Leandro Vendramin

Álgebra II

– Notas –

7 de diciembre de 2021

Prefacio

Las notas corresponden al curso Álgebra II.

Muchas personas leyeron las notas y reportaron errores: Cristian Meza Alarcon, Jessica Singer, Matías Conde, Santiago Varela.

Buenos Aires, XX de XX de 2021 *Leandro Vendramin*

Índice general

Parte I
Grupos

Capítulo 1
Grupos y subgrupos

Antes de dar la definición de grupo recordemos que una operación binaria en un cierto conjunto X es una función $X \times X \to X$, $(x,y) \mapsto xy$. Observemos que la notación que utilizamos para esta operación binaria genérica es la misma que usualmente se usa para la multiplicación de números, aunque nuestra operación sea algo mucho más general. Por ejemplo, $(x,y) \mapsto x-y$ es una operación binaria en $\mathbb{Z}$ pero no lo es en $\mathbb{N}$.

Definición 1.1. Un **grupo** es un conjunto no vacío G junto con una operación binaria en G que satisface las siguientes propiedades:

1) Asociatividad: $x(yz) = (xy)z$ para todo $x,y,z \in G$.
2) Existencia de elemento neutro: existe un elemento $e \in G$ tal que $ex = xe = x$ para todo $x \in G$.
3) Existencia del inverso: para cada $x \in G$ existe $y \in G$ tal que $xy = yx = e$.

El axioma sobre asociatividad que aparece en nuestra definición de grupo es suficiente para demostrar que todos los productos ordenados que podamos formar con los elementos $x_1, x_2, \ldots, x_n$ son iguales. Por ejemplo

$$(x_1x_2)((x_3x_4)x_5) = x_1(x_2(x_3(x_4x_5)))$$

y podemos escribir sin ambigüedad $x_1x_2\cdots x_5$, sin preocuparnos por poner paréntesis. Esta observación suele demostrarse por inducción, así se hace por ejemplo en el libro de Lang. Daremos una demostración mucho más sencilla en el capítulo 5, como aplicación del teorema de Cayley.

Proposición 1.2. *En un grupo G, cada $x \in G$ admite un único inverso $x^{-1} \in G$.*

Demostración. Si $y,z \in G$ son ambos inversos del elemento $x \in G$, entonces, gracias a los axiomas que definen un grupo, tenemos que $z = z(xy) = (zx)y = 1y = y$. □

Ejercicio 1.3. Demuestre que el elemento neutro de un grupo es único.

El elemento neutro de un grupo G será denotado por 1_G o simplemente como 1 cuando no haya peligro de confusión. El inverso de un elemento $x \in G$ será denotado por x^{-1}.

De la definición podemos obtener fácilmente otras propiedades de los inversos de elementos de un grupo:

1) $(x^{-1})^{-1} = x$ para todo $x \in G$.
2) $(xy)^{-1} = y^{-1}x^{-1}$ para todo $x, y \in G$.

Ejercicio 1.4. Demuestre que en un grupo G la ecuación $ax = b$ tiene a $x = a^{-1}b$ como única solución. Similarmente, $x = ba^{-1}$ es la única solución de la ecuación $xa = b$.

Definición 1.5. Un grupo G se dirá **abeliano** si $xy = yx$ para todo $x, y \in G$.

A veces, cuando tratemos con grupos abelianos, utilizaremos la notación aditiva. Eso significa que la operación binaria será $(x, y) \mapsto x + y$, el neutro será denotado por 0 y el inverso de un cierto elemento x será $-x$.

Definición 1.6. El **orden** $|G|$ de un grupo G es el cardinal de G. Un grupo G se dirá finito si $|G|$ es finito e infinito en caso contrario.

Ejercicio 1.7. Sean G un grupo y $g \in G$. Demuestre que las funciones $L_g \colon G \to G$, $x \mapsto gx$, y $R_g \colon G \to G$, $x \mapsto xg$, son biyectivas.

Ejemplos 1.8. Ejemplos de grupos abelianos:

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma usual.
2) Los enteros $\mathbb{Z}/n$ módulo n con la suma usual.
3) $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ y $\mathbb{C} \setminus \{0\}$ con la multiplicación usual.
4) El conjunto $(\mathbb{Z}/p)^{\times} = \mathbb{Z}/p \setminus \{0\}$ de enteros módulo p inversibles con la multiplicación usual, donde p es un número primo.

Si $G = \{g_1, g_2, \ldots, g_n\}$ es un grupo finito, la **tabla** del grupo G es la matriz de $n \times n$ que en el lugar i, j tiene al elemento $g_i g_j$. Esta tabla se conoce en la literatura como la *tabla de multiplicación* del grupo. Como esta terminología puede resultar confusa en caso de trabajar con grupos aditivos, preferimos hablar simplemente de tablas de un grupo y no hacer referencia al tipo de operación involucrada. Como ejemplo, vemos que la tabla del grupo $\mathbb{Z}/4$ es

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ejemplo 1.9. Sea $H = \{1, -1, i, -i, j, -j, k, -k\}$ con la multiplicación dada por las siguientes reglas:

$$i^2 = j^2 = k^2 = ijk = -1.$$

Dejamos como ejercicio calcular la tabla de H y verificar que H es un grupo.

Vimos que $\mathbb{Z}$ con la suma usual forma un grupo. Veamos la versión multiplicativa del mismo fenómeno. Primero, un poco de notación. Sea G un grupo y sea $g \in G$. Si $k \in \mathbb{Z} \setminus \{0\}$, escribimos

$$\begin{aligned} g^k &= g \cdots g \quad (k - \text{veces}) && \text{si } k > 0, \\ g^k &= g^{-1} \cdots g^{-1} \quad (|k| - \text{veces}) && \text{si } k < 0. \end{aligned}$$

Por convención, además, $g^0 = 1$.

Ejercicio 1.10. Si G es un grupo, entonces

1) $(g^k)^l = g^{kl}$ para todo $g \in G$ y todo $k, l \in \mathbb{Z}$.
2) Si G es abeliano, entonces $(gh)^k = g^k h^k$ para todo $g, h \in G$ y todo $k \in \mathbb{Z}$.

Ahora sí, el ejemplo.

Ejemplo 1.11. Fijemos formalmente un símbolo g y consideremos el conjunto de potencias enteras de g,

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

con la convención $g^0 = 1$. Entonces $\langle g \rangle$ con la operación $g^i g^j = g^{i+j}$ es un grupo abeliano.

Más adelante veremos que $\mathbb{Z}$ y el grupo que vimos en el ejemplo anterior son objetos indistinguibles para la teoría de grupos, aunque como conjuntos sean completamente distintos.

Ejemplo 1.12. Sea $n \in \mathbb{N}$. El conjunto $G_n = \{z \in \mathbb{C} : z^n = 1\}$ es un grupo abeliano con el producto usual de números complejos. También $\cup_{n \geq 1} G_n$ es un grupo abeliano.

Ejemplo 1.13. Sea $n \geq 2$. El conjunto $\mathbf{GL}_n(\mathbb{R})$ de matrices inversibles de $n \times n$ con la multiplicación usual de matrices es un grupo no abeliano.

Ejemplo 1.14. Sea X un conjunto. El conjunto $\mathbb{S}_X$ de funciones $X \to X$ biyectivas con la composición de funciones es un grupo. Si $|X| \geq 3$, el grupo $\mathbb{S}_X$ no es abeliano: sean tres elementos distintos $a, b, c \in X$ y sean $f\colon X \to X$ biyectiva tal que $f(a) = b$, $f(b) = c$ y $f(c) = a$ y $g\colon X \to X$ biyectiva tal que $g(a) = b$, $g(b) = a$ y $g(x) = x$ para todo $x \in X \setminus \{a, b\}$. Entonces $fg \neq gf$.

Si $X = \{1, 2, \ldots, n\}$, $\mathbb{S}_X$ será denotado por $\mathbb{S}_n$ y se denominará el **grupo simétrico** de grado n. Los elementos de $\mathbb{S}_n$ serán denominados **permutaciones** de grado n. Notemos que $|\mathbb{S}_n| = n!$ y que $\mathbb{S}_n$ es abeliano si y sólo si $n \in \{1, 2\}$. Cada elemento de $\mathbb{S}_n$ es una función $f\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ y por lo tanto puede escribirse como nos resulte conveniente. Una notación bastante utilizada es la siguiente: escribiremos

$$\begin{pmatrix} 12345 \\ 32145 \end{pmatrix}$$

para denotar a la función $f\colon \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ tal que $f(1) = 3$, $f(2) = 2$, $f(3) = 1$, $f(4) = 4$ y $f(5) = 5$.

Ejemplo 1.15 (el grupo de Klein). El grupo

$$K = \left\{ \mathrm{id}, \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} \right\}$$

es un grupo abeliano. Observar que K está contenido en $\mathbb{S}_4$. Dejamos como ejercicio calcular la tabla del grupo de Klein.

Ejemplo 1.16. Sabemos que el conjunto $\mathbb{S}_3$ de funciones $\{1,2,3\} \to \{1,2,3\}$ biyectivas es un grupo con la composición. El grupo $\mathbb{S}_3$ tiene orden seis y sus elementos son las permutaciones

$$\mathrm{id}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

Otra notación muy utilizada involucra la *descomposición de una permutación en ciclos disjuntos*. En este caso, los elementos de $\mathbb{S}_3$ serán escritos como

$$\mathrm{id}, (12), (13), (23), (123), (132),$$

donde, por ejemplo, el símbolo (12) representa la función $\{1,2,3\} \to \{1,2,3\}$ tal que $1 \mapsto 2$, $2 \mapsto 1$ y $3 \mapsto 3$. Queda como ejercicio calcular la tabla del grupo $\mathbb{S}_3$.

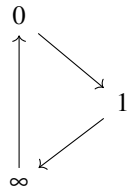
Más adelante veremos que la notación de una permutación como producto de ciclos disjuntos es de gran utilidad.

Ejemplo 1.17. El conjunto de funciones

$$G = \left\{ x, \frac{1}{x}, 1-x, \frac{1}{1-x}, \frac{x}{x-1}, \frac{x-1}{x} \right\}$$

es un grupo no abeliano con la composición usual de funciones.

Si definimos $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ y suponemos que valen las reglas $1/\infty = 0$, $1/\infty$, $\infty/\infty = 1$, $1 - \infty = \infty - 1 = \infty$, entonces vemos que G es el conjunto de funciones biyectivas $\{0,1,\infty\} \to \{0,1,\infty\}$. Observemos por ejemplo que la función $x \mapsto \frac{1}{x}$ puede itentificarse con la permutación del conjunto $\{0,1,\infty\}$ que intercambia 0 y ∞ y fija al 1. Similarmente, la función $\frac{1}{1-x}$ puede identificarse con la permutación que permuta cíclicamente los elementos de $\{0,1,\infty\}$, es decir



Más adelante veremos que las similitudes entre los grupos que aparecen en los ejemplos 1.16 y 1.17 no son accidentes, tenemos distintas representaciones para objetos indistinguibles desde la teoría de grupos.

Ejemplo 1.18. Sea $n \in \mathbb{N}$. Las unidades de $\mathbb{Z}/n$ forman un grupo con la multiplicación usual módulo n. La notación que utilizaremos es

$$\mathscr{U}(\mathbb{Z}/n) = \{x \in \mathbb{Z}/n : \text{mcd}(x,n) = 1\}.$$

En general, el orden de $\mathscr{U}(\mathbb{Z}/n)$ es $\varphi(n)$, donde φ denota a la función de Euler, es decir

$$\varphi(n) = |\{x \in \mathbb{Z} : 1 \leq x \leq n, \text{mcd}(x,n) = 1\}|.$$

Veamos un ejemplo concreto: la tabla del grupo $\mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\}$ es

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Ejercicio 1.19. Sean G y H grupos. El conjunto $G \times H$ es un grupo con la operación

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2).$$

Esta estructura de grupo sobre el producto cartesiano $G \times H$ se conoce como el **producto directo** de G y H.

Si se utiliza la inducción, el ejemplo anterior puede generalizarse productos finitos de tres o más grupos.

Definición 1.20. Un subconjunto S de G es un **subgrupo** de G si se satisfacen las siguientes propiedades:

1) $1 \in S$,
2) $x \in S \implies x^{-1} \in S$, y además
3) $x, y \in S \implies xy \in S$.

Notación: S es un subgrupo de G si y sólo si $S \leq G$.

Podríamos reemplazar la primera condición de la definición de subgrupo y pedir simplemente que el conjunto sea no vacío.

Ejemplo 1.21. Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G.

Ejemplo 1.22. $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Ejemplo 1.23. $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Ejemplo 1.24. Para cada $n \in \mathbb{N}$, definimos el grupo de raíces n-ésimas de la unidad como $G_n = \{z \in \mathbb{C} : z^n = 1\}$, es decir

$$G_n = \{1, \exp(2\pi i/n), \exp(4i\pi/n), \ldots, \exp(2(n-1)i\pi/n)\}.$$

Entonces

$$G_n \leq \bigcup_{n \in \mathbb{N}} G_n \leq S^1 \leq \mathbb{C}^\times.$$

Ejercicio 1.25. Si G un grupo, el **centro**

$$Z(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}$$

de G es un subgrupo de G.

Ejercicio 1.26. Si G es un grupo y $g \in G$, entonces el **centralizador**

$$C_G(g) = \{h \in G : gh = hg\}$$

de g en G es un subgrupo de G.

Ejercicio 1.27. Demuestre que $Z(\mathbb{S}_3) = \{\mathrm{id}\}$ y calcule $C_{\mathbb{S}_3}((12))$.

Una forma útil de chequear que un cierto subconjunto de un grupo es un subgrupo es la siguiente:

Ejercicio 1.28. Sea G un grupo y sea S un subconjunto de G. Demuestre que S es un subgrupo de G si y sólo si S es no vacío y para todo $x, y \in S$ vale que $xy^{-1} \in S$.

Ejemplo 1.29. $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$. En efecto, la matriz identidad pertenece a $\mathbf{SL}_2(\mathbb{R})$ y luego $\mathbf{SL}_2(\mathbb{R})$ es no vacío. Además si $a, b \in \mathbf{SL}_n(\mathbb{R})$, entonces $ab^{-1} \in \mathbf{SL}_2(\mathbb{R})$ pues $\det(ab^{-1}) = \det(a)\det(b)^{-1} = 1$.

Ejemplo 1.30. Sea $n \in \mathbb{N}$ y sean

$$r = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Se define el **grupo diedral** $\mathbb{D}_n$ como el subgrupo de $\mathbf{GL}_2(\mathbb{C})$ generado por r y s, es decir $\mathbb{D}_n = \langle r, s \rangle$. Un cálculo sencillo muestra que

$$r^n = s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad srs = r^{-1}.$$

Un elemento arbitrario de $\mathbb{D}_n$ es una palabra de la forma $r^{i_1} s^{j_1} r^{i_2} s^{j_2} \cdots$, donde $i_1, i_2, \cdots \in \{0, 1, \ldots, n-1\}$ y $j_1, j_2, \cdots \in \{0, 1\}$. Como $rs = sr^{-1}$, se concluye que todo elemento de $\mathbb{D}_n$ puede escribirse como $r^i s_j$, donde $i \in \{0, \ldots, n-1\}$ y $j \in \{0, 1\}$. Luego $|\mathbb{D}_n| = 2n$.

Para fijar ideas es conveniente hacer el ejemplo anterior en algunos casos particulares. En el caso $n = 3$, tendríamos

$$r = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

y obtnedríamos otra representación para el grupo de simetrías de un triángulo regular. En el caso $n = 4$ tendríamos

$$r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

y obtendríamos el grupo de simetrías de un cuadrado.

Ejercicio 1.31. La intersección de subgrupos es también un subgrupo.

La unión de subgrupos no es, en general, un subgrupo. Para convencerse, basta por ejemplo ver qué pasa en el subgrupo de Klein.

Teorema 1.32. *Si S es un subgrupo de $\mathbb{Z}$, entonces $S = m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ para algún $m \in \mathbb{N}_0$.*

Demostración. Si $S = \{0\}$, no hay nada para demostrar pues podemos tomar $m = 0$. Supongamos entonces que $S \neq \{0\}$ y sea $m = \text{mín}\{s \in S : s > 0\}$. Este mínimo existe porque, como S es no nulo, S contiene un elemento $n \in S \setminus \{0\}$. Existen entonces dos situaciones posibles: $n > 0$ o bien $-n > 0$. Y como S es un subgrupo de $\mathbb{Z}$, $-n \in S$.

Vamos a demostrar ahora que $S = n\mathbb{Z}$. Si $x \in S$, entonces $x = my + r$ para $y, r \in \mathbb{Z}$ con r tal que $0 \leq r < m$. Supongamos que $r \neq 0$. Como $x, m \in S$, entonces $r \in S$, una contradicción a la minimalidad de S. Luego $r = 0$ y entonces $x = my \in m\mathbb{Z}$. Recíprocamente, como $n \in S$, entonces $nk \in S$ para todo $k \in \mathbb{Z}$. En efecto, si $k = 0$, $nk = 0 \in S$. Si $k > 0$, entonces

$$\underbrace{n + \cdots + n}_{k-\text{veces}} \in S.$$

Por último, si $k < 0$, entonces

$$nk = \underbrace{-n + (-n) + \cdots + (-n)}_{|k|-\text{veces}} \in S. \qquad \square$$

Como la intersección de subgrupos es un subgrupo, el resultado anterior tiene además aplicaciones muy interesantes. Recordemos que si $a, b \in \mathbb{Z}$ se dice que a divide a b (o que b es divisible por a) si $b = ac$ para algún $c \in \mathbb{Z}$. La notación:

$$a \mid b \iff b = ac \text{ para algún } c \in \mathbb{Z}.$$

Si $a, b \in \mathbb{Z}$ son tales que $ab \neq 0$, entonces

$$S = a\mathbb{Z} + b\mathbb{Z} = \{m \in \mathbb{Z} : m = ar + bs \text{ para } r, s \in \mathbb{Z}\}$$

es un subgrupo de $\mathbb{Z}$ (ejercicio). El teorema anterior nos permite escribir a S como $S = d\mathbb{Z}$ para algún entero positivo d. Este entero d es el **máximo común divisor** de a y b, es decir $d = \text{mcd}(a, b)$. La terminología queda justificada por la siguiente proposición:

Proposición 1.33. *Sean $a, b \in \mathbb{Z}$ tales que $ab \neq 0$ y sea $d = \text{mcd}(a, b)$. Valen entonces las siguientes afirmaciones:*

1) d divide simultáneamente a los enteros a y b.
2) Si $e \in \mathbb{Z}$ divide a los enteros a y b, entonces e también divide a d.
3) Existen $r,s \in \mathbb{Z}$ tales que $d = ar + bs$.

Demostración. Como $d \in S$, existen $r,s \in \mathbb{Z}$ tales que $d = ar+bs$, esto demuestra la tercera afirmación. Si $e \in \mathbb{Z}$ es tal que $e \mid a$ y $e \mid b$, entonces $e \mid ar+bs = d$, lo que demuestra la segunda afirmación. Finalmente, la primera afirmación queda demostrada al observar que $a,b \in S$. □

Dos enteros a y b se dirán **coprimos** si y sólo si el único entero positivo que divide simultáneamente a ambos es 1, es decir

$$\begin{aligned} a \text{ y } b \text{ son coprimos} &\iff \operatorname{mcd}(a,b) = 1 \iff \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \\ &\iff \text{existen } r,s \in \mathbb{Z} \text{ tales que } ar+bs = 1. \end{aligned}$$

Proposición 1.34. *Sea p un primo y sean $a,b \in \mathbb{Z}$. Si $p \mid ab$, entonces $p \mid a$ o bien $p \mid b$.*

Demostración. Si $p \nmid a$, entonces $\operatorname{mcd}(a,p) = 1$, lo que implica que $1 = ra+sp$ para ciertos $r,s \in \mathbb{Z}$. Al multiplicar por b en ambos miembros, vemos que $b = r(ab)+spb$ es divisible por p, pues $p \mid ab$ por hipótesis. □

Si S y T son subgrupos de $\mathbb{Z}$, entonces $S \cap T$ es también un subgrupo de $\mathbb{Z}$. Sean $a,b \in \mathbb{Z}$ tales que $ab \neq 0$. Como $a\mathbb{Z} \cap b\mathbb{Z}$ es un subgrupo no nulo de $\mathbb{Z}$ (pues contiene al entero $ab \neq 0$), podemos escribir $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ para algún $m \in \mathbb{N}$. Ese entero positivo m es el **mínimo común múltiplo** de a y b y se denota por $m = \operatorname{mcm}(a,b)$. La terminología queda justificada por la siguinte proposición.

Proposición 1.35. *Sean $a,b \in \mathbb{Z} \setminus \{0\}$ y sea $m = \operatorname{mcm}(a,b)$. Valen entonces las siguientes propiedades:*

1) m es simultáneamente divisible por a y b.
2) Si n es simultáneamente divisible por a y b, entonces n es divisible por m.

