únicos $n \in \mathbb{Z}$ y $a \in R \setminus \{\mathfrak{p}\}$ tales que $x = ap^n$.

ii) Si x y n son como en i), entonces $\langle \pi(x) \rangle = \langle \pi(p^n) \rangle$.

iii) Sea $0 \neq S \subsetneq R_{p^\infty}$ un R-submódulo. Entonces existe $n \geq 1$ tal que $S = \langle \pi(1/p^n) \rangle$.

iv) Sea $\phi : R_{p^\infty} \to M$ un epimorfismo de R-módulos. Si $M \neq 0$, entonces $M \cong R_{p^\infty}$.

v) Si $0 \neq \phi \in \operatorname{End}_R(R_{p^\infty})$, entonces ϕ es suryectivo.

Demostración. i) Existencia: Sea $x \in R[1/p] \setminus \{0\}$. Si $x \in R \setminus \mathfrak{p}$, tomamos $a = x$ y $n = 0$. Si $x \in \mathfrak{p}$, entonces $x \in R \setminus (R^* \cup \{0\})$ y por el Teorema 4.2.4, tiene una factorización irreducible $x = up_1^{n_1} \cdots p_r^{n_r}$. Como $p \backslash x$, existen únicos i y $u_i \in R^*$ tales que $p_i = u_i p$. Luego $a = (uu_i^{n_i} \prod_{j \neq i} p_j^{n_j}) \notin \mathfrak{p}$ y $x = ap^{n_i}$. Si $x = y/p^n$ con $y \in R$ entonces por lo que ya vimos, $y = ap^m$ con $m \geq 0$, y $p \not\backslash a$ y por tanto $x = ap^{m-n}$. Unicidad: Si $p \not\backslash a$, $p \not\backslash b$ y $n, m \in \mathbb{Z}$ son tales que $p^n a = p^m b$ entonces o bien $n = m$, y por tanto $a = b$, o bien $n \neq m$. Supongamos $n > m$. Entonces $p^{n-m} a = b$ luego $p \backslash b$, que es una contradicción.

ii) Si $n \geq 0$, $\pi(x) = \pi(p^n) = 0$ y la afirmación es clara. Supongamos que $n = -m$ con $m > 0$. Como $a \notin \mathfrak{p}$ y $\mathfrak{p}$ es el único ideal maximal que contiene a p^m, $\langle a, p^m \rangle = R$. Luego existen $s, t \in R$ tales que $sa + tp^m = 1$. Entonces $sx + t = 1/p^m = p^n$, luego $s\pi(x) = \pi(p^n)$ y $a\pi(p^n) = \pi(x)$. Por tanto $\langle \pi(x) \rangle = \langle \pi(p^n) \rangle$.
iii) Como $S \neq R_{p^\infty}$, por la parte ii) existe $n \geq 1$ tal que $\pi(1/p^n) \notin S$. Luego $\pi(1/p^m) \notin S$ para todo $m \geq n$, y, nuevamente por ii), $\pi(a/p^m) \notin S$ para todo $a \in R \setminus \mathfrak{p}$. Luego si $x \in S$ entonces $x = \pi(b/p^r)$ con $r < n$. Por tanto $S \subset \langle \pi(1/p^{n-1}) \rangle$. Además, por ii), si $S \neq 0$, existe $s \geq 1$ tal que $\pi(1/p^s) \in S$. Sea r el máximo de tales s. Entonces $S_0 = \langle \pi(1/p^r) \rangle \subset S$, y si $\pi(a/p^m) \in S$, entonces, por ii), $\pi(1/p^m) \in S$, por lo que $m \leq r$, y por tanto $\pi(a/p^m) \in S_0$. Luego $S = S_0$.
iv) Sea $S = \mathrm{Ker}(\phi)$. Por el Teorema 3.3.4, $M \cong R_{p^\infty}/S$. Como $M \neq 0$, $S \neq R_{p^\infty}$. Si $S = 0$, $M \cong R_{p^\infty}$. Supongamos entonces que $0 \neq S \subsetneq R_{p^\infty}$. Por iii), existe $n \geq 1$ tal que $S = \langle \pi(1/p^n) \rangle$. Sea $L : R_{p^\infty} \to R_{p^\infty}$, $L(x) = p^n x$. Por la Proposición 4.6.6 y el Corolario 3.8.11, L es suryectiva; por tanto $R_{p^\infty}/\mathrm{Ker}(L) \cong R_{p^\infty}$. Además,

$$\begin{aligned} \mathrm{Ker}(L) =& \{x : p^n x = 0\} = \{\pi(y) : p^n y \in R\} \\ =& \{\pi(a/p^n) : a \in R\} = \langle \pi(1/p^n) \rangle = S. \end{aligned}$$