Demostración. Como $m \in a\mathbb{Z} \cap b\mathbb{Z}$, entonces $a \mid m$ y además $b \mid m$. Si $a \mid n$ y además $b \mid n$, digamos $n = ax = by$ para ciertos $x,y \in \mathbb{Z}$, entonces $n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, lo que implica que $m \mid n$. □

Proposición 1.36. *Sean $a,b \in \mathbb{N}$. Si $d = \operatorname{mcd}(a,b)$ es el máximo común divisor de a y b y $m = \operatorname{mcm}(a,b)$ es el mínimo común múltiplo de a y b, entonces $ab = dm$.*

Demostración. Como $b/d \in \mathbb{Z}$, entonces $a \mid a(b/d)$. Similarmente, $b \mid a(b/d)$. Como entonces $m \mid a(b/d)$, se concluye que $dm \mid ab$. Sean $r,s \in \mathbb{Z}$ tales que $d = ra+sb$. Al multiplicar por m en ambos miembros, vemos que $dm = ram+sbm$ es divisible por ab. □

Ejercicio 1.37. Sea S un subgrupo de G y sea $g \in G$. Demuestre que el **conjugado** gSg^{-1} de S por g es también un subgrupo de G. Notación: ${}^gS = gSg^{-1}$.

Definición 1.38. Sean G un grupo y X un subconjunto de G. El **subgrupo generado** por X se define como la intersección de todos los subgrupos de G que contienen a X, es decir

$$\langle X\rangle = \bigcap\{S : S \leq G, X \subseteq S\}.$$

Cuando el conjunto de generadores sea finito, se utilizará la siguiente notación. Si $X = \{g_1,\dots,g_k\}$, entonces $\langle X\rangle = \langle\{g_1,\dots,g_k\}\rangle = \langle g_1,\dots,g_k\rangle$.

Ejercicio 1.39. Demuestre que $\langle X\rangle$ es el menor subgrupo de G que contiene a X, es decir que si H es un subgrupo de G tal que $X \subseteq H$, entonces $\langle X\rangle \subseteq H$.

Ejercicio 1.40. Demuestre que

$$\langle X\rangle = \{x_1^{n_1}\cdots x_k^{n_k} : k \in \mathbb{N}, x_1,\dots,x_k \in X, -1 \leq n_1,\dots,n_k \leq 1\}.$$

Ejemplo 1.41. El conjunto

$$D_4 = \{\mathrm{id}, (1234), (1432), (13)(24), (14)(23), (12)(34), (24), (13)\}$$

es un subgrupo no abeliano de $\mathbb{S}_4$. Observar que D_4 está generado por las permutaciones $(12)(34)$ y (1234).

Ejemplo 1.42. Para $n \geq 2$ y $\theta = 2\pi/n$ sean

$$r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Se define entonces al **grupo diedral** $\mathbb{D}_n$ como el subgrupo de $\mathbf{GL}_2(\mathbb{R})$ generado por r y s, es decir $\mathbb{D}_n = \langle r, s\rangle$. Observar que

$$s^2 = r^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad srs = r^{-1}.$$

Además $|\mathbb{D}_n| = 2n$.

Es conveniente mencionar que la notación que suele usarse para el grupo diedral no es estándar. Para nosotros $\mathbb{D}_n$ será el grupo diedral de orden $2n$.

Definición 1.43. El **conmutador** $[G,G]$ de G es el subgrupo generado por los conmutadores, es decir

$$[G,G] = \langle [x,y] \mid x,y \in G\rangle,$$

donde $[x,y] = xyx^{-1}y^{-1}$ es el conmutador de x e y.

El subgrupo generado por los conmutadores de un grupo G a veces se conoce como el **subgrupo derivado** de G.

Ejemplo 1.44. $[\mathbb{Z},\mathbb{Z}] = \{0\}$ pues $\mathbb{Z}$ es un grupo abeliano. Obviamente, en este ejemplo utilizamos la notación aditiva.

Ejercicio 1.45. Demuestre que $[\mathbb{S}_3, \mathbb{S}_3] = \{\mathrm{id}, (123), (132)\}$.

Es natural preguntarse por qué el conmutador se define como el subgrupo generado por los conmutadores y no directamente como el subconjunto formado por los conmutadores. En realidad, esto se hace porque no es cierto que el subconjunto formado por los conmutadores sea un subgrupo, aunque no es muy fácil conseguir ejemplos. Con ayuda de algún software de matemática que permita trabajar con grupos, se pueden verificar los ejemplos que mencionamos a continuación. Tomamos el siguiente ejemplo del libro de Carmichael [2].

Ejemplo 1.46. Sea G el subgrupo de $\mathbb{S}_{16}$ generado por las permutaciones

$$\begin{aligned} a &= (13)(24), & b &= (57)(68), \\ c &= (9\,11)(10\,12), & d &= (13\,15)(14\,16), \\ e &= (13)(57)(9\,11), & f &= (12)(34)(13\,15), \\ g &= (56)(78)(13\,14)(15\,16), & h &= (9\,10)(11\,12). \end{aligned}$$

Puede demostrarse que $[G,G]$ tiene orden 16 y que el conjunto de conmutadores tiene tamaño 15.

Mencionamos otro ejemplo, encontrado por Guralnick [3] antes de que el uso de computadoras en teoría de grupos fuera masivo.

Ejemplo 1.47. El grupo

$$G = \langle (135)(246)(7\,11\,9)(8\,12\,10), (394\,10)(58)(67)(11\,12) \rangle.$$

tiene orden 96 y su subgrupo de conmutadores de G no es igual al conjunto de conmutadores. Puede demostrarse además que es el menor grupo finito con esta propiedad.

Capítulo 2
Grupos cíclicos

Definición 2.1. Un grupo G se dice **cíclico** si $G = \langle g \rangle$ para algún $g \in G$.

Un grupo cíclico G generado por el elemento g estará compuesto entonces por las potencias de g, es decir $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$. Todo grupo cíclico es entonces en particular un grupo abeliano.

Ejemplos 2.2.

1) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2) $\mathbb{Z}/n = \langle 1 \rangle$.
3) $G_n = \langle \exp(2i\pi/n) \rangle$.

Ejemplo 2.3. $\mathscr{U}(\mathbb{Z}/8) \neq \langle 3 \rangle$. De hecho, $\langle 3 \rangle = \{1,3\} \subsetneq \{1,3,5,7\} = \mathscr{U}(\mathbb{Z}/8)$.

Antes de resolver el siguiente ejercicio, es conveniente recordar cómo son los subgrupos de $\mathbb{Z}$.

Ejercicio 2.4. Todo subgrupo de un grupo cíclico es también un grupo cíclico.

Definición 2.5. Sean G un grupo y $g \in G$. El **orden** de g se define como el orden del subgrupo generado por g. Notación: $|g| = |\langle g \rangle|$.

Teorema 2.6. *Sean G un grupo, $g \in G$ y $n \in \mathbb{N}$. Las siguientes afirmaciones son equivalentes:*

1) $|g| = n$.
2) $n = \min\{k \in \mathbb{N} : g^k = 1\}$.
3) Para todo $k \in \mathbb{Z}$, $g^k = 1 \iff n \mid k$.
4) $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ *y los* $1, g, \ldots, g^{n-1}$ *son todos distintos.*

Demostración. Veamos que $(1) \implies (2)$. Si $g = 1$ entonces $n = 1$. Supongamos entonces que $g \neq 1$. Como $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$, sabemos que existen enteros positivos $i > j$ tales que $g^i = g^j$, es decir $g^{i-j} = 1$. En particular, el conjunto $\{k \in \mathbb{N} : g^k = 1\}$ es no vacío y posee entonces elemento mínimo, digamos

$$d = \text{mín}\{k \in \mathbb{N} : g^k = 1\}.$$

Tenemos entonces que $\langle g \rangle \subseteq \{1, g, \ldots, g^{d-1}\} \subseteq \langle g \rangle$. En efecto, si $g^k \in \langle g \rangle$, entonces $k = dq + r$ para $q, r \in \mathbb{Z}$ con $0 \leq r < d$. Como $g^d = 1$,

$$g^k = g^{dq+r} = (g^d)^q g^r = g^r \in \{1 = g^0, g, g^2, \ldots, g^{d-1}\}$$

Por otro lado, es trivial observar que $\{1, g, \ldots, g^{d-1}\} \subseteq \langle g \rangle$ y que $\{1, g, \ldots, g^{d-1}\}$ tiene d elementos.

Ahora demostremos que (2) $\implies$ (3). Supongamos que $g^k = 1$. Si escribimos $k = nt + r$ con $0 \leq r < n$, entonces $g^k = g^{nt+r} = g^r$. La minimalidad de n implica entonces que $r = 0$ y luego n divide a k. Recíprocamente, si $k = nt$ para algún $t \in \mathbb{Z}$, entonces $g^k = (g^n)^t = 1$.

Demostremos que (3) $\implies$ (4). Es trivial que $\{1, g, \ldots, g^{n-1}\} \subseteq \langle g \rangle$. Para demostrar la otra inclusión, escribimos $k = nt + r$ con $0 \leq r \leq n - 1$. Entonces

$$g^k = g^{nt+r} = (g^n)^t g^r = g^r$$

pues por hipótesis $g^n = 1$. Para ver que los $1, g, \ldots, g^{n-1}$ son todos distintos, basta observar que si $g^k = g^l$ con $0 \leq k < l \leq n - 1$, entonces, como $g^{l-k} = 1$ y además $0 < l - k \leq n - 1$, se concluye $n \leq l - k$ ya que por hipótesis n divide a $l - k$, una contradicción.

La implicación (4) $\implies$ (1) es trivial. □

Veamos una aplicación de la proposición anterior:

Corolario 2.7. *Si G es un grupo y $g \in G$ tiene orden n, entonces*

$$|g^m| = \frac{n}{\text{mcd}(n, m)}.$$

Demostración. Sea k tal que $(g^m)^k = 1 = g^{mk}$. Esto es equivalente a decir que n divide a km, pues g tiene orden n. A su vez esto es equivalente a pedir que n/d divida a mk/d, donde $d = \text{mcd}(n, m)$. En consecuencia, como los enteros n/d y m/d son coprimos, $(g^m)^k = 1$ es equivalente a pedir que n/d divida a k, que implica que g^m tiene orden n/d. □

Ejercicio 2.8. Sea G un grupo y sea $g \in G$. Demuestre que las siguientes afirmaciones son equivalentes:

1) g tiene orden infinito.
2) El conjunto $\{k \in \mathbb{N} : g^k = 1\}$ es vacío.
3) Si $g^k = 1$, entonces $k = 0$.
4) Si $k \neq l$, entonces $g^k \neq g^l$.

Ejercicio 2.9. Sea G un grupo y sea $g \in G \setminus \{1\}$. Demuestre las siguientes afirmaciones:

1) $|g| = 2$ si y sólo si $g = g^{-1}$.

2) $|g| = |g^{-1}|$.
3) Si $|g| = nm$', entonces $|g^m| = n$.

Ejercicio 2.10. Sea G un grupo abeliano. Demuestre que $T(G) = \{g \in G : |g| < \infty\}$ es un subgrupo de G. Calcule $T(\mathbb{C}^\times)$.

Ejercicio 2.11. Sea $G = \langle g \rangle$ un grupo cíclico.

1) Si G es infinito, los únicos generadores de G son g y g^{-1}.
2) Si G es finito de orden n, $G = \langle g^k \rangle$ si y sólo si k es coprimo con n.

El siguiente ejercicio es un caso particular del teorema de Cauchy, que veremos más adelante.

Ejercicio 2.12. Demuestre que todo grupo de orden par contiene un elemento de orden dos.

Mostremos ahora algunos órdenes de elementos concretos:

Ejemplo 2.13. En $\mathbb{S}_3$ tenemos los siguiente:

$$|\mathrm{id}| = 1, \quad |(12)| = |(13)| = |(23)| = 2, \quad |(123)| = |(132)| = 3.$$

Ejemplo 2.14. En $\mathbb{Z}$ todo elemento no nulo tiene orden infinito.

Ejemplo 2.15. En $\mathbb{Z} \times \mathbb{Z}/6$ hay elementos de orden finito y elementos de orden infinito. Por ejemplo, $(1,0)$ tiene orden infinito y $(0,1)$ tiene orden seis.

Ejercicio 2.16. Calcule los órdenes de los elementos de $\mathbb{Z}/6$.

Ejemplo 2.17. La matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ tiene orden infinito.

Ejemplo 2.18. El grupo $G_\infty = \bigcup_{n \geq 1} G_n$ es abeliano e infinito. Todo elemento de G_∞ tiene orden finito.

Ejercicio 2.19. Pruebe que la matrix $a = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ tiene orden cuatro, que la matrix $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ tiene orden tres y calcule el orden de ab.

Ejercicio 2.20. Calcule el orden de la matriz $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

Ejercicio 2.21. Demuestre que en $\mathbb{D}_n$ se tiene $|r^j s| = 2$ y $|r^j| = n/\operatorname{mcd}(n,j)$. Demuestre además que $\mathbb{D}_n$ tiene orden $2n$.

Ejercicio 2.22. Demuestre que un grupo con finitos subgrupos es finito.

Capítulo 3
El teorema de Lagrange

Sean G un grupo y H un subgrupo de G. Diremos que dos elementos $x, y \in G$ son equivalentes a izquierda módulo H si $x^{-1}y \in H$. Usaremos la siguiente notación:

$$x \equiv y \text{ mód } H \iff x^{-1}y \in H. \tag{3.1}$$

Ejercicio 3.1. Demuestre que (3.1) una relación de equivalencia. Esto significa que se tienen las siguientes propiedades:

1) $x \equiv x$ mód H para todo x.
2) Si $x \equiv y$ mód H, entonces $y \equiv x$ mód H.
3) Si $x \equiv y$ mód H y además $y \equiv z$ mód H, entonces $x \equiv z$ mód H.

Las clases de equivalencia de esta relación módulo H son los conjuntos de la forma $xH = \{xh : h \in H\}$ pues la clase de un cierto elemento $x \in G$ es el conjunto

$$\{y \in G : x \equiv y \text{ mód } H\} = \{y \in G : x^{-1}y \in H\} = \{y \in G : y \in xH\} = xH.$$

El conjunto xH se llama **coclase a izquierda** de H en G.

Tener una relación de equivalencia módulo H nos permite escribir a G como unión disjunta de coclases distintas de H en G, pues dos coclases cualesquiera son iguales o disjuntas.

Proposición 3.2. *Sean G un grupo y H un subgrupo de G.*

1) Si $xH \cap yH \neq \emptyset$, entonces $xH = yH$.
2) El grupo G puede descomponerse como unión disjunta de distintas coclases a izquierda de H.

Demostración. Demostremos la primera afirmación. Si $g \in xH \cap yH$, escribimos $g = xh$ para algún $h \in H$ y entonces

$$gH = (xh)H = x(hH) = xH.$$

Similarmente, $gH = yH$. En consecuencia, $xH = yH$.

La segunda afirmación se obtiene inmediatamente de la primera. □

Podríamos haber definido coclases a derecha mediante la relación $x \equiv y$ mód H si y sólo si $xy^{-1} \in H$. En este caso, las clases de equivalencia serían los conjuntos Hx con $x \in X$. Hx se llama **coclase a derecha** de H en G.

Proposición 3.3. *Si H es un subgrupo de G, entonces $|Hx| = |H| = |xH|$ para todo $x \in G$.*

Demostración. Sea $x \in G$. La función $H \to Hx$, $h \mapsto hx$, es una biyección con inversa $hx \mapsto h$. Análogamente se demuestra que la función $H \to xH$, $h \mapsto xh$, es una biyección. □

La función

$$\{\text{coclases a derecha de } H \text{ en } G\} \to \{\text{coclases a izquierda de } H \text{ en } G\}$$

dada por $Hx \mapsto x^{-1}H$ es una biyección pues

$$Hx = Hy \iff xy^{-1} \in H \iff (x^{-1})^{-1}y^{-1} \in H \iff x^{-1}H = y^{-1}H.$$

En particular, la cantidad de coclases a derecha de H en G coincide con la cantidad de coclases a izquierda de H en G.

Ejemplo 3.4. Si $G = \mathbb{Z}$ y $S = n\mathbb{Z}$, entonces

$$a + S = \{a + nq : q \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv a \text{ mód } n\}.$$

Ejemplo 3.5. Los subgrupos de $\mathbb{S}_3$ son $\{\text{id}\}$, $\mathbb{S}_3$, los subgrupos $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$ de orden dos y el subgrupo $\langle(123)\rangle = \{\text{id}, (123), (132)\}$ de orden tres. Si $H = \langle(12)\rangle = \{\text{id}, (12)\}$, entonces

$$\begin{aligned} H &= (12)H = \{\text{id}, (12)\}, \\ (123)H &= (13)H = \{(13), (123)\}, \\ (132)H &= (23)H = \{(23), (132)\}. \end{aligned}$$

Observemos que en este caso se tiene la descomposición

$$\mathbb{S}_3 = H \cup (123)H \cup (132)H \quad \text{(unión disjunta)}.$$

Ejemplo 3.6. Sea $G = \mathbb{R}^2$ con la suma usual y sea $v \in \mathbb{R}^2$. La recta $L = \{\lambda v : \lambda \in \mathbb{R}\}$ es un subgrupo de G y para cada $p \in R^2$, la coclase $p + L$ es la recta paralela a L que pasa por el punto p.

Definición 3.7. Si H es un subgrupo de G, se define el **índice** de H en G como la cantidad $(G : H)$ de coclases a izquierda (o a derecha) de H en G.

Teorema 3.8 (Lagrange). *Si G es un grupo finito y H es un subgrupo de G, entonces $|G| = |H|(G : H)$. En particular, $|H|$ divide a $|G|$.*

Demostración. Tenemos una relación de equivalencia módulo H que nos permite descomponer en G en clases de equivalencia, digamos

$$G = \bigcup_{i=1}^{n} x_i H \quad \text{(unión disjunta)}$$

para ciertos $x_1, \ldots, x_n \in G$, donde $n = (G : H)$. Como cada una de esas clases tiene exáctamente $|H|$ elementos,

$$|G| = \sum_{i=1}^{n} |x_i H| = \sum_{i=1}^{n} |H| = |H|(G : H). \qquad \square$$

Veamos algunos corolarios.

Corolario 3.9. *Si G es un grupo finito y $g \in G$, entonces $g^{|G|} = 1$.*

Demostración. Por definición $|g| = |\langle g \rangle|$. El teorema de Lagrange aplicado al subgrupo $H = \langle g \rangle$ nos dice que

$$g^{|G|} = g^{|H|(G:H)} = (g^{|H|})^{(G:H)} = 1. \qquad \square$$

Corolario 3.10. *Si G es un grupo de orden primo, entonces G es cíclico.*

Demostración. Sea $g \in G \setminus \{1\}$ y sea $H = \langle g \rangle$. Por el teorema de Lagrange, $|H|$ divide a $|G|$ y luego $|H| = |G|$ pues $|G|$ es un número primo. En consecuencia, $G = H = \langle g \rangle$. $\square$

Corolario 3.11. *Si G es un grupo abeliano y $g, h \in G$ son elementos de órdenes finitos y coprimos, entonces $|gh| = |g||h|$.*

Demostración. Sean $n = |g|$, $m = |h|$ y $l = |gh|$. Como G es abeliano,

$$(gh)^{nm} = (g^n)^m (h^m)^n = 1$$

y luego l divide a nm. Por otro lado, como $(gh)^l = 1$, $g^l = h^{-l} \in \langle g \rangle \cap \langle h \rangle = \{1\}$ (pues como $|\langle g \rangle| = n$ y $|\langle h \rangle| = m$ son coprimos, entonces nm divide a l gracias al teorema de Lagrange). $\square$

El pequeño teorema de Fermat es un caso particular del teorema de Lagrange.

Ejercicio 3.12 (pequeño teorema de Fermat). Sea p un número primo. Demuestre que $a^{p-1} \equiv 1$ mód p para todo $a \in \{1, 2, \ldots, p-1\}$.

El siguiente corolario utiliza la función φ de Euler. Recordemos que $\varphi(n)$ es la cantidad de enteros positivos $k \in \{1, \ldots, n\}$ coprimos con n. El grupo de unidades de $\mathbb{Z}/n$ tiene $\varphi(n)$ elementos (pues $x \in \mathbb{Z}/n$ es inversible si y sólo si x es coprimo con n).

Ejercicio 3.13 (teorema de Euler). Sean a y n enteros coprimos. Demuestre que $a^{\varphi(n)} \equiv 1$ mód n.

No vale la recíproca del teorema de Lagrange.

Ejemplo 3.14. Consideremos el grupo alternado

$$\begin{aligned}\mathbb{A}_4 = \{&\mathrm{id}, (234), (243), (12)(34), (123), (124),\\ &(132), (134), (13)(24), (142), (143), (14)(23)\} \leq \mathbb{S}_4.\end{aligned}$$

Vamos a demostrar que $\mathbb{A}_4$ no tiene subgrupos de orden seis. Si $H \leq \mathbb{A}_4$ es tal que $|H| = 6$, entonces, como $(\mathbb{A}_4 : H) = 2$, para todo $x \notin H$ podríamos descomponer a $\mathbb{A}_4$ como $\mathbb{A}_4 = H \cup xH$ (unión disjunta).

Afirmamos que para todo $g \in \mathbb{A}_4$ vale que $g^2 \in H$ (pues si $g \notin H$, entonces, como $g^2 \in \mathbb{A}_4 = H \cup gH$, se concluye que $g^2 \in H$). En particular, como $(ijk) = (ikj)^2$, todos los elementos de orden tres de $\mathbb{A}_4$ están en el subgrupo H, una contradicción pues hay ocho elementos de orden tres.

Todos deberíamos tener un grupo favorito. El mío es $\mathbf{SL}_2(3)$, el grupo formado por las matrices de 2×2 con coeficientes en $\mathbb{Z}/3$ con determinante uno.

Ejercicio 3.15. Demuestre que

$$\mathbf{SL}_2(3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1, a, b, c, d \in \mathbb{Z}/3 \right\}$$

es un grupo de orden 24 que no posee subgrupos de orden 12.