Luego $M \cong R_{p^\infty}/S \cong R_{p^\infty}$.
v) Sea $S = \mathrm{Im}(\phi)$; como $\phi \neq 0$, $S \neq 0$. Por iv) y la Proposición 4.6.6, S es un R-módulo inyectivo. Por iii) si S no fuera todo R_{p^∞}, entonces existiría $n \geq 1$ tal que $S = R\pi(1/p^n)$, y por tanto $p^n \in \mathrm{Ann}_R(S) \neq 0$, luego S no sería inyectivo, por el Corolario 3.8.13. Luego $S = R_{p^\infty}$ y por tanto ϕ es suryectivo. □

Lema 4.6.8. *Sean R un DIP y Q un R-módulo inyectivo libre de torsión. Entonces existe una única estructura de K-espacio vectorial en Q que extiende su estructura de R-módulo.*

Demostración. Sea $a \in R \setminus \{0\}$. Como Q es inyectivo, es divisible por el Corolario 3.8.11, y por tanto L_a es suryectiva. Como Q es libre de torsión, L_a es inyectiva. Luego el morfismo de anillos $L : R \to \mathrm{End}_{\mathbb{Z}}(Q)$, $a \mapsto L_a$ manda todo elemento no nulo de R en un elemento inversible y por tanto se extiende en forma única a un morfismo de anillos $L : K \to \mathrm{End}_{\mathbb{Z}}(Q)$, por el Ejercicio 10 de la Práctica 7. □

Sean R un DIP, $\mathfrak{p} \in \max(R)$ y $p \in R$ tal que $\mathfrak{p} = pR$. Por la Observación 4.6.5,

$$R_{\mathfrak{p}^\infty} := R_{p^\infty}$$

no depende del generador p elegido.

Teorema 4.6.9 (Teorema de estructura para módulos inyectivos)**.** *Sean R un DIP y Q un R-módulo inyectivo. Entonces existen conjuntos I e $I_{\mathfrak{p}}$, $\mathfrak{p} \in \max(R)$, tales que*

$$Q \cong K^{(I)} \oplus \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(I_{\mathfrak{p}})}.$$

Esta descomposición es única en el sentido de que si $Q \cong K^{(J)} \oplus \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(J_{\mathfrak{p}})}$, entonces $|I| = |J|$ y para todo $\mathfrak{p} \in \max(R)$, $|I_{\mathfrak{p}}| = |J_{\mathfrak{p}}|$.

Demostración. Existencia. Sea $M = \text{tors}(Q)$; si $M = 0$, entonces Q es un K-espacio vectorial por el Lema 4.6.8 y por tanto existe I tal que $Q \cong K^{(I)}$, por el Teorema 3.10.5; tomando $I_\mathfrak{p} = \emptyset$ para todo $\mathfrak{p} \in \max(R)$, se tiene una descomposición como en el teorema. Supongamos que $M \neq 0$; para cada $\mathfrak{p} \in \max(R)$ sea $M[\mathfrak{p}]$ la componente $\mathfrak{p}$-primaria del Teorema 4.3.7. Fijemos, por un rato, un maximal $\mathfrak{p}$ tal que $N = M[\mathfrak{p}] \neq 0$. Notemos que N es inyectivo; en efecto, por el Lema 4.3.4 y el Corolario 3.8.11, basta ver que si $\mathfrak{p} = pR$, $x \in N$ y $n \geq 1$, entonces existe $y \in N$ tal que $p^n y = x$. Como Q es inyectivo, un tal y existe en Q; como x es de $\mathfrak{p}$-torsión, y también lo es, y por tanto $y \in N$. Luego N es inyectivo, y por el Corolario 4.6.3 y el Lema 4.6.7 cada elemento $x \in N$ está en un submódulo de N isomorfo a $R_{\mathfrak{p}^\infty}$. Sea $\mathcal{C}$ la colección de todos los submódulos de N isomorfos a $R_{\mathfrak{p}^\infty}$. Por lo que acabamos de ver, $N = \sum_{S \in \mathcal{C}} S$. Sea $X = \{\mathcal{Y} \subset \mathcal{C} : \sum_{S \in \mathcal{Y}} S = \bigoplus_{S \in \mathcal{Y}} S\}$; $X \ni \{S\}$ para cada $S \in \mathcal{C}$. Luego $X \neq \emptyset$; más aún, es un ejercicio verificar que la unión de una cadena de elementos de X es de nuevo un elemento de X. Por Zorn, X tiene un elemento maximal $\mathfrak{X}$. Sea $N_0 = \bigoplus_{S \in \mathfrak{X}} S$; por defininición, $N_0 \subset N$; queremos ver que $N_0 = N$. Observemos que, por el Corolario 3.8.12 y el Ejercicio 4.6.4, N_0 es inyectivo. Luego, por el Ejercicio 3.8.7 existe un R-submódulo $N_1 \subset N$ tal que $N = N_0 \oplus N_1$. Por el Ejercicio 3.8.8, N_1 es inyectivo. Por tanto tiene que ser $N_1 = 0$, ya que si no, contendría un elemento S de $\mathcal{C}$, por el Corolario 4.6.3 y el Lema 4.6.7, entonces $\mathfrak{X} \cup \{S\} \in X$, lo que contradice la maximalidad de $\mathfrak{X}$. Hemos probado que $N = \bigoplus_{S \in \mathfrak{X}} S \cong R_{\mathfrak{p}^\infty}^{(\mathfrak{X})}$. Luego existen conjuntos $I_\mathfrak{p}$ tales que $M = \bigoplus_{\mathfrak{p} \in \max(R)} R_\mathfrak{p}^{(I_\mathfrak{p})}$. En particular, M es inyectivo por la Proposición 4.6.6 y el Corolario 3.8.12 y por el Ejercicio 3.8.7 existe un submódulo $M' \subset Q$ tal que $Q = M \oplus M'$. Luego M' es inyectivo y $M' \cong Q_{\text{tf}}$, así que es libre de torsión, por el Lema 4.1.6. Luego por lo visto al principio de la demostración, existe un conjunto I tal que $M' \cong K^{(I)}$. Esto completa la demostración de la existencia de la descomposición del teorema.