Capítulo 4
El grupo simétrico

Sea $\sigma \in \mathbb{S}_n$. Diremos que σ es un r-ciclo si existen $a_1, \ldots, a_r \in \{1, \ldots, n\}$ tales que $\sigma(j) = j$ para todo $j \notin \{a_1, \ldots, a_r\}$ y

$$\sigma(a_i) = \begin{cases} a_{i+1} & \text{si } i < r, \\ a_1 & \text{si } i = r. \end{cases}$$

Ejemplos 4.1. Por ejemplo, (12), (13) y (23) son 2-ciclos de $\mathbb{S}_3$. Los 2-ciclos se denominan **trasposiciones**. Las permutaciones (123) y (132) son 3-ciclos de $\mathbb{S}_3$.

Dos permutaciones $\sigma, \tau \in \mathbb{S}_n$ se dicen **disjuntas** si para todo $j \in \{1, \ldots, n\}$ se tiene que $\sigma(j) = j$ o bien $\tau(j) = j$.

Ejemplos 4.2. Las permutaciones (134) y (25) son disjuntas. En cambio, las permutaciones (134) y (24) no lo son.

Si $\sigma \in \mathbb{S}_n$ y j es tal que $\sigma(j) = j$, entonces j es un punto fijo de σ. En cambio, los j tales que $\sigma(j) \neq j$ son los puntos movidos por σ.

Observación 4.3. Las permutaciones disjuntas conmutan.

Observación 4.4. Cada permutación puede escribirse como producto de trasposiciones. Para demostrar esta afirmación procederemos de la siguiente forma. Supongamos que las personas invitadas a un concierto se sientan en la primera fila, pero sin respetar el orden que figura en la lista de invitados. ¿Qué podemos hacer para ordenar a esas personas? Primero identificamos a la persona que debería sentarse en el primer lugar y le pedimos que intercambie asientos con la persona sentada en esa primera butaca. Luego identificamos a la persona que debería sentarse en el segundo lugar y le pedimos que intercambie asientos con la persona que ocupe la segunda butaca. Hacemos lo mismo con el tercer lugar, con el cuarto... y una vez terminado el proceso, gracias a haber utilizado finitas trasposiciones, habremos conseguido acomodar correctamente a cada una de las personas invitadas al concierto.

A continuación demostraremos que toda permutación puede escribirse como producto de ciclos disjuntos, algo que usamos en el primer capítulo en el caso particular del grupo $\mathbb{S}_3$. Necesitamos el siguiente lema:

Lema 4.5. *Sea $\sigma = \alpha\beta \in \mathbb{S}_n$ con α y β permutaciones disjuntas. Si $\alpha(i) \neq i$, entonces $\sigma^k(i) = \alpha^k(i)$ para todo $k \geq 0$.*

Demostración. Sin perder generalidad podemos suponer que $k > 0$. En ese caso, $\sigma^k(i) = (\alpha\beta)^k(i) = \alpha^k(\beta^k(i)) = \alpha^k(i)$. □

Ahora sí estamos en condiciones de demostrar el teorema:

Teorema 4.6. *Toda $\sigma \in \mathbb{S}_n \setminus \{\mathrm{id}\}$ puede escribirse como producto de ciclos disjuntos de longitud ≥ 2. Además esta descomposición es única salvo el orden de los factores involucrados.*

Demostración. Procederemos por inducción en el número k de elementos del conjunto $\{1,\ldots,n\}$ movidos por σ. Si $k = 2$ el resultado es trivial. Supongamos entonces que el resultado es cierto para todas las permutaciones que mueven $< k$ puntos. Sea $i_1 \in \{1,\ldots,n\}$ tal que $\sigma(i_1) \neq i_1$. Vamos a considerar el ciclo que contiene al elemento i_1. Sea entonces $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$... Sabemos que existe $r \in \mathbb{N}$ tal que $\sigma(i_r) = i_1$ (pues, de lo contrario, si $\sigma(i_r) = i_j$ para algún $j \in \{2,\ldots,n\}$, entonces $\sigma(i_{j-1}) = i_j = \sigma(i_r)$, una contradicción a la biyectividad de σ). Sea $\sigma_1 = (i_1 \cdots i_r)$. La hipótesis inductiva nos dice que, como $\sigma_1^{-1}\sigma$ mueve $< k$ puntos (pues los i_j son puntos fijos de $\sigma_1^{-1}\sigma$), podemos escribir $\sigma_1^{-1}\sigma = \sigma_2 \cdots \sigma_s$, donde $\sigma_2,\ldots,\sigma_s$ son ciclos disjuntos. Esto implica que $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$, tal como queríamos.

Demostremos ahora la unicidad. Supongamos que $\sigma = \sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_t$, con $s > 0$. Sea $i_1 \in \{1,\ldots,n\}$ tal que $\sigma(i_1) \neq i_1$. El lema implica que $\sigma^k(i_1) = \sigma_1^k(i_1)$ para todo $k \geq 0$. Existe entonces $j \in \{1,\ldots,t\}$ tal que $\tau_j(i_1) \neq i_1$. Como los t_k conmutan, sin perder generalidad podemos suponer que $j = 1$. Luego $\sigma^k(i_1) = \tau_1^k(i_1)$ para todo $k \geq 0$. Esto implica que $\sigma_1 = \tau_1$ pues σ_1 y τ_1 son ciclos y entonces $\sigma_2 \cdots \sigma_s = \tau_2 \cdots \tau_t$. Al repetir el argumento, vemos que $s = t$ y luego $\sigma_j = \tau_j$ para todo j. □

Corolario 4.7.

1) $\mathbb{S}_n = \langle (ij) : i < j \rangle$.
2) $\mathbb{S}_n = \langle (12), (13), \ldots, (1n) \rangle$.
3) $\mathbb{S}_n = \langle (12), (23), \ldots, (n-1\,n) \rangle$.
4) $\mathbb{S}_n = \langle (12), (12\cdots n) \rangle$.

Demostración. Ya demostramos que toda permutación puede escribirse como producto de trasposiciones. Otra demostración puede obtenerse al usar el teorema anterior ya que

$$(a_1 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2).$$

En efecto, si escribimos a $\sigma \in \mathbb{S}_n$ como producto de ciclos disjuntos y usamos la fórmula anterior, tenemos que $\mathbb{S}_n \subseteq \langle (ij) : i < j \rangle$. La otra inclusión es trivial. ‘

Para demostrar la segunda afirmación hay que usar la primera afirmación y las fórmulas

$$(1i)(1j)(1i) = (ij)$$

válidas siempre que $i \neq j$.

Para la tercera afirmación escribimos a σ como producto de trasposiciones y luego observamos que

$$(13) = (12)(23)(12), \quad (1k+1) = (kk+1)(1k)(kk+1)$$

para todo $k \geq 3$.

Por último, la cuarta afirmación se obtiene al utilizar la tercera propiedad junto con la fórmula

$$(12\cdots n)^{k-1}(12)(12\cdots n)^{1-k} = (kk+1),$$

válida para todo $k \geq 1$. □

Cada permutación tiene asociada una matriz de permutación. Por ejemplo, para $\sigma = \mathrm{id} \in \mathbb{S}_3$ se tiene a P_σ como la matriz identidad de 3×3. Para la permutación $\sigma = (123)$ se tiene

$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Si e_1, e_2, e_3 es la base canónica de $\mathbb{R}^{3\times 1}$, entonces $P_\sigma(e_1) = e_2$, $P_\sigma(e_2) = e_1$ y $P_\sigma(e_3) = e_1$. En general, la matriz de permutación P_σ correspondiente a $\sigma \in \mathbb{S}_n$, permuta los elementos de la base canónica de $\mathbb{R}^{n\times 1}$ tal como σ permuta los elementos del conjunto $\{1, 2, \ldots, n\}$.

En general, si $\sigma \in \mathbb{S}_n$, entonces

$$P_\sigma = \sum_{i=1}^{n} E_{\sigma(i),i},$$

donde $E_{i,j}$ es la matriz con un uno en la posición (i, j) e igual a cero en todas las otras entradas. Recordemos que valen las siguientes fórmulas

$$E_{i,j}E_{k,l} = \begin{cases} E_{i,l} & \text{si } j = k, \\ 0 & \text{si } j \neq k. \end{cases} \tag{4.1}$$

Es claro que toda matriz de permutación tendrá un único uno en cada fila y cada columna y que el resto de las entradas serán todas iguales a cero. Luego el determinante de una matriz de permutación será ± 1.

Proposición 4.8. *Si $\sigma, \tau \in \mathbb{S}_n$, entonces $P_{\sigma\tau} = P_\sigma P_\tau$.*

Demostración. Es un cálculo directa que utiliza la fórmula (4.1). Tenemos

$$P_\sigma P_\tau = \left(\sum_{i=1}^n E_{\sigma(i),i}\right)\left(\sum_{j=1}^n E_{\tau(j),j}\right)$$
$$= \sum_{i=1}^n \sum_{j=1}^n E_{\sigma(i),i}E_{\tau(j),j} = \sum_{j=1}^n E_{\sigma(\tau(j)),j} = P_{\sigma\tau},$$

ya que la suma doble será nula a menos que $i = \tau(j)$. □

Definición 4.9. El **signo** de una permutación $\sigma \in \mathbb{S}_n$ se define como el determinante de la matriz P_σ, es decir $\text{signo}(\sigma) = \det P_\sigma$. Una permutación σ se dirá **par** si $\text{signo}(\sigma) = 1$ e **impar** si $\text{signo}(\sigma) = -1$.

Ejemplos 4.10. La identidad es una permutación par y todo 3-ciclo es también una permutación par. Cualquier trasposición es una permutación impar.

Toda permutación puede escribirse como producto de trasposiciones, aunque no de forma única. Sin embargo, puede demostrarse el siguiente resultado. Si σ se escribe como producto de traposiciones $\sigma = \sigma_1 \cdots \sigma_s$, entonces

$$\text{signo}(\sigma) = (-1)^s.$$

En particular, σ es una permutación par si y sólo si s es par.

Proposición 4.11. *Si $\sigma, \tau \in \mathbb{S}_n$, entonces* $\text{signo}(\sigma\tau) = (\text{signo}\,\sigma)(\text{signo}\,\tau)$.

Demostración. Es fácil pues

$$\text{signo}(\sigma\tau) = \det(P_\sigma P_\tau) = (\det P_\sigma)(\det P_\tau) = \text{signo}(\sigma)\,\text{signo}(\tau).$$ □

Ejemplo 4.12. Vamos a demostrar que si $n \geq 3$ entonces $Z(\mathbb{S}_n) = \{\text{id}\}$. Supongamos que $Z(\mathbb{S}_n) \neq \{\text{id}\}$ y sea $\sigma \in Z(\mathbb{S}_n)$ tal que $\sigma(i) = j$ para $i \neq j$. Como $n \geq 3$, existe $k \in \{1, \ldots, n\} \setminus \{i, j\}$ y entonces $\tau = (jk) \in \mathbb{S}_n$. Como σ es central,

$$j = \sigma(i) = \tau\sigma\tau^{-1}(i) = \tau(\sigma(i)) = \tau(j) = k,$$

una contradicción.

El **grupo alternado**

$$\mathbb{A}_n = \{\sigma \in \mathbb{S}_n : \text{signo}(\sigma) = 1\}$$

es el subgrupo de $\mathbb{S}_n$ formado por las permutaciones de signo positivo.

Proposición 4.13. $|\mathbb{A}_n| = n!/2$.

Demostración. Sea $\sigma = (12) \notin \mathbb{A}_n$. Vamos a demostrar que $\mathbb{S}_n = \mathbb{A}_n \cup \mathbb{A}_n\sigma$ (unión disjunta), donde $\mathbb{A}_n\sigma = \{\tau\sigma : \tau \in \mathbb{A}_n\}$. En efecto, si $\tau \in \mathbb{S}_n$ es tal que $\tau \notin \mathbb{A}_n$, entonces $\text{signo}(\tau\sigma) = (\text{signo}\,\tau)(\text{signo}\,\sigma) = 1$ y luego $\tau\sigma \in \mathbb{A}_n$. En conclusión, probamos que $\tau \in \mathbb{A}_n\sigma$. Como $|\mathbb{A}_n\sigma| = |\mathbb{A}_n|$ (por ejemplo, pues la función $\mathbb{A}_n \to \mathbb{A}_n\sigma, x \mapsto x\sigma$, es biyectiva), se obtiene $n! = |\mathbb{S}_n| = 2|\mathbb{A}_n|$. □

Ejemplo 4.14. Es fácil verificar que $\mathbb{A}_3 = \{\mathrm{id}, (123), (132)\}$ y que

$$\mathbb{A}_4 = \{\mathrm{id}, (234), (243), (12)(34), (123), (124), \\ (132), (134), (13)(24), (142), (143), (14)(23)\}$$

El grupo $\mathbb{A}_3$ es abeliano. Si $n \geq 4$, el grupo $\mathbb{A}_n$ es no abeliano ya que, por ejemplo, las permutaciones (123) y (124) no conmutan.

Proposición 4.15. $\mathbb{A}_n = \langle \{3\text{-}ciclos\} \rangle$.

Demostración. Todo 3-ciclo es una permutación par pues $(ijk) = (ik)(ij)$. Demostremos entonces la otra inclusión. Sea $\sigma \in \mathbb{A}_n$. Escribimos $\sigma = \sigma_1 \cdots \sigma_s$ para algún entero s par y $\sigma_1, \ldots, \sigma_s$ trasposiciones. Para completar la demostración de la proposición basta utilizar las fórmulas

$$(kl)(ij) = (kl)(ki)(ki)(ij) = (kil)(ijk), \quad (ik)(ij) = (ijk). \qquad \square$$

Veamos algunas aplicaciones sencillas:

Ejemplo 4.16. Veamos que si $n \geq 5$ entonces $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$. Vamos a demostrar la inclusión no trivial y para eso basta con observar que $\mathbb{A}_n$ está generado por 3-ciclos y que, como $n \geq 5$, cada 3-ciclo puede escribirse como producto de conmutadores. En efecto,

$$(abc) = [(acd), (ade)][(ade), (abd)],$$

donde $\#\{a,b,c,d,e\} = 5$.

Ejemplo 4.17. Si $n \geq 3$ entonces $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. Primero veamos que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathbb{A}_n$. Si $\sigma \in [\mathbb{S}_n, \mathbb{S}_n]$, digamos $\sigma = [\sigma_1, \tau_1][\sigma_2, \tau_2] \cdots [\sigma_k, \tau_k]$, entonces

$$\mathrm{signo}(\sigma) = \mathrm{signo}([\sigma_1, \tau_1]) \cdots \mathrm{signo}([\sigma_k, \tau_k]) = 1.$$

Recíprocamente, si $\sigma \in \mathbb{A}_n$, la proposición anterior nos dice que podemos escribir a σ como producto de 3-ciclos. De aquí el resultado se obtiene inmediatamente pues cada 3-ciclo es un conmutador, tal como vemos en la siguiente fórmula

$$(abc) = (ab)(ac)(ab)(ac) = [(ab), (ac)] \in [\mathbb{S}_n, \mathbb{S}_n].$$

Capítulo 5
Cocientes

Si G es un grupo y N es un subgrupo de G, nos interesa saber cuándo el conjunto G/N de coclases es un grupo con la operación $G/N \times G/N \to G/N$, $(xN, yN) \mapsto xyN$, es decir, cuándo esta operación está bien definida. ¿Qué significa eso? Queremos que esa operación sea una función. Para eso, se necesita que si $xN = x_1N$ y además $yN = y_1N$, entonces $xyN = x_1y_1N$. Veamos cómo puede interpretarse esa condición. Si $x^{-1}x_1 \in N$ y $y^{-1}y_1 \in N$, entonces $x_1 = xn$ y además $y_1 = ym$ para ciertos $m, n \in N$. Entonces

$$(xy)^{-1}(x_1y_1) = y^{-1}x^{-1}x_1y_1 = y^{-1}nym \in N$$

si y sólo si $y^{-1}ny \in N$.

Ejemplo 5.1. Si $G = \mathbb{S}_3$ y $H = \langle(12)\rangle$, entonces $(xN, yN) \mapsto xyN$ no es una función. Para verlo, primero recordemos que $G/H = \{H, (123)H, (132)H\}$, donde $H = (12)H$, $(123)H = (13)H$ y $(132)H = (23)H$. Tenemos

$$(132)N = (13)(23)N = (13)N(23)N = (123)N(132)N = N,$$

una contradiccion.

Definición 5.2. Sea G un grupo. Un subgrupo N de G se dice **normal** si $gNg^{-1} \subseteq N$ para todo $g \in G$. Notación: si N es normal en G, entonces $N \trianglelefteq G$.

Si G es un grupo abeliano, todo subgrupo de G es normal en G.

Proposición 5.3. *Sea N un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

1) $gNg^{-1} \subseteq N$ para todo $g \in G$.
2) $gNg^{-1} = N$ para todo $g \in G$.
3) $gN = Ng$ para todo $g \in G$.

Demostración. Demostremos que $(1) \implies (2)$, que es la única implicación no trivial. Si $n \in N$ y $g \in G$, entonces $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$. □

Proposición 5.4. *Sea N un subgrupo de G. Las siguientes propiedades son equivalentes:*

1) N es normal en G.
2) $(gN)(hN) = (gh)N$ para todo $g,h \in G$.

Demostración. Vamos a demostrar que $(1) \implies (2)$. Sea $g \in G$. Como $gNg^{-1} = N$, entonces $(gN)(hN) = g(Nh)N = g(hN)N = (gh)N$. Veamos ahora que $(2) \implies (1)$. Si $g \in G$, entonces $gNg^{-1} \subseteq (gN)(g^{-1}N) = (gg^{-1})N = N$. □

Ejemplos 5.5. Si G es un grupo, entonces $\{1\}$ y G son subgrupos normales de G.

Ejemplo 5.6. Si G es un grupo, $Z(G)$ es un subgrupo normal de G. Más aún, si $N \leq Z(G)$, entonces $N \trianglelefteq G$.

Ejemplo 5.7. Si G es un grupo, entonces $[G,G]$ es un subgrupo normal de G pues si $x \in [G,G]$ y $g \in G$, entonces $gxg^{-1} = (gxg^{-1}x^{-1})x = [g,x]x \in [G,G]$. Alternativamente,

$$g\left(\prod_{i=1}^{k}[x_i,y_i]\right)g^{-1} = \prod_{i=1}^{k}[gx_ig^{-1}, gy_ig^{-1}]$$

para todo $g,x_1,\ldots,x_k,y_1,\ldots,y_k \in G$.

Ejemplo 5.8. Para todo $n \in \mathbb{N}$, $\mathbb{A}_n$ es un subgrupo normal de $\mathbb{S}_n$. De hecho, si $\sigma \in \mathbb{A}_n$ y $\tau \in \mathbb{S}_n$, entonces $\tau\sigma\tau^{-1} \in \mathbb{A}_n$ pues

$$\operatorname{signo}(\tau\sigma\tau^{-1}) = \operatorname{signo}(\sigma) = 1.$$

Ejemplo 5.9. Si N es un subgrupo de G tal que $(G:N) = 2$, entonces N es normal en G. Queremos demostrar que $gN = Ng$ para todo $g \in G$. Sea $g \in G$. Si $g \in N$, entonces $gN = Ng$. Si $g \notin N$, entonces $gN \neq N$. Como $(G:N) = 2$, podemos escribir a G como $G = N \cup gN$ (unión disjunta). En consecuencia, $gN = G \setminus N$. Similarmente se demuestra que $Ng = G \setminus N$ y luego $gN = Ng$.

Ejemplo 5.10. El ejemplo anterior nos permite demostrar que $\langle(123)\rangle \trianglelefteq \mathbb{S}_3$. Por otro lado, $\langle(12)\rangle$ no es normal en $\mathbb{S}_3$ pues por ejemplo $(13)(12)(13) = (23) \notin \langle(12)\rangle$.

Ejemplo 5.11. $\mathbf{SL}_n(\mathbb{R})$ es normal en $\mathbf{GL}_n(\mathbb{R})$ pues si $g \in \mathbf{GL}_n(\mathbb{R})$ y $x \in \mathbf{SL}_n(\mathbb{R})$, entonces $\det(gxg^{-1}) = (\det g)(\det x)(\det g)^{-1} = 1$.

Ejemplo 5.12. El grupo de Klein $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en $\mathbb{S}_4$. Para verificar la afirmación tenemos que ver que $\sigma K\sigma^{-1} \subseteq K$ para todo $\sigma \in \mathbb{S}_4$. En principio, tendríamos que chequear la contención para cada uno de los elementos de $\mathbb{S}_4$. Por suerte, hay algo mejor para hacer. Recordemos que, por ejemplo, $\mathbb{S}_4$ está generado por (12) y (1234). Como entonces todo elemento de $\mathbb{S}_4$ es una palabra en (12) y (1234), si vemos que $\sigma K\sigma^{-1} \subseteq K$ para todo $\sigma \in \{(12),(1234)\}$, habremos probado que K es normal en $\mathbb{S}_4$. Dejamos como ejercicio verificar que

$$(12)K(12)^{-1} \subseteq K, \quad (1234)K(1234)^{-1} \subseteq K.$$

En el ejercicio siguiente nos encontramos con un caso particular del producto semidirecto de dos grupos, una construcción general que resulta de mucha utilidad.

Ejercicio 5.13. Sea $G = \mathbb{R} \times \mathbb{R}^\times$ el grupo dado por la operación

$$(x,y)(u,v) = (x+yu, yv).$$

Demuestre que $\{(x,1) : x \in \mathbb{R}\}$ es normal en G y que $\{(0,y) : y \in (\mathbb{R})^\times\}$ no es normal en G.

En el ejemplo anterior el cuerpo $\mathbb{R}$ puede reemplazarse por cualquier otro cuerpo, por ejemplo el cuerpo finito $\mathbb{Z}/p$ para cualquier número primo p.

Veamos algunos ejemplos de subgrupos normales un poco más difíciles. Primero calcularemos los subgrupos normales de $\mathbb{A}_4$.

Ejemplo 5.14. Vamos a demostrar que $\{\mathrm{id}\}$, $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ y $\mathbb{A}_4$ son los únicos subgrupos normales de $\mathbb{A}_4$.

Como $\mathbb{A}_4 = \{3\text{-ciclos}\} \cup K$, K es el único subgrupo de $\mathbb{A}_4$ con cuatro elementos, y esto implica que K es normal en $\mathbb{A}_4$ (pues cada conjugado gKg^{-1} también será un subgrupo de $\mathbb{A}_4$ de cuatro elementos). Sea $N \neq \{\mathrm{id}\}$ un subgrupo normal de $\mathbb{A}_4$. Si N contiene un 3-ciclo, digamos $(abc) \in N$. entonces

$$(acd) = (bcd)(abc)(bcd)^{-1} \in N$$

y luego $N = \mathbb{A}_4$ (pues todos los 3-ciclos están en N). Supongamos entonces que N no contiene 3-ciclos. Entonces algún elemento no trivial de K pertenece a N, digamos $(ab)(cd) \in N$. En consecuencia,

$$(ac)(bd) = (bcd)(ab)(cd)(bcd)^{-1} \in N, \quad (ad)(bc) = (ab)(cd)(ac)(bd) \in N$$

y luego $N = K$.

Es importante remarcar que la normalidad no es transitiva.

Ejercicio 5.15. Sea $G = \mathbb{D}_4$ el grupo diedral de tamaño ocho y sean $N = \langle s, r^2 \rangle$ y $H = \langle s \rangle$. Demuestre que H es normal en N, N es normal en G pero H no es normal en G.

Vamos a calcular ahora los subgrupos normales de $\mathbb{S}_4$.

Ejemplo 5.16. Vamos a demostrar que $\{\mathrm{id}\}$, K, $\mathbb{A}_4$ y $\mathbb{S}_4$ son los únicos subgrupos normales de $\mathbb{S}_4$.

Sea N un subgrupo normal de $\mathbb{S}_4$. Si $N \subseteq \mathbb{A}_4$, entonces N es normal en $\mathbb{A}_4$ y luego, por lo visto en el ejemplo anterior, $N = \{\mathrm{id}\}$, $N = K$ o bien $N = \mathbb{A}_4$. Supongamos entonces que $N \not\subseteq \mathbb{A}_4$, es decir N contiene una permutación impar. Si $\sigma \in \mathbb{S}_4$ es una permutación impar, entonces σ es una trasposición o σ es un 4-ciclo.

Si N contiene una trasposición, entonces todas las trasposiciones también pertenecen a N pues

$$\tau(ij)\tau^{-1} = (\tau(i)\,\tau(j))$$

para todo $\tau \in \mathbb{S}_4$. En este caso, $N = \mathbb{S}_4$ pues $\mathbb{S}_4$ está generado por trasposiciones.

Si N contiene un 4-ciclo, todos los 4-ciclos también están en N pues

$$\tau(ijkl)\tau^{-1} = (\tau(i)\,\tau(j)\,\tau(k)\,\tau(l))$$

para todo $\tau \in \mathbb{S}_4$ y además $K \subseteq N$ pues

$$(ac)(bd) = (abcd)^2.$$

Esto nos dice que $|N| \geq 10$. Como además $K \subseteq N$, se tiene que $|N \cap \mathbb{A}_4| \geq 5$. Por otro lado, $N \cap \mathbb{A}_4$ es un subgrupo normal de $\mathbb{A}_4$. Por lo visto en el ejemplo anterior, $N \cap \mathbb{A}_4 = \mathbb{A}_4 \subseteq N$. En conclusión, $N = \mathbb{S}_4$.

Teorema 5.17. *Si N es un subgrupo normal de G, entonces G/N es un grupo con la operación $(xN)(yN) = (xy)N$.*

Demostración. Sabemos que la normalidad de N en G garantiza la buena definición de la operación. Calculos rutinarios, que dejamos como ejercicio, demuestran que esta operación transforma al conjunto G/N en un grupo. □

No estamos en condiciones de poder entender qué tipo de grupo obtenemos como grupo cociente, ya que para eso es necesario poder entender qué significa que dos grupos sean "iguales" aunque parezcan distintos.

Ejemplo 5.18. Sabemos que $\{\mathrm{id}\}$, K, $\mathbb{A}_4$ y $\mathbb{S}_4$ son los únicos subgrupos normales de $\mathbb{S}_4$. Trivialmente obtenemos que

$$\mathbb{S}_4/\{\mathrm{id}\} \simeq \mathbb{S}_4, \quad \mathbb{S}_4/\mathbb{A}_4 \simeq \mathbb{Z}/2, \quad \mathbb{S}_4/\mathbb{S}_4 \simeq \{\mathrm{id}\}.$$

Veamos qué podemos decir del cociente $Q = \mathbb{S}_4/K$. Sabemos que Q tiene orden seis y que Q es no abeliano pues

$$(12)K(13)K = (12)(13)K = (132)K \neq (123)K = (13)(12)K = (13)K(12)K.$$

Vimos que existe un único grupo no abeliano de orden seis. Luego $Q \simeq \mathbb{S}_3$.

Proposición 5.19. *Si H es un subgrupo normal de G, entonces G/H es abeliano si y sólo si $[G,G] \subseteq H$.*

Demostración. Sean $x, y \in G$. Entonces

$$(xH)(yH) = (yH)(xH) \iff (xy)H = (yx)H \iff x^{-1}y^{-1}xy \in H.$$

Luego G/H es conmutativo si y sólo si $[x,y] = xyx^{-1}y^{-1} \in H$ para todo $x, y \in G$. □

Veamos una pequeña aplicación:

Ejemplo 5.20. $[\mathbb{A}_4, \mathbb{A}_4] = K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Sabemos que K es normal en $\mathbb{A}_4$. Como $\mathbb{A}_4/K$ tiene tres elementos, es abeliano. El ejercicio anterior, entonces, nos dice que $[\mathbb{A}_4, \mathbb{A}_4] \subseteq K$. Por otro lado, como

$$(ab)(cd) = [(abc), (cda)],$$

se concluye que $K \subseteq [\mathbb{A}_4, \mathbb{A}_4]$.

Otra propiedad importante:

Proposición 5.21. *Si $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Supongamos que $G/Z(G) = \langle gZ(G)\rangle$. Sean $x, y \in G$. Escribamos $xZ(G) = g^k Z(G)$ y también $yZ(G) = g^l Z(G)$, es decir $x = g^k z_1$, $y = g^l z_2$ para ciertos $k, l \in \mathbb{Z}$ y $z_1, z_2 \in Z(G)$. Luego $xy = yx$. □

Teorema 5.22. *Sea p un número primo y sea H un subgrupo de G. Si $(G : H) = p$, las siguientes afirmaciones son equivalentes:*

1) H es normal en G.
2) Si $g \in G \setminus H$, entonces $g^p \in H$.
3) Si $g \in G \setminus H$, entonces $g^n \in H$ para algún $n \in \mathbb{N}$ sin divisores primos $< p$.
4) Si $g \in G \setminus H$, entonces $g^k \notin H$ para todo $k \in \{2, \ldots, p-1\}$.

Demostración. La implicación $(1) \implies (2)$ es consecuencia inmediata del teorema de Lagrange, pues $|G/H| = p$.

La implicación $(2) \implies (3)$ es trivial pues p es un número primo.

Demostremos que $(3) \implies (4)$. Si $g^k \in H$ para algún $k \in \{2, \ldots, p-1\}$, como $\mathrm{mcd}(k, n) = 1$, existen $r, s \in \mathbb{Z}$ tales que $rk + sn = 1$. Luego

$$g = g^1 = g^{rk+sn} = (g^k)^r (g^n)^s \in H,$$

una contradicción.

Para finalizar demostremos que $(4) \implies (1)$. Sea $x \in G \setminus H$ y sea $h \in H$. Queremos demostrar que entonces $xhx^{-1} \in H$. Si $y = xhx^{-1} \notin H$, entonces $y^k \notin H$ para todo $k \in \{2, \ldots, p-1\}$. Esto implica que las coclases

$$H, yH, y^2H, \ldots, y^{p-1}H$$

son todas distintas (pues si $y^i H = y^j H$ para i, j tales que $i < j$, entonces $y^{j-i} \in H$ con $j - i \leq p - 2$). Como $y = xhx^{-1}$, entonces

$$(yx)H = (xh)H = xH = y^i H$$

para algún $i \in \{0, 1, \ldots, p-1\}$. Si $i = 0$, entonces $yx = xh \in H$ y luego $x \in H$, una contradicción. Luego $(yx)H = y^i H$ para algún $i \in \{1, \ldots, p-1\}$ y entonces

$$y^i H = xH = y^{i-1} H$$

para algún $i \in \{0, \ldots, p-2\}$, una contradicción. □

Veamos algunas consecuencias. La primera se hará en el caso en que el grupo sea finito.

Corolario 5.23. *Sea p el menor número primo que divide al orden de un grupo finito G y sea H es un subgrupo de G índice p. Entonces H es normal en G.*

Demostración. Si $g \in G \setminus H$, entonces $g^n = 1 \in H$, donde $n = |G|$. Como p es primo, n no tiene divisores primos $< p$. El teorema anterior impica entonces que H es normal en G. □

En el teorema no pedimos que G sea un grupo finito. Podemos entonces obtener el siguiente resultado.

Corolario 5.24. *Sea p un número primo y sea G un grupo tal que todo elemento tiene orden una potencia de p. Si H es un subgrupo de G de índice p, entonces H es normal en G.*

Demostración. Sea $g \in G \setminus H$ y sea $n = |g|$. Como todo elemento de G tiene orden una potencia de p, n es en particular una potencia de p y, en consecuencia, n no posee divisores primos $< p$. Como además $g^n = 1 \in H$, el teorema anterior implica que H es normal en G. en particular $g^n \in H$. □

El siguiente ejercicio es útil.

Ejercicio 5.25. Si S es un subgrupo de G, se define el **normalizador** de S en G al subgrupo

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

Demuestre que valen las siguientes afirmaciones:

1) $S \trianglelefteq N_G(S)$.
2) Si $S \leq T \leq G$ y $S \trianglelefteq T$, entonces $T \leq N_G(S)$.

El ejercicio anterior nos dice que el normalizador de un subgrupo S en G es el mayor subgrupo de G que contiene a S como subgrupo normal.

Terminamos el capítulo con una definición importante.

Definición 5.26. Diremos que un grupo G es **simple** si $G \neq \{1\}$ y sus únicos subgrupos normales son G y $\{1\}$.

Por ahora, nos quedaremos conformes al observar que si p es un número primo, entonces $\mathbb{Z}/p$ es un grupo simple. Veremos otros ejemplos más adelante.

Capítulo 6
Subgrupos permutables

Si H y K son subgrupos de un grupo G, definimos

$$HK = \{hk : h \in H, k \in K\}.$$

Observemos que

$$H \cup K \subseteq HK \subseteq \langle H \cup K \rangle.$$

Nos interesa saber cuándo XY es un subgrupo de G. Observemos que $HK \leq G$ si y sólo si $\langle H \cup K \rangle = HK$.

Proposición 6.1. *Sean H y K subgrupos de un grupo G. Entonces HK es un subgrupo de G si y sólo si $HK = KH$.*

Demostración. Supongamos que $HK = KH$. Como $1 \in H \cap K$, el conjunto HK es no vacío. Si $h \in H$ y $k \in K$, entonces $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Además $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ y luego HK es cerrado para la multiplicación.

Supongamos ahora que HK es un subgrupo de G. Como $H \subseteq HK$, $K \subseteq HK$ y además HK es cerrado para la multiplicación, $KH \subseteq (HK)(HK) \subseteq HK$. Recíprocamente, sea $g \in HK$. Como $g^{-1} \in HK$, existen $h \in H$ y $k \in K$ tales que $g^{-1} = hk$. Luego $HK \subseteq KH$ pues $g = k^{-1}h^{-1} \in KH$. □

Proposición 6.2. *Sean H y K subgrupos de G. Si H es normal en G, entonces HK es un subgrupo de G.*

Demostración. Nos alcanza con demostrar que $HK = KH$. Veamos primero que $HK \subseteq KH$. Si $x = hk \in HK$, entonces $x = k(k^{-1}hk) \in KH$ pues $k^{-1}hk \in H$. Para demostrar la otra inclusión, sea $y = kh \in KH$. Entonces $y = (khk^{-1})k \in HK$ pues $khk^{-1} \in H$. □

Ejemplo 6.3. Sea $G = \mathbb{S}_4$. Los subgrupos $H = \langle (12) \rangle$ y $K = \langle (34) \rangle$ cumplen que $HK = KH = \{\mathrm{id}, (12), (34), (12)(34)\}$ es un subgrupo de $\mathbb{S}_4$. Es interesante observar que aquí ni H ni K son normales en G.

Ejercicio 6.4. Demuestre que si H y K son subgrupos normales de G, entonces HK es también normal en G.

Ejercicio 6.5. Sean G un grupo y S un subgrupo de G. Si $T \leq N_G(S)$, entonces TS es un grupo y además $S \leq TS$.

Dos subgrupos H y K de un grupo G se dirán **permutables** si $HK = KH$. El siguiente resultado será de mucha utilidad más adelante.

Teorema 6.6. *Sean H y K subgrupos finitos de un grupo G. Entonces*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demostración. Sea $L = H \cap K$. Descomponemos al grupo H como unión disjunta de coclases de L, digamos $H = \cup_{i=1}^{k} x_i L$, donde $k = (H : L)$. Observemos que $LK = K$, pues $L \subseteq K$ y además $K \subseteq 1K \subseteq LK$. Entonces

$$HK = \bigcup_{i=1}^{k} x_i LK = \bigcup_{i=1}^{k} x_i K,$$

En particular, como la unión es disjunta,

$$|HK| = \sum_{i=1}^{k} |x_i K| = k|K| = \frac{|H||K|}{|H \cap K|}. \qquad \square$$

Es importante remarcar que en el teorema anterior no es necesario pedir que HK sea un subgrupo de G. Como una primera aplicación, daremos otra demostración del resultado que vimos en el corolario 5.23 en la página 32.

> Sea p el menor número primo que divide al orden de un grupo finito G y sea H un subgrupo de G índice p. Entonces H es normal en G.

Si $\{gHg^{-1} : g \in G\} = \{H\}$, entonces H es normal en G. Supongamos que existe $g \in G$ tal que $H \neq g^{-1}Hg = K$. Como $(H : H \cap K)$ divide al orden de H y todos los divisores primos de $|G|$ son $\geq p$, sabemos que $(H : H \cap K) \geq p$. Luego

$$|HK| = \frac{|H||K|}{|H \cap K|} \geq p|K| = |G|$$

pues $(G : H) = p$ y $|K| = |H|$. En particular, $HK = G$. Como $K = g^{-1}Hg$, se tiene que $g = h(g^{-1}h_1 g)$ para ciertos $h, h_1 \in H$. Luego

$$1 = hg^{-1}h_1 \implies h_1 h = g \in H \implies H = K,$$

una contradicción.

Ejemplo 6.7. Sean $G = \mathbb{S}_3$, $H = \langle (12) \rangle$ y $K = \langle (23) \rangle$. En este caso,

$$HK = \{\mathrm{id}, (12), (23), (123)\}$$

no es un subgrupo de G ya que el teorema de Lagrange implica que G no tiene subgrupos de orden cuatro. Otra forma de ver que HK no es un subgrupo es observar que $KH = \{\mathrm{id}, (12), (23), (132)\} \neq HK$.

Ejemplo 6.8. Sean $G = \mathbb{S}_3$, $H = \langle (12) \rangle$ y $K = \langle (123) \rangle$. Como K es normal en G, entonces HK es un subgrupo de G. El teorema de Lagrange nos dice que HK tiene orden seis y luego $G = HK$. Todo elemento $g \in G$ puede escribirse unívocamente como $g = hk$ para $h \in H$ y $k \in K$ (esto puede demostrarse considerando todos los posibles casos u observando que $H \cap K = \{\mathrm{id}\}$). Esto implica que la función

$$H \times K \to G, \quad (h,k) \mapsto hk,$$

es una biyección. Es importante remarcar que esta biyección no se lleva bien con la multiplicación de G (más adelante haremos más precisa esta observación y simplemente diremos que la función no es un morfismo de grupos), ya que en general $(h_1k_1)(h_2k_2) \neq (h_1h_2)(k_1k_2)$.

Capítulo 7
Morfismos

Definición 7.1. Sean G y H dos grupos. Una función $f\colon G \to H$ es un **morfismo de grupos** si $f(xy) = f(x)f(y)$ para todo $x, y \in G$.

Si un morfismo de grupos es una función inyectiva, se denominará **monomorfismo**. Si es una función sobreyectiva, se denominará **epimorfismo**. Si fuera una función biyectiva, **isomorfismo**. Dos grupos G y H se dirán **isomorfos** (la notación será $G \simeq H$) cuando exista un isomorfismo $G \to H$.

Ejemplos 7.2.

1) Si G es un grupo, la función $\mathrm{id}\colon G \to G$ es un morfismo de grupos.
2) Si G y H son grupos, la función $e\colon G \to H$, $e(g) = 1_H$, es un morfismo de grupos.
3) Para cada $n \in \mathbb{Z}$, la función $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto nx$, es un morfismo de grupos.
4) Si G es un grupo abeliano y $n \in \mathbb{Z}$, la función $G \to G$, $g \mapsto g^n$, es un morfismo de grupos.

El siguiente ejemplo es particularmente importante.

Ejemplo 7.3. Sea G un grupo y sea $g \in G$. La función $\gamma_g\colon G \to G$, $\gamma_g(x) = gxg^{-1}$, se denomina **conjugación** por el elemento g y es un morfismo de grupos.

Ejemplo 7.4. La función $\exp\colon \mathbb{R} \to \mathbb{R}^\times$, $\exp(x) = e^x$, es un morfismo de grupos.

Ejemplo 7.5. La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ es un morfismo inyectivo de grupos.

En general, si S es un subgrupo de un grupo G, entonces la **inclusión** $S \hookrightarrow G$ es un morfismo de grupos.

Ejemplo 7.6. $\det\colon \mathbf{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ es un morfismo de grupos.

Ejemplo 7.7. Sea $f\colon G \to H$ un morfismo de grupos y sea S un subgrupo de G. La **restricción** $f|_S\colon S \to H$ es también un morfismo de grupos.

Ejemplo 7.8. La función $f\colon \mathbb{R} \to \mathbb{C}^\times$, $f(x) = \cos x + i \sin x$, es un morfismo de grupos pues $f(x+y) = f(x)f(y)$ para todo $x, y \in \mathbb{R}$.

Ejercicio 7.9. Sea $f\colon G \to H$ un morfismo de grupos. Demuestre que $f(1) = 1$, que $f(g^{-1}) = f(g)^{-1}$ y que $f(g^n) = f(g)^n$ para todo $g \in G$ y $n \in \mathbb{N}$.

Ejemplo 7.10. Sea $f\colon \mathbb{R}_{>0} \to \mathbb{R}$, $f(x) = \log(x)$. La fórmula

$$\log(xy) = \log(x) + \log(y)$$

nos dice que f es un morfismo de grupos. Los resultados del ejercicio anterior se traducen en las siguientes propiedades de la función logaritmo:

$$\log(1) = 0, \quad \log\left(\frac{1}{x}\right) = -\log(x), \quad \log(x^n) = n\log(x).$$

Definición 7.11. Sea $f\colon G \to H$ un morfismo de grupos. El **núcleo** de f es el conjunto $\ker f = \{x \in G : f(x) = 1\}$.

La propiedad fundamental que tiene el núcleo de un morfismo f es la siguiente: $f(x) = f(y)$ si y sólo si $x = yk$ para algún $k \in \ker f$.

Ejemplo 7.12. Sea $f\colon \mathscr{U}(\mathbb{Z}/21) \to \mathscr{U}(\mathbb{Z}/21)$ el morfismo de grupos definido por $f(x) = x^3$. Entonces $\ker f = \{1, 4, 16\}$ y $f(\mathscr{U}(\mathbb{Z}/21)) = \{1, 8, 13, 20\}$.

Ejemplo 7.13. Sea

$$\mathrm{Aff}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^\times, b \in \mathbb{R} \right\} \leq \mathbf{GL}_2(\mathbb{R}).$$

La función

$$f\colon \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}^\times, \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$$

es un morfismo de grupos (de hecho, $f(x) = \det(x)$ para todo $x \in \mathrm{Aff}(\mathbb{R})$) tal que

$$\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}.$$

Dejamos como ejercicio verificar que la función $g\colon \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}$, $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto b$, no es un morfismo de grupos.

Ejemplo 7.14. Sea $f\colon \mathbb{R} \to \mathbb{C}^\times$, $f(x) = \cos x + i \sin x$. Entonces

$$\ker f = \{2\pi k : k \in \mathbb{Z}\} = 2\pi\mathbb{Z}.$$

Definición 7.15. La **imagen** de f es el conjunto $f(G) = \{f(x) : x \in G\}$.