Unicidad. Sean $Q_1 = K^{(I)} \oplus \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(I_\mathfrak{p})}$ y $Q_2 = K^{(J)} \oplus \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(J_\mathfrak{p})}$ y sea $\phi : Q_1 \to Q_2$ la composición de los isomorfismos $Q_1 \cong Q \cong Q_2$. Entonces ϕ induce un isomorfismo entre los submódulos de torsión, que son, respectivamente, $\text{tors}(Q_1) = \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(I_\mathfrak{p})}$ y $\text{tors}(Q_2) = \bigoplus_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}^\infty}^{(J_\mathfrak{p})}$ y también entre los cocientes $(Q_1)_{\text{tf}} = K^{(I)}$ y $(Q_2)_{\text{tf}} = K^{(J)}$. Dado que un morfismo R-lineal de K-espacios vectoriales es automáticamente K-lineal, se sigue que $|I| = |J|$ por el Teorema 3.10.5. Sean $\mathfrak{p} \in \max(R)$ y $k = R/\mathfrak{p}$. El isomorfismo $\phi : \text{tors}(Q_1) \xrightarrow{\sim} \text{tors}(Q_2)$ induce un isomorfismo $M = \text{tors}(Q_1)[\mathfrak{p}] = R_\mathfrak{p}^{(I_\mathfrak{p})} \xrightarrow{\sim} \text{tors}(Q_2)[\mathfrak{p}] = R_\mathfrak{p}^{(J_\mathfrak{p})} = N$ que a su vez induce un isomorfismo entre $\{x \in M : px = 0\} = (\langle \pi(1/p) \rangle)^{(I_p)} \cong k^{(I_\mathfrak{p})}$ y $\{x \in M : px = 0\} \cong k^{(J_p)}$. En particular $k^{(I_\mathfrak{p})}$ y $k^{(J_\mathfrak{p})}$ son isomorfos como R-módulos y por tanto como k-espacios vectoriales. Luego $|I_p| = |J_p|$, de nuevo por el Teorema 3.10.5. □

Bibliografía

[1] Paul E. Bland, *Rings and their modules*, De Gruyter, 2011. ↑72

[2] Nathan Jacobson, *Basic algebra II, ed.2*, W.H. Freeman and Company, 1989. ↑3, 72

[3] Serge Lang, *Algebra*, 3rd ed., Graduate texts in mathematics, vol. 211, Springer, 2002. ↑3

[4] William G. Leavitt, *The module type of homomorphic images*, Duke Math. J. **32**, no. 2, 305–311. ↑44

[5] Horacio Hernán O'Brien, *Estructuras algebraicas III (Grupos finitos)*, The general secretariat of the Organization of American States, Washington, DC, 1973. ↑3

[6] Wikipedia, *Classification of finite simple groups*, https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups. ↑29