Proposición 7.16. *Si $f\colon G \to H$ un morfismo de grupos. Valen las siguientes propiedades:*

1) $\ker f$ *es un subgrupo normal de* G.

2) $f(G)$ es un subgrupo de H.

Demostración. Demostraremos solamente la primera afirmación, la segunda quedará como ejercicio. Primero debemos demostrar que $\ker f$ es un subgrupo de G. Para eso, observamos que $1 \in \ker f$ y además que si $x, y \in \ker f$ entonces $xy^{-1} \in \ker f$ (pues como f es morfismo de grupos se tiene que $f(xy^{-1}) = f(x)f(y)^{-1} = 1$). Para verificar que $\ker f$ es normal en G, sean $x \in \ker f$ y $g \in G$. Entonces $gxg^{-1} \in \ker f$ pues $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = 1$. □

La imagen en general no es un subgrupo normal.

Ejemplo 7.17. La inclusión $\langle(12)\rangle \hookrightarrow \mathbb{S}_3$ es un morfismo de grupos cuya imagen no es un subgrupo normal de $\mathbb{S}_3$.

Ejemplo 7.18. Sabemos que $\mathscr{U}(\mathbb{Z}/21) = \{1,2,4,5,8,10,11,13,16,17,19,20\}$ es un grupo abeliano. La función $f\colon \mathscr{U}(\mathbb{Z}/21) \to \mathscr{U}(\mathbb{Z}/21)$, $f(x) = x^3$, es un morfismo de grupos. La imagen de f es igual a $\{1,8,13,20\}$, que es un subgrupo de $\mathscr{U}(\mathbb{Z}/21)$.

Ejemplo 7.19. La función signo$\colon \mathbb{S}_n \to \{-1,1\}$ es un morfismo sobreyectivo de grupos tal que $\ker(\text{signo}) = \mathbb{A}_n$. En particular, $\mathbb{A}_n$ es un subgrupo normal de $\mathbb{S}_n$.

Ejemplo 7.20. Si N es un subgrupo normal de G, la función $\pi\colon G \to G/N$, $x \mapsto xN$, es un morfismo sobreyectivo tal que $\ker \pi = N$. La función π se conoce como el **morfismo canónico** $G \to G/N$.

El ejemplo anterior nos dice, en particular, que cada subgrupo normal de un grupo G es el núcleo de un morfismo con dominio en G.

Ejercicio 7.21. Sea $f\colon G \to H$ un morfismo de grupos. Demuestre las siguientes afirmaciones:

1) Si $S \leq G$, entonces $f(S) \leq H$ y además $f^{-1}(f(S)) = S\ker f$.
2) Si $T \leq H$, entonces $\ker f \leq f^{-1}(T) \leq G$ y además $f(f^{-1}(T)) = T \cap f(G)$.
3) f es inyectiva si y sólo si $\ker f = \{1\}$.
4) Si $g \in G$ tiene orden finito, entonces $|f(g)|$ divide a $|g|$.

Si $f\colon G \to H$ es un isomorfismo de grupos, entonces $f^{-1}\colon H \to G$ es también un isomorfismo. Observemos además que un morfismo de grupos $f\colon G \to H$ será un isomorfismo si y sólo si existe un morfismo de grupos $g\colon H \to G$ tal que $g \circ f = \mathrm{id}_G$ y $f \circ g = \mathrm{id}_H$.

Ejemplo 7.22. $\mathbb{S}_2 \simeq \mathbb{Z}/2 \simeq G_2$.

Ejemplo 7.23. $\mathbb{D}_3 \simeq \mathbb{S}_3$ y el isomorfismo está dado por la función $\mathbb{D}_3 \to \mathbb{S}_3$,

$$1 \mapsto \mathrm{id}, \quad r \mapsto (123), \quad r^2 \mapsto (132), \quad s \mapsto (12), \quad rs \mapsto (13), \quad r^2 s \mapsto (23).$$

Ejemplo 7.24. $\mathbb{Z}/2 \times \mathbb{Z}/3 \simeq \mathbb{Z}/6$ y el isomorfismo está dado por

$$(0,0) \mapsto 0, \quad (1,0) \mapsto 3, \quad (0,1) \mapsto 4, \quad (1,1) \mapsto 1, \quad (0,2) \mapsto 2, \quad (1,2) \mapsto 5.$$

Ejemplo 7.25. La función $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ es un morfismo de grupos. Como log es biyectiva, $\mathbb{R}_{>0} \simeq \mathbb{R}$.

Es fácil demostrar que si $f\colon G \to H$ es un isomorfismo entonces $|g| = |f(g)|$ para todo $g \in G$.

Ejemplo 7.26. $\mathbb{Z}/2 \times \mathbb{Z}/2 \not\simeq \mathbb{Z}/4$ pues en $\mathbb{Z}/2 \times \mathbb{Z}/2$ no hay elementos de orden cuatro.

Ejemplo 7.27. $\mathbb{Q}/\mathbb{Z} \not\simeq \mathbb{Q}$. Ambos son grupos abelianos, pero no son isomorfos. Para verlo, primero observamos que en $\mathbb{Q}$ todo elemento no trivial tiene orden infinito (pues si $kx = 0$ con $k \in \mathbb{Z}$ y $x \in \mathbb{Q} \setminus \{0\}$ entonces $k = 0$). En cambio, en $\mathbb{Q}/\mathbb{Z}$ todo elemento tiene orden finito. En efecto, si $x = r/s \in \mathbb{Q}$, entonces, como

$$s(x+\mathbb{Z}) = sx+\mathbb{Z} = r+\mathbb{Z} = \mathbb{Z}$$

se concluye que $|x+\mathbb{Z}| \leq s$.

Ejemplo 7.28. Veamos que $\mathscr{U}(\mathbb{Z}/5) \simeq \mathscr{U}(\mathbb{Z}/10)$. En efecto, ambos grupos son cíclicos de orden cuatro pues $\mathscr{U}(\mathbb{Z}/5) = \langle 2\rangle$ y $\mathscr{U}(\mathbb{Z}/10) = \langle 3\rangle$. En cambio, $\mathscr{U}(\mathbb{Z}/10) \not\simeq \mathscr{U}(\mathbb{Z}/12)$ pues en $\mathscr{U}(\mathbb{Z}/12)$ no hay elementos de orden cuatro.

Ejercicio 7.29. Demuestre que $F = \{\sigma \in \mathbb{S}_n : \sigma(n) = n\} \leq \mathbb{S}_n$ y que $F \simeq \mathbb{S}_{n-1}$.

Si G y H son grupos, utilizaremos la siguiente notación:

$$\mathrm{Hom}(G,H) = \{f\colon G \to H : f \text{ es morfismo}\}.$$

Veamos algunos ejemplos.

Ejemplo 7.30. Veamos que $\mathrm{Hom}(\mathbb{Q},\mathbb{Z}) = \{0\}$. Sea $f \in \mathrm{Hom}(\mathbb{Q},\mathbb{Z})$ y sea p un número primo. Si fijamos $x \in \mathbb{Q}$ tenemos entonces, como

$$f(x) = f\left(p(x/p)\right) = pf(x/p),$$

p divide a $f(x)$, de donde se concluye que $f(x) = 0$ para todo $x \in \mathbb{Q}$ pues el primo p es arbitrario.

Ejemplo 7.31. Si G es un grupo, entonces $\mathrm{Hom}(\mathbb{Z},G) = \{k \mapsto g^k : g \in G\}$. Primero observemos que para cada $g \in G$ la función $\mathbb{Z} \to G$, $k \mapsto g^k$, es un morfismo de grupos, pues $k+l \mapsto g^{k+l} = g^k g^l$. Sea $f \in \mathrm{Hom}(\mathbb{Z},G)$ y sea $g = f(1)$. Si $k > 0$,

$$f(k) = f(\underbrace{1+\cdots+1}_{k-\text{veces}}) = f(1)^k = g^k.$$

Si, en cambio $k < 0$, entonces

$$f(k) = f(\underbrace{(-1)+\cdots+(-1)}_{|k|-\text{veces}}) = f(-1)^{-k} = (g^{-1})^{-k} = g^k.$$

Ejemplo 7.32. Vamos a demostrar que $\mathrm{Hom}(\mathbb{Z}/8,\mathbb{Z}/10)$ tiene dos elementos. Sea $f\colon \mathbb{Z}/8 \to \mathbb{Z}/10$ un morfismo no nulo. Si $n = |f(1)|$, entonces n divide a 8, es decir $n \in \{1,2,4,8\}$. Como además $f(1) \in \mathbb{Z}/10$ y f es no nulo, $n = 2$. Luego $f(1) = 5$ y eso define únivocamente al morfismo f. En nuestro caso, vemos que $f(k) = 5k$ para $k \in \{0,1,\ldots,7\}$.

Ejercicio 7.33. Calcule $\mathrm{Hom}(\mathbb{Z}/n, G)$ para cualquier grupo G.

Ejercicio 7.34. Sean A, B y C grupos. Si $f \in \mathrm{Hom}(A,B)$ y $g \in \mathrm{Hom}(B,C)$, entonces $g \circ f \in \mathrm{Hom}(A,C)$.

Ejercicio 7.35. Demuestre que $\mathbb{Z}/2 \times \mathbb{Z}/2$ y $\mathbb{Z}/4$ son los únicos subgrupos de orden cuatro (salvo isomorfismo).

Veamos un ejemplo de isomorfismo un poco más difícil que los anteriores.

Ejemplo 7.36. Si G es un grupo de orden seis, entonces $G \simeq \mathbb{S}_3$ o bien G es cíclico de orden seis. Para demostrar nuestra afirmación primero observamos que, como $|G|$ es par, existe en G un elemento de orden dos, esto lo vimos en el ejercicio 2.12. Si todo elemento de $G \setminus \{1\}$ tuviera orden dos, entonces $xy = yx$ para todo $x, y \in G$ y luego

$$\langle x,y\rangle = \{1,x,y,xy\} \leq G,$$

una contradicción al teorema de Lagrange. Existe entonces $x \in G$ tal que x tiene orden dos y existe $y \in G \setminus \{1\}$ tal que y no tiene orden dos. Nuevamente el teorema de Lagrange nos dice que $|y| \in \{3,6\}$ (pues el orden de y es un divisor del orden del grupo G). Si $|y| = 6$, entonces $G \simeq \mathbb{Z}/6$. En cualquier caso, existe $z \in G$ tal que $|z| = 3$. Tenemos

$$\langle x,z\rangle = \{1,x,z,z^2,xz,xz^2\} = G.$$

Para saber qué grupo es $\langle x,z\rangle$ necesitamos entender el producto zx. Sabemos que $zx \in \{xz,xz^2\}$. Si $xz = zx$, entonces $|xz| = 6$ (pues $(xz)^k \neq 1$ para todo $k \in \{1,\ldots,5\}$ y además $(xz)^6 = 1$) y luego $G = \langle xz\rangle \simeq \mathbb{Z}/6$. Si, en cambio, estamos en el caso $zx = xz^2$, entonces $G = \langle x,z : x^2 = z^3 = 1, xzx^{-1} = z^2\rangle \simeq \mathbb{D}_3$.

Lo que hicimos hasta ahora nos permite clasificar las clases de isomorfismo de grupos de orden ≤ 8.

Orden	Cantidad	Grupos
1	1	$\{1\}$
2	1	$\mathbb{Z}/2$
3	1	$\mathbb{Z}/3$
4	2	$\mathbb{Z}/4$, $\mathbb{Z}/2 \times \mathbb{Z}/2$
5	1	$\mathbb{Z}/5$
6	2	$\mathbb{Z}/6$, $\mathbb{S}_3$
7	1	$\mathbb{Z}/7$

Cuadro 7.1: Grupos de orden ≤ 7.

Ejercicio 7.37. Demuestre que salvo isomorphismo los únicos grupos de orden nueve son $\mathbb{Z}/9$ y $\mathbb{Z}/3 \times \mathbb{Z}/3$.

Estamos en condiciones de enunciar y demostrar los teoremas de isomorfismos.

Teorema 7.38 (primer teorema de isomorfismos). *Si $f\colon G \to H$ es un morfismo de grupos, entonces $G/\ker f \simeq f(G)$.*

Demostración. Sean $K = \ker f$ y $\varphi\colon G/K \to H$ la función dada por $xK \mapsto f(x)$. Primero debemos demostrar que φ está bien definida, lo que significa demostrar que si $xK = yK$ entonces $f(x) = f(y)$. En efecto, si $xK = yK$, entonces, como $y^{-1}x \in K$, se tiene que

$$f(y)^{-1}f(x) = f(y^{-1}x) \in f(K) = \{1\}.$$

Luego $f(x) = f(y)$.

Veamos que φ es morfismo de grupos:

$$\varphi(xKyK) = \varphi(xyK) = f(xy) = f(x)f(y) = \varphi(xK)\varphi(yK).$$

Para calcular $\ker\varphi$ procedemos así:

$$\pi(x) = xK \in \ker\varphi \iff \varphi(xK) = 1 \iff f(x) = 1 \iff x \in K.$$

En consecuencia, $\ker\varphi$ es trivial y entonces φ es inyectiva. Como es trivial verificar que φ es sobreyectica, se concluye que $G/K \simeq f(G)$. □

Ejemplos 7.39. Si G es un grupo, entonces $G/\{1\} \simeq G$ y $G/G \simeq \{1\}$.

Ejemplo 7.40. Como $f\colon \mathbb{Z} \to \mathbb{Z}/n$, $x \mapsto x$ mód n, es un morfismo sobreyectivo con $\ker f = n\mathbb{Z}$, del primer teorema de isomorfismos se concluye que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.

Ejemplo 7.41. Sea G un grupo cíclico infinito, digamos $G = \langle g\rangle$. Es fácil verificar que la función $f\colon \mathbb{Z} \to G$, $k \mapsto g^k$, es un isomorfismo de grupos, es decir $G \simeq \mathbb{Z}$. En particular, $G = \langle g^k\rangle$ si y sólo si $k \in \{-1, 1\}$.

Ejemplo 7.42. Vamos a demostrar que $\mathbb{Z}/n\mathbb{Z} \simeq G_n$. Sea

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

Es claro que f es morfismo sobreyectivo y que $\ker f = n\mathbb{Z}$. El resultado que queremos demostrar se obtiene entonces inmediatemente del primer teorema de isomorfismos.

Ejemplo 7.43. Observemos con $2\mathbb{Z} \simeq 3\mathbb{Z}$ (observar que ambos son cíclicos de orden infinito o considerar la función $2k \mapsto 3k$) y que

$$\mathbb{Z}/2 \simeq \mathbb{Z}/2\mathbb{Z} \not\simeq \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/3.$$

Ejemplo 7.44. Como

$$f\colon \mathbb{C}^\times \to \mathbb{C}^\times, \quad f(z) = \frac{z}{|z|},$$

es un morfismo tal que $\ker f = \mathbb{R}_{>0}$ y $f(\mathbb{C}^\times) = S^1$, se concluye del primer teorema de isomorfismos que $\mathbb{C}^\times/\mathbb{R}_{>0} \simeq S^1$.

Ejemplo 7.45. El primer teorema de isomorfismos aplicado a $f\colon S^1 \to S^1$, $f(z) = z^2$, permite demostrar que $S^1/\{\pm 1\} \simeq S^1$ pues $\ker f = \{-1,1\}$ y $f(S^1) = S^1$.

Ejemplo 7.46. Sea $f\colon \mathbb{C}^\times \to \mathbb{C}^\times$, $f(z) = |z|$. Como $\ker f = S^1$ y $f(\mathbb{C}^\times) = \mathbb{R}_{>0}$, se conluye del primer teorema de isomorfismos que $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$.

Ejemplo 7.47. Veamos que $(\mathbb{Z}\times\mathbb{Z})/\langle(1,3)\rangle \simeq \mathbb{Z}$. Para eso, consideramos el morfismo sobreyectivo $f\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$, $f(x,y) = 3x - y$. Como

$$\ker f = \{(x,3x) : x \in \mathbb{Z}\} = \langle(1,3)\rangle,$$

el primer teorema de isomorfismos implica que $(\mathbb{Z}\times\mathbb{Z})/\langle(1,3)\rangle \simeq \mathbb{Z}$.

Ejercicio 7.48. Demuestre que $\mathbb{R}/\mathbb{Z} \simeq S^1$.

Ejercicio 7.49. Demuestre que $\mathbb{Q}/\mathbb{Z} \simeq \cup_{n\geq 1} G_n$.

Ejercicio 7.50. Demuestre que $(\mathbb{Z}\times\mathbb{Z})/\langle(6,3)\rangle \simeq \mathbb{Z}\times(\mathbb{Z}/3)$.

Ejemplo 7.51. Si V es un espacio vectorial y W es un subespacio de V, entonces, en particular, V es un grupo abeliano y W es un subgrupo normal de V. El grupo abeliano V/W es entonces un espacio vectorial con

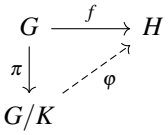
$$\lambda(v+W) = (\lambda v) + W, \quad \lambda \in \mathbb{R},\, v \in V,$$

y el morfismo canónico $\pi\colon V \to V/W$ resulta ser una transformación lineal. Dejamos como ejercicio demostrar que $\dim(V/W) = \dim V - \dim W$ si $\dim V < \infty$.

Si $f\colon V \to U$ es una transformación lineal, entonces, por el primer teorema de isomorfismos, en particular, $V/\ker f \simeq f(V)$ como grupos abelianos. Como el morfismo del primer teorema de isomorfismos es además una transformación lineal, se concluye que $V/\ker f \simeq f(V)$ como espacios vectoriales. En particular, si $\dim V < \infty$, entonces

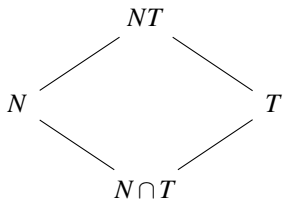
$$\dim V - \dim \ker f = \dim f(V).$$

Ejercicio 7.52. Sea $f\colon G \to H$ un morfismo de grupos y K un subgrupo normal de G tal que $K \subseteq \ker f$. Demuestre que existe un único morfismo $\varphi\colon G/K \to H$ tal que el diagrama



es conmutativo, lo que significa que $\varphi \circ \pi = f$, donde $\pi\colon G \to G/K$ es el morfismo canónico. Más aún, $\ker\varphi = \pi(\ker f)$ y $\varphi(G/K) = f(G)$. En particular, φ es inyectiva si y sólo si $\ker f = K$ y φ es sobreyectiva si y sólo si f es sobreyectiva.

El segundo teorema de isomorfismos resultará de gran utilidad al estudiar series de composición y resolubilidad. El diagrama que vemos a continuación nos ayudará a recordar cómo funciona el segundo teorema de isomorfismos:



Teorema 7.53 (segundo teorema de isomorfismos). *Si N es un subgrupo normal de G y T es un subgrupo de G, entonces $N \cap T$ es normal en T y además*

$$T/N \cap T \simeq NT/N.$$

Demostración. Sea $\pi\colon G \to G/N$ el morfismo canónico. Ya vimos que la restricción $\pi|_T\colon T \to G/N$ es un morfismo de grupos con núcleo $\ker(\pi|_T) = T \cap N$. En particular, $T \cap N$ es normal en T. Al aplicar el primer teorema de isomorfismos, $T/(T \cap N) \simeq \pi(T)$. Como N es normal en G, NT es un subgrupo de G que contiene a N. La restricción $\pi|_{NT}$ es entonces un morfismo de grupos con núcleo $NT \cap N = N$. Al aplicar el primer teorema de isomorfismos a $\pi|_{NT}$ obtenemos $NT/N \simeq \pi(NT) = \pi(T)$. □

Ejercicio 7.54. Sea N normal en G y sea $\pi\colon G \to G/N$ el morfismo canónico. Demuestre que si L es un subgrupo de G, entonces $\pi^{-1}(\pi(L)) = NL$.

En el siguiente ejemplo utilizaremos la notación aditiva.

Ejemplo 7.55. Sea $G = \mathbb{Z}/24$ y sean $H = \langle 4\rangle$ y $N = \langle 6\rangle$. Como G es abeliano, H y K son ambos normales en G. Un cálculo directo nos muestra que $H + N = \langle 2\rangle$ y que $H \cap N = \{0, 12\}$. Notemos que este ejemplo está completamente hecho en la notación aditiva. Calculemos las coclases de N en $H + N$:

$$0 + N = \{0, 6, 12, 18\}, \quad 2 + N = \{2, 8, 14, 20\}, \quad 4 + N = \{4, 10, 16, 22\}.$$

Las coclases de $H \cap N$ en H son:

$$0 + (H \cap N) = \{0, 12\}, \quad 4 + (H \cap N) = \{4, 16\}, \quad 8 + (H \cap N) = \{8, 20\}.$$

El segundo teorema de isomorfismos nos dice que $(H + N)/N \simeq H/H \cap N$. El isomorfismo está dado por $f\colon H/(H \cap N) \to (H + N)/N$, $h + (H \cap N) \mapsto h + N$. En nuestro caso,

$$f(0+(H\cap N)) = 0+N,$$
$$f(4+(H\cap N)) = 4+N,$$
$$f(8+(H\cap N)) = 8+N = 2+N.$$

En los ejemplos que siguen veremos que el segundo teorema de isomorfismos no es algo raro sino que nos permite obtener fórmulas ya conocidas.

Ejemplo 7.56. Sean $a,b\in\mathbb{Z}$ no nulos. Sabemos que $a\mathbb{Z}+b\mathbb{Z} = \operatorname{mcd}(a,b)\mathbb{Z}$ y que $a\mathbb{Z}\cap b\mathbb{Z} = \operatorname{mcm}(a,b)\mathbb{Z}$. Al aplicar el segundo teorema de isomorfismos,

$$\frac{\operatorname{mcd}(a,b)\mathbb{Z}}{b\mathbb{Z}} = \frac{a\mathbb{Z}+b\mathbb{Z}}{b\mathbb{Z}} \simeq \frac{a\mathbb{Z}}{a\mathbb{Z}\cap b\mathbb{Z}} = \frac{a\mathbb{Z}}{\operatorname{mcm}(a,b)\mathbb{Z}}.$$

Al aplicar orden, obtenemos la fórmula

$$ab = \operatorname{mcd}(a,b)\operatorname{mcm}(a,b).$$

Veamos otra aplicación. Un grupo G que contiene un subgrupo normal abeliano N y es tal que G/N es abeliano se conoce como grupo **meta-abeliano**. Claramente, los grupos meta-abelianos no son necesariamente abelianos (el grupo simétrico $\mathbb{S}_3$ es meta-abeliano y no abeliano). El segundo teorema de isomorfismos nos permite demostrar que subgrupos de meta-abelianos son meta-abelianos.

Proposición 7.57. *Si G es un grupo meta-abeliano y H es un subgrupo de G, entonces H es también meta-abeliano.*

Demostración. Como G es meta-abeliano, existe un subgrupo normal N de G tal que N y G/N son ambos abelianos. El subgrupo abeliano $H\cap N$ es normal en H. Gracias al segundo teorema de isomorfismos,

$$H/(H\cap N) \simeq HN/N$$

es un grupo abeliano pues HN/N es un subgrupo del grupo abeliano G/N. □

Dejamos la demostración del tercer teorema de isomorfismos como ejercicio. Primero, un resultado auxiliar que facilitará los cálculos.

Ejercicio 7.58. Sea $f\colon G\to H$ un morfismo de grupos y sean $U\trianglelefteq G$ y $V\trianglelefteq H$. Demuestre que existe un morfismo de grupos $g\colon G/U\to H/V$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & H \\ {\scriptstyle\pi_U}\downarrow & & \downarrow{\scriptstyle\pi_V} \\ G/U & \xrightarrow[\ g\ ]{} & H/V \end{array}$$

es conmutativo si y sólo si $f(U)\subseteq V$, donde $\pi_U\colon G\to G/U$ y $\pi_V\colon H\to H/V$ son los morfismos canónicos. Además, en este caso,

1) Si f es sobreyectiva, entonces g es sobreyectiva.
2) Si $U = f^{-1}(V)$, entonces g es inyectiva.

Ejercicio 7.59 (tercer teorema de isomorfismos). Sean S y T subgrupos normales de un grupo G tales que $S \subseteq T$. Demuestre que entonces S es normal en T y T/S es normal en G/S. Además

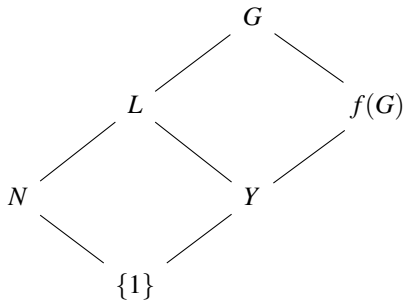
$$\frac{G/S}{T/S} \simeq G/T,$$

donde $T/S = \{tS : t \in T\}$.

Ejemplo 7.60. Si m divide a n, entonces $n\mathbb{Z} \leq m\mathbb{Z} \leq \mathbb{Z}$. Luego

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/m\mathbb{Z}.$$

El teorema que sigue es también muy importante. Para recordar cómo funciona, podemos hacer uso del siguiente diagrama:



Teorema 7.61 (de la correspondencia). *Sea $f\colon G \to H$ un morfismo de grupos y sea $K = \ker f$. Existe una correspondencia biyectiva entre*

$$\mathscr{A} = \{L : K \leq L \leq G\} \underset{\tau}{\overset{\sigma}{\rightleftarrows}} \{Y : Y \leq f(G)\} = \mathscr{B}$$

La correspondencia está dada por $\sigma(L) = f(L)$ y $\tau(Y) = f^{-1}(Y)$. Valen además las siguientes afirmaciones:

1) $L_1 \leq L_2$ si y sólo si $\sigma(L_1) \leq \sigma(L_2)$.
2) $L \trianglelefteq G$ si y sólo si $\sigma(L) \trianglelefteq f(G)$.

Demostración. Primero observamos que σ y τ están ambas bien definidas pues vimos en un ejercicio que $f(L) \leq f(G)$ y $K \leq f^{-1}(Y) \leq G$.

Veamos que $\tau \circ \sigma = \mathrm{id}_{\mathscr{A}}$. Queremos ver que $\tau(\sigma(L)) = L$ para todo $L \in \mathscr{A}$. Si $x \in f^{-1}(f(L))$ entonces $f(x) \in f(L)$ y luego $f(x) = f(l)$ para algún $l \in L$. Esto implica que $xl^{-1} \in K$ y entonces $x \in Kl \subseteq L$ pues $K \subseteq L$. Recíprocamente, si $l \in L$ entonces $f(l) \in f(L)$ y luego $l \in f^{-1}(f(L))$.

Veamos que $\sigma \circ \tau = \mathrm{id}_{\mathscr{B}}$. Si $Y \in \mathscr{B}$, entonces $\sigma(\tau(Y)) = Y$. Si $y \in Y \subseteq f(G)$, entonces $y = f(x)$ para algún $x \in G$, es decir $x \in f^{-1}(y)$, lo que trivialmente implica que $y = f(x) \in f(f^{-1}(Y))$. Recíprocamente, si $y \in f(f^{-1}(Y))$, entonces $y = f(x)$ para $x \in f^{-1}(Y)$. Pero esto significa que $y = f(x) \in Y$.

Dejamos como ejercicio demostrar que $X \leq Y$ si y sólo si $f(X) \leq f(Y)$.

Vamos a demostrar que $L \trianglelefteq G$ si y sólo si $f(L) \trianglelefteq f(G)$. Si $L \trianglelefteq G$ y $x \in G$, entonces $xLx^{-1} = L$. Esto implica que $f(L) = f(xLx^{-1}) = f(x)f(L)f(x)^{-1}$, es decir que $f(L)$ es normal en $f(G)$. Recíprocamente, si $f(L) \trianglelefteq f(G)$ y $x \in G$, entoces

$$f(xLx^{-1}) = f(x)f(L)f(x)^{-1} = f(L).$$

Esto implca que $xLx^{-1} \subseteq LK \subseteq L$ y luego $xLx^{-1} \subseteq L$, que implica la normalidad de L en G gracias a la proposición 5.3. □

Veamos una aplicación del teorema anterior.

Proposición 7.62. *Si $f\colon G \to f(G)$ es un morfismo sobreyectivo de grupos y $H \leq G$ es tal que $K = \ker f \subseteq H$, entonces $(G : H) = (f(G) : f(H))$.*

Demostración. Por el teorema anterior sabemos que existe una correspondencia biyectiva

$$\{L : K \leq L \leq G\} \rightleftarrows \{Y : Y \leq f(G)\}$$

dada por $H \mapsto f(H)$ e inversa dada por $f^{-1}(T) \hookleftarrow T$. Sea $H \leq G$ tal que $\ker f \subseteq H$ y sea $\alpha\colon G/H \to f(G)/f(H)$ la función dada por $\alpha(gH) = f(g)f(H)$. Dejamos como ejercicio verificar que α está bien definida. Veamos que α es una función biyectiva pues, en ese caso,

$$(G : H) = |G/H| = |f(G)/f(H)| = (f(G) : f(H)).$$

Veamos que α es sobreyectiva: si $yf(H) \in f(G)/f(H)$ entonces $y = f(g)$ para algún $g \in G$ (pues f es sobreyectiva). Luego

$$yf(H) = f(g)f(H) = f(gH) = \alpha(gH).$$

Veamos ahora que α es inyectiva: si $\alpha(gH) = \alpha(g_1H)$, entonces, por la definición de la función α,

$$f(g)^{-1}f(g_1) = f(h) \in f(H)$$

para algún $h \in H$, es decir $f(g_1) = f(g)f(h) = f(gh)$ para algún $h \in H$. Esto implica que $g_1 = ghk$ para algún $k \in \ker f \subseteq H$ y luego $g_1 = gh_1$ para algún $h_1 \in H$, es decir $g_1H = gH$. □

Es conviente enfatizar qué forma toma el teorema anterior en el caso del morfismo canónico $\pi\colon G \to G/N$. Si N es un subgrupo normal de G, entonces la función $K \mapsto K/N$ es una biyección entre el conjunto de subgrupos (normales) de G que contienen a N y el conjunto de subgrupos (normales) de G/N. Observemos que si H es un subgrupo de G, entonces

$$\pi(H) = HN/N.$$

Ejemplo 7.63. Como aplicación del teorema de la correspondencia, vamos a demostrar que todo subgrupo del grupo no abeliano

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

es normal en Q_8. Sea $N = \{-1, 1\}$. Entonces N es normal en Q_8 (pues $N \subseteq Z(Q_8)$) y además, como Q_8/N tiene cuatro elementos, Q_8/N es un grupo abeliano.

Afirmamos que N está contenido en cualquier subgrupo no trivial de Q_8. En efecto, si K es un subgrupo no trivial de Q_8, entonces $-1 \in K$ (pues, por ejemplo, si $-i \in K$, entonces $-1 = (-i)^2 \in K$). Esto implica que cualquier subgrupo de Q_8 se corresponde con un subgrupo de Q_8/N y allí todo subgrupo es normal pues Q_8/N es abeliano. Más precisamente, si $S \leq Q_8$, entonces $\pi(S) \leq Q_8/N$. Como Q_8/N es abeliano, $\pi(S)$ es normal en Q_8/N. Como $N \subseteq S$, se tiene que $S = \pi^{-1}(\pi(S))$. Luego S es normal en Q_8.

En el ejemplo anterior, podríamos haber demostrado que $G/N \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, ya que como sabemos que $|G/N| = 4$, hubiera alcanzado con calcular el orden de cada uno de los elementos de G/N.

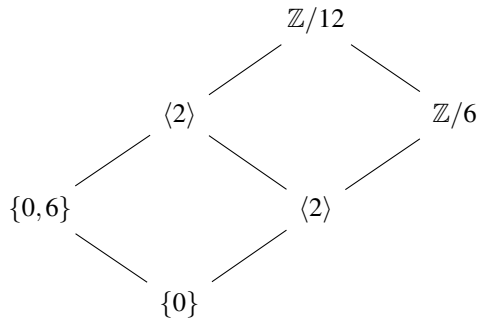
Ejemplo 7.64. Sea $f\colon \mathbb{Z}/12 \to \mathbb{Z}/6$ el morfismo dado por $1 \mapsto 1$. Un cálculo sencillo nos muestra que $K = \ker f = \{0, 6\}$. Los subgrupos de $\mathbb{Z}/12$ que contienen a K son

$$\langle 1\rangle = \{0, 1, \ldots, 11\}, \quad \langle 2\rangle = \{0, 2, 4, 6, 8, 10\}, \quad \langle 3\rangle = \{0, 3, 6, 9\}, \quad \langle 6\rangle = \{0, 6\},$$

que vía f se corresponden con los subgrupos

$$\langle 1\rangle = \{0, 1, \ldots, 5\}, \quad \langle 2\rangle = \{0, 2, 4\}, \quad \langle 3\rangle = \{0, 3\}, \quad \{0\}$$

de $\mathbb{Z}/6$, respectivamente. Por ejemplo,



Si se tiene un morfismo entre dos grupos, en cierto sentido, el teorema de la correspondencia nos permite trasladar propiedades de la imagen del morfismo al dominio. Veamos una aplicación concreta.

Ejemplo 7.65. Sea G un grupo finito que contiene un subgrupo normal N tal que $N \simeq \mathbb{Z}/5$ y $G/N \simeq \mathbb{S}_4$. Vamos a demostrar las siguientes afirmaciones sobre G.

1) $|G| = 120$
2) G contiene un subgrupo normal de tamaño 20.
3) G contiene tres subgrupos de orden 15, ninguno de ellos normal en G.

Para demostrar la primera afirmación usamos el teorema de Lagrange pues

$$24 = |G/N| = \frac{|G|}{|N|} = |G|/5.$$

Para la segunda afirmación, sea K el subgrupo de G/N isomorfo al grupo de Klein. Entonces K es normal en G/N y $|K| = 4$. Como $(G/N : K) = 6$, el subgrupo K de G/N se corresponde con un subgrupo normal H de G de índice 6. El teorema de Lagrange y el teorema de la correspondencia implican entonces que $|H| = 20$ pues

$$6 = (G/N : K) = (G : H) = \frac{|G|}{|H|}.$$

Para demostrar la tercera afirmación observamos que $G/N \simeq \mathbb{S}_4$ tiene cuatro subgrupos de orden 3 (son los subgrupos generados por un 3-ciclo), ninguno de ellos normal en G/N. Nuevamente, el teorema de la correspondencia, nos dice que estos grupos se corresponderán con 4 subgrupos de G, todos de orden 15 y ninguno de ellos normal en G.

Recordemos que si G es un grupo, $\mathbb{S}_G = \{f : G \to G : f \text{ es biyectiva}\}$. Terminaremos el capítulo con el siguiente teorema.

Teorema 7.66 (Cayley). *Todo grupo G es isomorfo a un subgrupo de $\mathbb{S}_G$.*

Demostración. Sea $f : G \to \mathbb{S}_G$, $g \mapsto L_g$, donde $L_g : G \to G$, $L_g(x) = gx$. La función f es un morfismo de grupos pues

$$L_{gh}(x) = (gh)x = g(hx) = L_g(hx) = L_g L_h(x)$$

para todo $g, h, x \in G$. Además es fácil verificar que f es inyectivo (si $f(g) = f(h)$ entonces $L_g = L_h$, es decir que $gx = L_g(x) = L_h(x) = hx$ para todo $x \in G$, que implica que $g = h$). □

Como aplicación, observamos que todo grupo finito es isomorfo a un subgrupo $\mathbb{S}_n$ para algún $n \in \mathbb{N}$. En particular, las matrices de permutación nos permiten observar que todo grupo finito es un **grupo lineal**, es decir, isomorfo a un subgrupo de $\mathbf{GL}_n(\mathbb{Z})$ para algún $n \in \mathbb{N}$. Veamos una aplicación un poquito más sofisticada.

Proposición 7.67. *Todo grupo simple finito G está contenido en algún $\mathbb{A}_n$.*

Demostración. Si $|G| = 2$, el resultado es trivial pues $G \simeq \mathbb{A}_2$. Supongamos entonces que $|G| > 2$. Sea $f : G \to \mathbb{S}_n$ el morfismo inyectivo obtenido del teorema de

Cayley. Si $H = f(G)$, entonces $G \simeq H$ por el primer teorema de isomorfismos. Afirmamos que $H \subseteq \mathbb{A}_n$. Si H no es un subgrupo de $\mathbb{A}_n$, existe $h \in H$ tal que $h \notin \mathbb{A}_n$. Escribimos $h = f(g)$ para algún $g \in G$. Como $h \notin \mathbb{A}_n$,

$$\text{signo}(f(g)) = \text{signo}(h) = -1,$$

entonces $g \notin \ker(\text{signo} \circ f)$. Sea $K = \ker(\text{signo} \circ f)$. Entonces $K = \{1\}$ pues G es simple. Además, $\text{signo} \circ f$ es una función biyectiva pues $\text{signo}(f(1)) = 1$ y $\text{signo}(f(g)) = -1$. En consecuencia, $G \simeq G/K \simeq \mathbb{Z}/2$, por el primer teorema de isomorfismos. En particular, $|G| = 2$, una contradicción. Luego $H \subseteq \mathbb{A}_n$. □

Como aplicación simpática del teorema de Cayley puede obtenerse que el axioma de asociatividad en un grupo permite demostrar que ningún producto necesita llevar paréntesis. En efecto, el teorema de Cayley afirma que G es un subgrupo de $\mathbb{S}_G$. La composición de funciones es asociativa y es trivial observar que ninguna composición arbitraria y finita de funciones necesita llevar paréntesis, por eso escribimos

$$(f_1 \circ \cdots \circ f_n)(g) = f_1(f_2(\cdots f_n(g)) \cdots).$$

Capítulo 8
Grupos simples

Recordemos que un grupo G es **simple** si $G \neq \{1\}$ y sus únicos subgrupos normales son G y $\{1\}$.

Ejemplo 8.1. Si p es un número primo, $\mathbb{Z}/p$ es simple.

No es difícil demostrar que $\mathbb{A}_5$ es simple, pero necesitamos repasar algunos conceptos. Si G es un grupo y $g \in G$, la clase de conjugación de g en G es el conjunto $\{xgx^{-1} : x \in G\}$. Una observación sencilla pero importante: Si el subgrupo N de G es normal en G, entonces N es uníón de clases de conjugación de G, y una de esas clases es $\{1\}$, pues

$$N = \bigcup_{n \in N} \{xnx^{-1} : x \in G\}.$$

Veamos una aplicación sencilla de la afirmación anterior.

Proposición 8.2. *El grupo alternado $\mathbb{A}_5$ es simple.*

Demostración. Para demostrar el teorema vamos a contar los tamaños de las clases de conjugación de $\mathbb{A}_5$. Las clases de conjugación de $\mathbb{A}_5$ y sus tamaños son:

id	1
(123)	20
$(12)(34)$	15
(12345)	12
(21345)	12

Si N es un subgrupo normal de $\mathbb{A}_5$, entonces N es unión de clases de conjugación de $\mathbb{A}_5$ y una de esas clases es $\{id\}$. Sin embargo, ninguna unión de clases de conjugación de $\mathbb{A}_5$ que incluya $\{id\}$ tendrá tamaño un divisor de 60, a menos que $N = \{\mathrm{id}\}$ o bien que $N = \mathbb{A}_5$. □

Nuestro objetivo es demostrar que los grupos alternados $\mathbb{A}_n$ son simples siempre que $n \geq 5$. Para eso, necesitamos demostrar varios lemas auxiliares.

Recordemos toda permutación $\rho \in \mathbb{S}_n$ puede descomponerse como producto de ciclos disjuntos, digamos

$$\rho = (a_1 \cdots a_r)(b_1 \cdots b_s) \cdots (c_1 \cdots c_t)$$

donde por convención omitiremos aquellos ciclos de longitud uno. La estrucutra cíclica de ρ será entonces la sucesión ordenada de los números $r,s,\ldots t$, donde convenientemente omitiremos los puntos fijos. Por ejemplo, la estructura cíclica de la trasposición (ab) es 2, del 3-ciclo $(abc)(d)$ es 3 y de la permutación $(123)(45)(789a)(bcd)(d)$ es 2,3,3,4.

El primer lema que demostraremos afirma que dos permutaciones tienen la misma estructura cíclica si y sólo si son conjugadas.

Lema 8.3. *Si ρ_1 y ρ_2 son permutaciones de $\mathbb{S}_n$ con la misma estructura cíclica, entonces $\rho_2 = \sigma\rho_1\sigma^{-1}$ para alguna permutación $\sigma \in \mathbb{S}_n$.*

Demostración. Supongamos que

$$\rho_1 = (a_1 \cdots a_r)(b_1 \cdots b_s) \cdots (c_1 \cdots c_t), \quad \rho_2 = (x_1 \cdots x_r)(y_1 \cdots y_s) \cdots (z_1 \cdots z_t).$$

Sean

$$\mathrm{Fix}(\rho_1) = \{x \in \{1,\ldots,n\} : \rho_1(x) = x\} = \{k_1,\ldots,k_m\}, \quad \mathrm{Fix}(\rho_2) = \{l_1,\ldots,l_m\}$$

los puntos fijos de las permutaciones ρ_1 y ρ_2, respectivamente. Entonces

$$\sigma(x) = \begin{cases} x_j & \text{si } x = a_j \text{ para algún } j, \\ y_j & \text{si } x = b_j \text{ para algún } j, \\ \vdots & \\ z_j & \text{si } x = c_j \text{ para algún } j, \\ l_j & \text{si } x = k_j \text{ para algún } j, \end{cases}$$

cumple que $\sigma\rho_1\sigma^{-1} = \rho_2$. □

El siguiente lema es la variante del anterior correspondiente al grupo alternado. Nos interesa saber cuándo dos permutaciones conjugadas en $\mathbb{S}_n$ son también conjugadas en $\mathbb{A}_n$.

Lema 8.4. *Si $\rho_1, \rho_2 \in \mathbb{S}_n$ son conjugados en $\mathbb{S}_n$ y además $|\mathrm{Fix}(\rho_1)| \geq 2$, entonces $\mu\rho_1\mu^{-1} = \rho_2$ para algún $\mu \in \mathbb{A}_n$.*

Demostración. Supongamos que $\rho_2 = \sigma\rho_1\sigma^{-1}$ para algún $\sigma \in \mathbb{S}_n$. Por hipótesis, sabemos que existen $a,b \in \{1,\ldots,n\}$ tales que $\rho_1(a) = a$, $\rho_1(b) = b$ y $a \neq b$. Sea

$$\mu = \begin{cases} \sigma & \text{si } \sigma \in \mathbb{A}_n, \\ \sigma(ab) & \text{en caso contrario.} \end{cases}$$

Entonces $\mu \in \mathbb{A}_n$ y además $\mu\rho_1\mu^{-1} = \rho_2$ pues (ab) conmuta on ρ_1. □

Veamos algunos ejemplos.

Ejemplo 8.5. Si $\rho_1 = (23)(156)$ y $\rho_2 = (45)(123)$, entonces el lema anterior nos dice que $\rho_2 = \sigma\rho_1\sigma^{-1}$ si

$$\sigma = \begin{pmatrix} 123456 \\ 145623 \end{pmatrix}.$$

Ejemplo 8.6. Los 3-ciclos $\rho_1 = (123)$ y $\rho_2 = (132)$ son conjugados en $\mathbb{S}_3$ pues $(123) = \sigma(132)\sigma^{-1}$ si $\sigma = (23)$. Sin embargo, ρ_1 y ρ_2 no son conjugados en $\mathbb{A}_3$.

Estamos en condiciones de probar el teorema del capítulo.

Teorema 8.7 (Jordan). *Si $n \geq 5$, $\mathbb{A}_n$ es simple.*

Demostración. Sea $N \neq \{\mathrm{id}\}$ un subgrupo normal de $\mathbb{A}_n$. Si $(abc) \in N$, entonces cualquier 3-ciclo también está en N (pues todos los 3-ciclos son conjugados en $\mathbb{S}_n$ y por el lema anterior sabemos que $(ijk) = \mu(abc)\mu^{-1} \in N$ para algún $\mu \in \mathbb{A}_n$. Luego $N = \mathbb{A}_n$.

Vamos a demostrar ahora que nuestro N siempre contiene un 3-ciclo. Como N es no trivial, existe $\sigma \in N \setminus \{\mathrm{id}\}$. Sean $m = |\sigma|$ y p un primo tal que divide a m. Entonces $\tau = \sigma^{m/p}$ tiene orden p y luego $\tau = \rho_1 \cdots \rho_s$, donde los ρ_j son p-ciclos disjuntos.

Si $p = 2$, entonces $1 = \mathrm{signo}(\tau) = (-1)^s$ y luego s es par. Escribimos

$$\tau = (ab)(cd)\rho_3 \cdots \rho_s$$

y entonces, como $\rho_3 \cdots \rho_s$ conmuta con (abc) y (acb),

$$(ac)(bd)\tau = (abc)\tau(abc)^{-1} \in N$$

y luego $(ab)(cd) \in N$. Sea $e \in \{1, \ldots, n\} \setminus \{a, b, c, d\}$. Entonces

$$(ae)(bd) = (aec)\underbrace{(ac)(bd)}_{\in N}(aec)^{-1} \in N$$

y luego

$$(aec) = (ac)(ae) = (ac)(bd)(ae)(bd) \in N.$$

Si $p = 3$, podemos suponer sin perder generalidad que $s \geq 2$ (pues de lo contrario τ sería un 3-ciclo). Entonces $\tau = (abc)(def)\rho_3 \cdots \rho_s$. Como (bcd) conmuta con $\rho_3 \cdots \rho_s$ y N es normal en $\mathbb{A}_n$, entonces

$$(adbce) = (bcd)\tau(bcd)^{-1}\tau^{-1} \in N$$

y luego

$$(adc) = (adb)(adbce)(adb)^{-1}(adbce)^{-1} \in N.$$

Si $p > 3$, entonces $\tau = (abcd\cdots z)\rho_2\cdots\rho_s$. En particular, (abc) conmuta con $\rho_2\cdots\rho_s$ y entonces

$$(abd) = (abc)\tau(abc)^{-1}\tau^{-1} \in N. \qquad \square$$

Como aplicación, vamos a calcular los subgrupos normales de $\mathbb{S}_n$ para $n \geq 5$.

Proposición 8.8. *Sea $n \geq 5$ y sea N un subgrupo normal de $\mathbb{S}_n$. Entonces $N = \{\mathrm{id}\}$, $N = \mathbb{A}_n$ o bien $N = \mathbb{S}_n$.*

Demostración. Sea N un subgrupo normal de $\mathbb{S}_n$. Como la restricción signo$|_N$ de la función signo a N es un morfismo de grupos,

$$(N : \ker(\mathrm{signo}|_N)) = |\mathrm{signo}(N)| \in \{1,2\}.$$

Si $(N : \ker(\mathrm{signo}|_N) = 1$, entonces $N \subseteq \mathbb{A}_n$ y entonces N es normal en $\mathbb{A}_n$. Luego $N = \{\mathrm{id}\}$ o bien $N = \mathbb{A}_n$ pues $\mathbb{A}_n$ es un grupo simple si $n \geq 5$.

Si $(N : \ker(\mathrm{signo}|_N) = 2$, entonces $N \cap \mathbb{A}_n = \ker(\mathrm{signo}|_N)$ es normal en $\mathbb{A}_n$ y luego, por la simplicidad de $\mathbb{A}_n$ para $n \geq 5$, $N \cap \mathbb{A}_n = \{\mathrm{id}\}$ o bien $N \cap \mathbb{A}_n = \mathbb{A}_n$.

En el primer caso, $|N| = 2$ y entonces N contiene una permutación impar que además tiene orden dos, digamos $\tau = (ij)\tau_2\cdots\tau_s$, escrita como producto de trasposiciones disjuntas. Entonces $\pi = (ik)\tau(ik) \in N$ si $k \notin \{i,j\}$ y $\pi \neq \tau$ pues $\tau(j) = i$ y $\pi(j) = k$. Luego $|N| \geq 3$, una contradicción.

En el segundo caso, si $N \cap \mathbb{A}_n = \mathbb{A}_n$, entonces $N = \mathbb{A}_n$. $\square$

Capítulo 9
Grupos de automorfismos

Si G es un grupo y $f\colon G \to G$ es un isomorfismo, diremos que f es un automorfismo de G. La composición de automorfismos de un grupo G es también un automorfismo de G. Se define entonces el **grupo de automorfismos** de G como

$$\mathrm{Aut}(G) = \{f\colon G \to G : f \text{ es un automorfismo de } G\}.$$

Obviamente $\mathrm{Aut}(G)$ es un grupo con la composición.

Ejemplo 9.1. $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}/2$ pues $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id}\}$.

Ejemplo 9.2. Sea G un grupo y sea $g \in G$. La conjugación $\gamma_g : G \to G$, $x \mapsto gxg^{-1}$, por g es un automorfismo de G pues

$$\gamma_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \gamma_g(x)\gamma_g(y).$$

Además $\gamma\colon G \to \mathrm{Aut}(G)$, $g \mapsto \gamma_g$, es un morfismo de grupos pues

$$\gamma_{gh}(x) = (gh)x(gh)^{-1} = g(\gamma_h(x))g^{-1} = \gamma_g(\gamma_h(x)) = (\gamma_g \circ \gamma_h)(x).$$

El grupo de **automorfismos interiores** de G se define como $\mathrm{Inn}(G) = \gamma(G)$. Observemos que $\ker\gamma = Z(G)$ pues si $g \in G$ es tal que $\gamma_g = \mathrm{id}$, entonces

$$\gamma_g(x) = gxg^{-1} = x$$

para todo $x \in G$. El primer teorema de isomorfismos implica entonces que

$$G/Z(G) \simeq \gamma(G) = \mathrm{Inn}(G).$$

Puede demostrarse que $\mathrm{Inn}(G)$ es un subgrupo normal de $\mathrm{Aut}(G)$. El cociente $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ se conoce como el grupo de **automorfismos exteriores** de G. Observemos que

$$\mathrm{Inn}(G) \text{ es cíclico} \iff |\mathrm{Inn}(G)| = 1 \iff G \text{ es abeliano.}$$

Ejemplo 9.3. Si G es no abeliano, entonces $\mathrm{Aut}(G)$ no es cíclico. En efecto, si $\mathrm{Aut}(G)$ es cíclico, entonces $G/Z(G) \simeq \mathrm{Inn}(G)$ es cíclico (por ser subgrupo de un cíclico) y luego G es abeliano.

Ejercicio 9.4. Si G es finito, entonces $\mathrm{Aut}(G)$ es finito.

Ejemplo 9.5. Veamos que $\mathrm{Aut}(\mathbb{S}_3) \simeq \mathbb{S}_3$. Sabemos que $Z(\mathbb{S}_3) = \{\mathrm{id}\}$. El ejemplo anterior nos permite entonces demostrar que $\mathrm{Inn}(\mathbb{S}_3) \simeq \mathbb{S}_3/Z(\mathbb{S}_3) \simeq \mathbb{S}_3$. Observemos entonces que

$$\mathrm{Inn}(\mathbb{S}_3) = \{\gamma_g | g \in \mathbb{S}_3\}.$$

Como $\mathrm{Inn}(\mathbb{S}_3) \subseteq \mathrm{Aut}(\mathbb{S}_3)$, sabemos que $\mathrm{Aut}(\mathbb{S}_3)$ tiene al menos seis elementos. Por otro lado, como $\mathbb{S}_3 = \langle (12), (13), (23) \rangle$, cada $f \in \mathrm{Aut}(\mathbb{S}_3)$ induce una permutación del conjunto $\{(12), (13), (23)\}$ y entonces $|\mathrm{Aut}(\mathbb{S}_3)| \leq 6$. En conclusión,

$$\mathrm{Aut}(\mathbb{S}_3) = \mathrm{Inn}(\mathbb{S}_3) \simeq \mathbb{S}_3.$$

Ejemplo 9.6. Si p es un número primo, entonces

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p) \simeq \mathbf{GL}_2(p).$$

En efecto, $\mathbb{Z}/p \times \mathbb{Z}/p$ es un espacio vectorial bidimensional sobre el cuerpo $\mathbb{Z}/p$ y todo automorfismo del grupo es también una transformación lineal inversible.

El ejemplo anterior puede generalizarse.

Ejercicio 9.7. Si p es un primo, C_p es el grupo cíclico de orden p y $G = C_p \times \cdots \times C_p$ (n-veces), demuestre que $\mathrm{Aut}(G) \simeq \mathbf{GL}_n(p)$.

Ejemplo 9.8. Vamos a demostrar que

$$\mathrm{Aut}(\mathbb{Z}/n) \simeq \mathscr{U}(\mathbb{Z}/n) = \{m + n\mathbb{Z} : \mathrm{mcd}(n,m) = 1\}.$$

Sea $G = \langle g \rangle \simeq \mathbb{Z}/n$. Si $\alpha \in \mathrm{Aut}(G)$, entonces $\alpha(g)$ es algún generador del grupo G, es decir $|\alpha(g)| = n$. En particular, $\alpha(g) = g^m$ para algún m. Vimos en el capítulo 2 que

$$|g^m| = \frac{n}{\mathrm{mcd}(n,m)}.$$

Como consecuencia, los generadores de G serán los elementos de la forma g^m con m tal que $\mathrm{mcd}(n,m) = 1$. La función

$$f\colon\ \mathrm{Aut}(G) \to \mathscr{U}(\mathbb{Z}/n), \quad \alpha \mapsto m,$$

donde m es tal que $\alpha(g) = g^m$, es un morfismo de grupos: si $\alpha, \beta \in \mathrm{Aut}(G)$, digamos $\alpha(g) = g^m$ y $\beta(g) = g^t$, entonces

$$\alpha(\beta(g)) = \alpha(g^t) = (g^t)^m = g^{tm},$$

es decir $f(\alpha \circ \beta) = f(\alpha) f(\beta)$. Además puede demostrarse que f no depende del generador g pues si $G = \langle g_1 \rangle$, entonces $g_1 = g^i$ para algún i y luego

$$\alpha(g_1) = \alpha(g^i) = \alpha(g)^i = (g^m)^i = g^{mi} = (g^i)^m = g_1^m.$$

Dejamos como ejercicio verificar que f es biyectiva.

Veamos algunos ejemplos concretos del resultado anterior.

Ejemplo 9.9. $\mathrm{Aut}(\mathbb{Z}/8) \simeq \mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\} = \langle 3,5\rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

El ejemplo siguiente es bastante más difícil. Vamos a demostrar que si p es un número primo, entonces $\mathrm{Aut}(\mathbb{Z}/p)$ es cíclico y tiene orden $p-1$. Vamos a necesitar el siguiente resultado auxiliar, que resulta ser de interés incluso en otros contextos.

Lema 9.10. *Sean G un grupo finito y abeliano y $n = \max\{|g| : g \in G\}$. Si $x \in G$, entonces $|x|$ divide a n.*

Demostración. Sean $g \in G$ tal que $n = |g|$, $x \in G$ y $m = |x|$. Queremos ver que m divide a n. Supongamos que m no divide a n. Existe entonces algún número primo p tal que $n = p^\alpha n_1$ y $m = p^\beta m_1$, donde $\mathrm{mcd}(p,n_1) = \mathrm{mcd}(p,m_1) = 1$ y $\beta > \alpha$. Sabemos que

$$|g^{p^\alpha}| = \frac{n}{p^\alpha}$$

no es divisible por p y además

$$|x^{\frac{m}{p^\beta}}| = p^\beta.$$

Como n/p^α y p^β son coprimos y G es abeliano,

$$|g^{p^\alpha} x^{\frac{m}{p^\beta}}| = np^{\beta-\alpha} > n,$$

una contradicción a la maximalidad de n. □

Necesitamos otro resultado auxiliar, nuevamente de gran interés no solamente en este contexto.

Lema 9.11. *Sea K un cuerpo. Si $f \in K[X]$ es un polinomio de grado n, entonces f tiene a lo sumo n raíces distintas.*

Demostración. Procederemos por inducción en n. Si $n = 1$, el resultado es trivial. Supongamos entonces que el lema es válido para polinomios de grado $n-1$ y sea $f \in K[X]$. Si f no tiene raíces en K, no hay nada para demostrar. Si, en cambio, α es una raíz de f, entonces

$$f = (X - \alpha)q$$

para un cierto $q \in K[X]$ de grado $n-1$. Si $\beta \neq \alpha$ es otra raíz de f, entonces $0 = f(\beta) = (\beta - \alpha)q(\beta)$ y luego $q(\beta) = 0$, es decir β es raíz de q. Por hipótesis inductiva, el polinomio q tiene a lo sumo $n-1$ raíces distintas. En consecuencia, f tiene a lo sumo n raíces distintas. □

Ahora sí estamos en condiciones de demostrar el siguiente resultado.

Teorema 9.12. *Si p es un número primo, entonces $\mathscr{U}(\mathbb{Z}/p)$ es cíclico de orden $p-1$.*

Demostración. Sabemos que $\mathrm{Aut}(\mathbb{Z}/p)$ es un grupo abeliano. Sea

$$n = \text{máx}\{|g| : g \in \mathscr{U}(\mathbb{Z}/p)\}.$$

Veamos que $n = p-1$. Como $|\mathscr{U}(\mathbb{Z}/p)| = \varphi(p) = p-1$, tenemos $n \leq p-1$. Por otro lado, como gracias al lema anterior sabemos que el polinomio $X^n - 1$ tiene a lo sumo n soluciones, obtenemos $p-1 \leq n$. Luego $n = p-1$. En particular, esto demuestra que $\mathscr{U}(\mathbb{Z}/p)$ es cíclico ya que contiene al menos un elemento de orden $p-1$. □

Veamos otra aplicación importante de los resultados auxiliares que utilizamos para demostrar el teorema anterior. Primero, un lema, que bien podría quedar como ejercicio.

Lema 9.13. *Sea G un grupo abeliano. Si G tiene elementos de órdenes k y l, entonces G tiene un elemento de orden* $\mathrm{mcm}(k,l)$.

Demostración. Sean $g,h \in G$ tales que $|g| = k$ y $|h| = l$. Sea $m = |gh|$. Si k y l son coprimos, el resultado fue demostrado en el corolario 3.11 en la página 19 como aplicación del teorema de Lagrange. Supongamos entonces que $d = \mathrm{mcd}(k,l) > 1$. Escribimos

$$k = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} \cdots p_s^{\alpha_s},$$
$$l = p_1^{\beta_1} \cdots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s},$$

donde los primos $p_1, \ldots, p_s$ son todos distintos, $0 \leq \alpha_j < \beta_j$ para todo $j \in \{1, \ldots, r\}$ y $\alpha_j \geq \beta_j \geq 0$ para todo $j \in \{r+1, \ldots, s\}$. Sean

$$x = g^{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}, \quad y = h^{p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s}}.$$

Como $|x|$ y $|y|$ son coprimos, se concluye que $|xy| = |x||y| = m$. □

Antes de demostrar el teorema, veamos un ejemplo que ilustra qué pasa en el lema anterior.

Ejemplo 9.14. Vamos a calcular el orden de $(8,8) \in (\mathbb{Z}/10) \times (\mathbb{Z}/80)$. Primero observamos que $8 \in \mathbb{Z}/10$ tiene orden $10/\mathrm{mcd}(8,10) = 10/2 = 5$ y que $8 \in \mathbb{Z}/80$ tiene orden $80/\mathrm{mcd}(8,80) = 80/8 = 10$. Tenemos entonces que $g = (8,0)$ tiene orden 5 y $h = (0,8)$ tiene orden 10. La prueba del lema anterior nos dice que el elemento gh^2 tendrá orden $\mathrm{mcm}(5,10) = 10$.

Ahora sí, el teorema.

Teorema 9.15. *Sea K un cuerpo. Si G es un subgrupo finito de $K^\times = K \setminus \{0\}$, entonces G es cíclico. En particular, si K es un cuerpo finito, entonces $K^\times$ es cíclico.*

Demostración. Sea $g \in G$ de orden maximal, digamos $n = |g|$. Vamos a demostrar que $G = \langle g \rangle$. Si eso no fuera cierto, sea $h \in G \setminus \langle g \rangle$. Sabemos que $k = |h| \leq n$. Si $k = n$, entonces los $n+1$ elementos

$$1, g, g^2, \ldots, g^{n-1}, h$$

son raíces distintas del polinomio $X^n - 1$, una contradicción al lema 9.11. Luego $k < n$. Observemos ahora que k divide a n pues, de lo contrario, como G es abeliano, tendríamos en G un elemento de orden $\text{mcm}(k,n) > n$, una contradicción a la maximalidad de n. Como k divide n, tenemos también los $n+1$ elementos

$$1, g^{n/k}, g^{2n/k}, \ldots, g^{(k-1)n/k}$$

son raíces distintas de $X^n - 1$, una contradicción al lema 9.11. □

Terminamos el capítulo con algunos ejercicios sobre grupos de automorfismos.

Ejercicio 9.16. Si G es un grupo tal que $|G| \geq 3$, entonces $|\operatorname{Aut}(G)| \geq 2$.

Ejercicio 9.17. No existe un grupo finito cuyo grupo de automorfismos sea no trivial cíclico y de orden impar.

Ejercicio 9.18. Sea p un número primo. Si G es un p-grupo no abeliano, entonces p^2 divide a $|\operatorname{Aut}(G)|$.

Ejercicio 9.19. Si $G = H \times K$, entonces $\operatorname{Aut}(H)$ es isomorfo a un subgrupo de $\operatorname{Aut}(G)$.

Ejercicio 9.20. Si G tiene centro trivial, entonces $\operatorname{Aut}(G)$ también.

Capítulo 10
Producto semidirecto

Primero comenzaremos con una descripción alternativa del producto directo de dos grupos que vimos en el capítulo 1.

Teorema 10.1. *Sea G un grupo y sean H y K subgrupos normales de G. Si $G = HK$ y $H \cap K = \{1\}$, entonces $G \simeq H \times K$.*

Demostración. Sea $f\colon G \to H \times K$, $f(g) = (h,k)$, donde $h \in H$ y $k \in K$ son únicos tales que $g = hk$. Esto tiene sentido pues si $g \in G$ entonces $g = hk$ para algún $h \in H$ y $k \in K$; si además $g = h_1h_1$ para $h_1 \in H$ y $k_1 \in K$, entonces, como $hk = h_1k_1$, se tiene que $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$ y luego $h = h_1$ y $k = k_1$.

Veamos que si $g = hk$ y $g_1 = h_1k_1$ para $h, h_1 \in H$ y $k, k_1 \in K$, entonces $kh_1 = h_1k$. En efecto, $[k,h_1] = kh_1k^{-1}h_1^{-1} \in H \cap K = \{1\}$ pues la normalidad de H y K implican que $kh_1k^{-1} \in H$ y $h_1k^{-1}h_1^{-1} \in K$.

La observación anterior nos permite demostrar que f es un morfismo de grupos. Si $g = hk$ y $g_1 = h_1k_1$ con $h, h_1 \in H$ y $k, k_1 \in K$, entonces, como $f(g) = (h,k)$ y $f(g_1) = (h_1,k_1)$, tenemos que

$$f(gg_1) = f((hk)(h_1k_1)) = f(h(kh_1)k_1) = f((hh_1)(kk_1)) = (hh_1, kk_1).$$

Queda como ejercicio demostrar que f es biyectiva. □

Un grupo G se dice que admite una factorización exacta mediante los subgrupos H y K si $G = HK$ y adenás $H \cap K = \{1\}$. El teorema anterior puede entonces enunciarse con la siguiente terminología: Si un grupo admite una factorización exacta mediante dos subgrupos normales, entonces es isomorfo al producto directo de esos subgrupos.

Ejemplo 10.2. Sea $G = \mathbb{S}_3$ y sean $H = \langle (123) \rangle \trianglelefteq G$ y $K = \langle (12) \rangle$. Observemos que K no es normal en G, no podemos utilizar el teorema anterior. Tenemos $G = HK$ y $H \cap K = \{\mathrm{id}\}$, pero $H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/2 \not\simeq \mathbb{S}_3$ pues $\mathbb{Z}/3 \times \mathbb{Z}/2$ es un grupo abeliano y $\mathbb{S}_3$ no lo es.

Mencionamos a continuación un corolario sencillo. La demostración quedará como ejercicio.

Corolario 10.3. *Sean A un subgrupo normal de H y B un subgrupo normal de K. Entonces $A \times B$ es un subgrupo normal de $H \times K$ y vale además que*

$$\frac{H \times K}{A \times B} \simeq (H/A) \times (K/B).$$

Bosquejo de la demostración. Sea $\varphi\colon H \times K \to (H/A) \times (K/B)$, $\varphi(h,k) = (hA, kB)$. Dejamos como ejercicio verficar que φ es un isomorfismo de grupos tal que $\ker\varphi = A \times B$. Al aplicar el primer teorema de isomorfismos tendremos entonces el resultado deseado. □

Veremos a continuación qué pasa cuando solamente uno de los factores es normal. Nos encontraremos con un grupo que admite una factorización exacta donde uno de los subgrupos es normal.

Definición 10.4. Sea G un grupo y sean K un subgrupo normal de G y Q un subgrupo de G. Diremos que Q es un **complemento** de K en G si $K \cap Q = \{1\}$ y $G = KQ$.

Ejemplo 10.5. Sea $G = \mathbb{S}_3$ y sea $K = \langle(123)\rangle \trianglelefteq G$. Los subgrupos $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$ son complementos de K en G.

El ejemplo anterior nos muestra que los complementos no son únicos. Sin embargo, sí son únicos salvo isomorfismos pues cualquier complemento será isomorfo a G/K. En efecto, gracias a los teoremas de isomorfismo,

$$G/K = KQ/K \simeq Q/K \cap Q = Q/\{1\} \simeq Q.$$

Definición 10.6. Diremos que un grupo G es un **producto semidirecto** de Q en K si K es normal en G y además K admite un complemento en G isomorfo a Q. La notación que utilizaremos será $G = K \rtimes Q$

Veamos algunas caracterizaciones del producto semidirecto.

Proposición 10.7. *Sea K un subgrupo normal de G. Las siguientes afirmaciones son equivalentes:*

1) K admite un complemento en G.
2) Existe un subgrupo Q de G tal que cada $g \in G$ se escribe unívocamente como $g = xy$ con $x \in K$ e $y \in Q$.
3) Existe un morfismo $s\colon G/K \to G$ tal que $\pi \circ s = \mathrm{id}_{G/K}$, donde $\pi\colon G \to G/K$, $g \mapsto Kg$, es el morfismo canónico.
4) Existe un morfismo $\rho\colon G \to G$ tal que $\ker\rho = K$ y la restricción $\rho|_{\rho(G)}$ es igual a la identidad.

Demostración. Veamos que $(1) \implies (2)$. Si Q es un complemento de K, entonces $G = KQ$ y $K \cap Q = \{1\}$. En particular, si $g \in G$, entonces $g = xy$ para $x \in K$ e $y \in Q$. Y la escritura es única pues si además $g = x_1y_1$ con $x_1 \in K$ e $y_1 \in Q$, entonces $x_1^{-1}x = yy_1^{-1} \in K \cap Q = \{1\}$ y luego $x = x_1$ y también $y = y_1$.

Dejamos como ejercicio verificar que $(2) \implies (1)$.

Veamos que (2) $\implies$ (3). Sea $s\colon G/K \to G$, $s(Kg) = y$ si $g = xy$ con $x \in K$ e $y \in Q$. (Es importante observar que acá, para definir s, nos es conveniente utilizar coclases a derecha.) Veamos que s está bien definida. Para eso, tenemos que ver que si $Kg = Kg_1$, entonces $s(Kg) = s(Kg_1)$. Si escribimos $g = xy$ y $g_1 = x_1y_1$ con $x, x_1 \in K$ e $y, y_1 \in Q$, entonces Como $Kg = Kg_1$, sabemos que $xyy_1^{-1}x_1^{-1} = gg_1^{-1} \in K$, es decir $yy_1^{-1} \in x^{-1}Kx_1 = K$ pues $x, x_1 \in K$. Luego $yy_1^{-1} \in K \cap Q = \{1\}$ y entonces $y = y_1$. Veamos ahora que $\pi \circ s = \mathrm{id}_{G/K}$. Si $g = xy$ con $x \in K$ e $y \in Q$, entonces $(\pi \circ s)(Kg) = \pi(y) = Ky = Kxy = Kg$. Queda como ejercicio demostrar que s es un morfismo de grupos.

Veamos ahora que (3) $\implies$ (4). Sea $\rho = s \circ \pi$. Es claro que ρ es un morfismo, pues es composición de morfismos. Calculamos:

$$\rho(\rho(g)) = \rho((s \circ \pi)(g)) = \rho(s(Kg)) = ((s \circ \pi) \circ s)(Kg) = s(Kg) = \rho(g).$$

Por último, calculamos $\ker \rho$. Si $g \in \ker \rho$, entonces $s(\pi(g)) = \rho(g) = 1$. Luego

$$\pi(g) = \pi(s(\pi(g))) = \pi(1) = 1_{G/K},$$

es decir $g \in \ker \pi = K$. Recíprocamente, si $x \in K$, entonces

$$\rho(x) = \rho(s(Kx)) = \rho(s(K)) = \rho(1) = 1$$

y luego $x \in \ker \rho$.

Por último, demostremos que (4) $\implies$ (1). Afirmamos que $Q = \rho(G)$ es un complemento para K en G. Veamos primero que $K \cap Q = \{1\}$: si $x \in K \cap Q$, entonces $x = \rho(g)$ para algún $g \in G$ y además

$$1 = \rho(x) = \rho(\rho(g)) = \rho(g).$$

Luego $g \in \ker \rho = K$ y entonces $x = 1$. Veamos ahora que $G = KQ$. Para demostrar que $G \subseteq KQ$ observamos que

$$g = (g\rho(g^{-1}))\rho(g)$$

y que $g\rho(g^{-1}) \in K = \ker \rho$ pues $\rho(g\rho(g^{-1})) = \rho(g)\rho(g^{-1}) = 1$. □

Ejemplo 10.8. $\mathbb{S}_n = \mathbb{A}_n \rtimes \mathbb{Z}/2$ pues $Q = \langle (12) \rangle \simeq \mathbb{Z}/2$ es un complemento para el subgrupo normal $\mathbb{A}_n$ de $\mathbb{S}_n$.

La siguiente proposición permite construir productos semidirectos. La demostración quedará como ejercicio.

Proposición 10.9. *Sean K y Q grupos y sea $\theta\colon Q \to \mathrm{Aut}(K)$, $x \mapsto \theta_x$, un morfismo de grupos. El conjunto $K \times Q$ con la operación*

$$(a,x)(b,y) = (a\theta_x(b), xy)$$

es un grupo. Este grupo será denotado por $K \rtimes_\theta Q$.

Bosquejo de la demostración. Dejamos como ejercicio verificar que la operación es asociativa. Hay que verificar además que el elemento neutro de $K \rtimes_\theta Q$ será $(1,1)$ y que el inverso de $(a,x) \in K \rtimes_\theta Q$ será $(\theta_{x^{-1}}(a^{-1}), x^{-1})$. □

El grupo que construimos en la proposición anterior es, de hecho, un producto semidirecto. En efecto, es un producto semidirecto de los subgrupos

$$K \times \{1\} = \{(a,1) : a \in K\} \simeq K, \qquad \{1\} \times Q = \{(1,x) : x \in Q\} \simeq Q$$

de $K \rtimes_\theta Q$. Observar que $K \times \{1\}$ es normal en $K \rtimes_\theta Q$. Es importante remarcar que si identificamos al subgrupo normal $K \rtimes \{1\}$ con K y al subgrupo $\{1\} \rtimes Q$ con Q, podemos escribir

$$\theta_x(a) = xax^{-1}$$

para todo $x \in Q$ y $a \in K$.

Proposición 10.10. *Si G es un producto semidirecto del subgrupo normal K con el subgrupo Q, existe un morfismo de grupos $\theta\colon Q \to \mathrm{Aut}(K)$ tal que $G \simeq K \rtimes_\theta Q$.*

Bosquejo de la demostración. Para $x \in Q$ sea $\theta_x\colon K \to K$, $\theta_x(a) = xax^{-1}$. Ya vimos que $\theta_x \in \mathrm{Aut}(K)$ y que $Q \to \mathrm{Aut}(K)$, $x \mapsto \theta_x$ es un morfismo de grupos. Queda verificar que la función $K \rtimes_\theta Q \to G$, $(a,x) \mapsto ax$, es un morfismo biyectivo de grupos. □

Veamos algunos ejemplos.

Ejemplo 10.11. Sean $N \simeq \mathbb{Z}/n$ y $H \simeq \mathbb{Z}/2 = \{0,1\}$. La función $\theta\colon H \to \mathrm{Aut}(N)$, $1 \mapsto (x \mapsto x^{-1})$, es un morfismo de grupos. Sea $G = N \rtimes_\theta H$. Entonces $G \simeq \mathbb{D}_n$, el grupo diedral de orden $2n$.

Recordemos que

$$\mathbb{D}_n = \langle r, s : r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Supongamos que $N = \langle x \rangle$ y que $H = \langle y \rangle$. Entonces $|(x,1)| = n$ y $|(1,y)| = 2$. Además

$$\begin{aligned}(1,y)(x,1)(1,y)^{-1} &= (\varphi_y(x),y)(1,y) = (\varphi_y(x),y^2)\\ &= (\varphi_y(x),1) = (x^{-1},1) = (x,1)^{-1}.\end{aligned}$$

Si $u = (x,1)$ y $v = (1,y)$, entonces $u^n = v^2 = (1,1)$ y además $vuv^{-1} = u^{-1}$. Esto significa que existe un morfismo de grupos $\mathbb{D}_n \to G$ que además es sobreyectivo (pues G está generado por u y v). Además $|G| = |N||H| = 2n$, luego G también tiene orden $2n$ y en consecuencia $G \simeq \mathbb{D}_n$.

Ejemplo 10.12. Sea $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, que sabemos es normal en $\mathbb{A}_4$ y sea $H = \langle (123) \rangle \simeq \mathbb{Z}/3$. Como $K \cap H$ es un subgrupo de H y K y además los órdenes de K y H son coprimos, $H \cap K = \{\mathrm{id}\}$. Luego $\mathbb{A}_4 = K \rtimes H$.

Ejemplo 10.13. Tal como en el ejercicio anterior, sea K el subgrupo de Klein de $\mathbb{S}_4$. Sea $H = \{\sigma \in \mathbb{S}_4 : \sigma(4) = 4\}$, que es un subgrupo de $\mathbb{S}_4$ isomorfo a $\mathbb{S}_3$. Simplemente al observar los elementos vemos que $H \cap K = \{\mathrm{id}\}$ y luego $\mathbb{S}_4 = K \rtimes H$.

Ejemplo 10.14. Si $n \geq 5$, $\mathbb{A}_n$ no es un producto semidirecto de subgrupos propios (pues $\mathbb{A}_n$ es simple para todo $n \geq 5$).

Ejemplo 10.15. Sea $K \simeq \mathbb{Z}/3$ y sea $Q = \mathbb{Z}/4$. Como $\mathrm{Hom}(Q, \mathrm{Aut}(K)) = \{1, \tau\}$, donde

$$\tau \colon \mathbb{Z}/4 \to \mathrm{Aut}(\mathbb{Z}/3) = \{\mathrm{id}, \rho\} \simeq \mathbb{Z}/2, \quad 1 \mapsto \rho,$$

el producto semidirecto $T = K \rtimes_t Q$ es un grupo no abeliano de orden 12. Además $T \not\simeq \mathbb{A}_4$ pues, por ejemplo, $|(2,2)| = 6$ y sabemos que en $\mathbb{A}_4$ no existen elementos de orden seis.

Capítulo 11
Acciones

Definición 11.1. Sean G un grupo y X un conjunto. Una acción (a izquierda) de G en X es una función $G \times X \to X$, $(g,x) \mapsto g \cdot x$, tal que

1) $1 \cdot x = x$ para todo $x \in X$, y
2) $g \cdot (h \cdot x) = (gh) \cdot x$ para todo $g,h\, nG$ y $x \in X$.

Cuando un grupo G actúa en un conjunto X, se dice también que X es un G-conjunto.

Ejemplo 11.2. Todo grupo G actúa en G trivialmente: $g \cdot h = h$ para todo $g,h \in G$.

Ejemplo 11.3. Todo grupo G actúa en G por multplicación a izquierda, es decir $g \cdot h = gh$ para todo $g,h \in G$.

Ejemplo 11.4. Todo grupo G actúa en G por $g \cdot h = hg^{-1}$ para todo $g,h \in G$.

Ejemplo 11.5. Si N es un subgrupo normal de G, entonces G actúa en N por conjugación, es decir $g \cdot x = gxg^{-1}$ para todo $g \in G$ y $x \in N$. En particular, todo grupo G actúa en G por conjugación.

Ejemplo 11.6. Sea G un grupo y sea H un subgrupo de G. Entonces G actúa en el conjunto de coclases G/H por multiplicación a izquierda, es decir $g \cdot (xH) = (gx)H$ para todo $g,x \in G$.

Toda acción a izquierda de G en X se corresponde biyectivamente con un morfismo $\rho \colon G \to \mathbb{S}_X$. La correspondencia está dada por la fórmula

$$\rho(g)(x) = g \cdot x, \quad g \in G, x \in X.$$

Para simplificar, utilizaremos la notación $\rho_g = \rho(g)$.

Como ejemplo veamos que si $G \times X \to X$, $(g,x) \mapsto x$, es una acción de G en X, entonces cada $\rho_g \colon X \to X$ es una función biyectiva con inversa $(\rho_g)^{-1} = \rho_{g^{-1}}$. Además ρ es un morfismo de grupos pues

$$\rho(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \rho_g(h \cdot x) = \rho_g(\rho_h(x))$$

para todo $g,h \in G$ y todo $x \in X$.

Ejemplo 11.7. Sea $G = \mathbb{S}_3$ y sea $H = \langle (123) \rangle = \{\mathrm{id}, (123), (132)\}$. Si hacemos actuar al grupo G en el conjunto $X = G/H = \{H, (12)H\}$ por multiplicación a izquierda, y escribimos $x_1 = H$ y $x_2 = (12)H$, tenemos entonces

$$(12) \cdot x_1 = x_2, \qquad (12) \cdot x_2 = x_1, \qquad (123) \cdot x_1 = x_1, \qquad (123) \cdot x_2 = x_2.$$

Como $G = \langle (12), (123) \rangle$, queda definido el morfismo $\rho \colon G \to \mathbb{S}_X \simeq \mathbb{S}_2$ de la siguiente forma: $(12) \mapsto (12)$, $(123) \mapsto \mathrm{id}$.

Ejemplo 11.8. Sea $G = \mathbb{S}_3$ y sea $H = \langle (12) \rangle = \{\mathrm{id}, (12)\}$. Si hacemos actuar a G en $X = G/H = \{H, (123)H, (132)H\}$ por multiplicación a izquierda y escribimos $x_1 = H$, $x_2 = (123)H$ y $x_3 = (132)H$, entonces

$$\begin{aligned} (12) \cdot x_1 &= x_1, & (12) \cdot x_2 &= x_3, & (12) \cdot x_3 &= x_2, \\ (123) \cdot x_1 &= x_2, & (123) \cdot x_2 &= x_3, & (123) \cdot x_3 &= x_1. \end{aligned}$$

Como $G = \langle (12), (123) \rangle$, queda definido el morfismo $\rho \colon G \to \mathbb{S}_X \simeq \mathbb{S}_3$ de la siguiente forma: $(12) \mapsto (23)$, $(123) \mapsto (123)$.

Ejemplo 11.9. Sea $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ y sea $N = \{1, -1, i, -i\}$. Como N es normal en G, el grupo G actúa por conjugación en $X = N$. Si $x_1 = 1$, $x_2 = -1$, $x_3 = i$ y $x_4 = -i$, entonces $i \cdot x = x$ para todo $x \in N$ y además

$$j \cdot x_1 = x_1, \qquad j \cdot x_2 = x_2, \qquad j \cdot x_3 = x_4, \qquad j \cdot x_4 = x_3.$$

Como $G = \langle i, j \rangle$, el morfismo $\rho \colon G \to \mathbb{S}_X \simeq \mathbb{S}_4$ queda determinado por $\rho_i = \mathrm{id}$ y $\rho_j = (34)$.

El ejemplo siguiente es particularmente importante, ya que suele generar confusión.

Ejemplo 11.10. El grupo $\mathbb{S}_n$ actúa en $\mathbb{R}^n$ por

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

Es muy importante remarcar que debe usarse σ^{-1} en la definición y no σ, ya que lo que queremos es permutar los elementos de la base canónica de $\mathbb{R}^3$.

Como ejemplo, veamos que la operación $\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$ no define una acción de $\mathbb{S}_3$ en $\mathbb{R}^3$. Si $\sigma = (12)$ y $\tau = (23)$, entonces $\sigma\tau = (123)$. Como

$$\begin{aligned} &(123) \cdot (5,6,7) = (6,7,5), \\ &(12) \cdot ((23) \cdot (5,6,7)) = (1,2) \cdot (5,7,6) = (7,5,6), \end{aligned}$$

no tenemos una acción. En general, no se tiene una acción porque si calculamos

$$\sigma \cdot (\tau \cdot (x_1, \ldots, x_n)) = \sigma \cdot (x_{\tau(1)}, \ldots, x_{\tau(n)})$$

y para cada $i \in \{1,\dots,n\}$ hacemos $y_i = x_{\tau(i)}$, entonces

$$\sigma \cdot (\tau \cdot (x_1,\dots,x_n)) = \sigma \cdot (y_1,\dots,y_n) = (y_{\sigma(1)},\dots,y_{\sigma(n)}) = (x_{\tau\sigma(1)},\dots,x_{\tau\sigma(n)}),$$

aunque σ y τ no conmuten.

Veamos que se tiene una acción si usamos el inverso. Para cada $j \in \{1,\dots,n\}$ sea $y_j = x_{\tau(j)}$, es decir

$$(y_1,y_2,\dots,y_n) = \tau \cdot (x_1,x_2,\cdots,x_n) = (x_{\tau^{-1}(1)},x_{\tau^{-1}(2)},\dots,x_{\tau^{-1}(n)}).$$

Calculamos entonces

$$\begin{aligned}
\sigma \cdot (\tau \cdot (x_1,x_2,\dots,x_n)) &= \sigma \cdot (y_1,y_2,\dots,y_n) \\
&= \left(y_{\sigma^{-1}(1)},y_{\sigma^{-1}(2)},\cdots,y_{\sigma^{-1}(n)}\right) \\
&= \left(x_{\tau^{-1}(\sigma^{-1}(1))},x_{\tau^{-1}(\sigma^{-1}(2))},\dots,x_{\tau^{-1}(\sigma^{-1}(n))}\right) \\
&= \left(x_{(\sigma\tau)^{-1}(1))},x_{(\sigma\tau)^{-1}(2))},\dots,x_{(\sigma\tau)^{-1}(n))}\right).
\end{aligned}$$

El ejemplo anterior y el siguiente están relacionados.

Ejemplo 11.11. El grupo simétrico $\mathbb{S}_n$ actúa en el conjunto de polinomios de n variables $X_1,\dots,X_n$ permutando las variables. Por ejemplo, en el caso de tres variables, si $\sigma = (123)$ y $f = X_2X_3 - X_1 + 5X_2X_3^2X_1$, entonces $\sigma \cdot f = X_2^2X_3 - X_1 + 5X_2X_3^2X_1$.

Al restringir la acción, vemos que $\mathbb{S}_n$ actúa en el conjunto

$$\{\lambda_1X_1 + \cdots \lambda_nX_n : \lambda_1,\dots,\lambda_n \in \mathbb{R}\}.$$

Podemos escribir entonces

$$\sigma \cdot (\lambda_1X_1 + \cdots + \lambda_nX_n) = (\lambda_1X_{\sigma(1)} + \cdots + \lambda_nX_{\sigma(n)}) = (\lambda_{\sigma(1)}X_1 + \cdots + \lambda_{\sigma(n)}X_n)$$

y vemos cuál es la relación que tiene esta acción con la que vimos en el ejemplo anterior.

Es importante poder calcular el núcleo de la acción.

Ejemplo 11.12. Sea G un grupo y sea H un subgrupo de G. Entonces G actúa en el conjunto de coclases G/H por multiplicación a izquierda, es decir $g \cdot (xH) = (gx)H$ para todo $g,x \in G$. Sea $\rho\colon G \to \mathbb{S}_{G/H}$ el morfismo inducido por la acción.

Veamos que $\ker\rho = \cap_{x\in G}xHx^{-1}$. Demostremos primero $\supseteq$. Si $g \in xHx^{-1}$ para todo $x \in G$, entonces fijado $x \in G$,

$$\rho(g)(xH) = g \cdot (xH) = (gx)H = (xhx^{-1})xH = (xh)H = xH$$

pues $g = xhx^{-1}$ para algún $h \in H$. Luego $\rho(g) = \mathrm{id}$ y entonces $g \in \ker\rho$. Veamos ahora que vale $\subseteq$. Si $g \in \ker\rho$, entonces $\rho(g) = \mathrm{id}$, es decir que, para todo $x \in G$,

$$\rho(g)(xH) = xH \iff (gx)H = xH \iff x^{-1}gx \in H \iff g \in xHx^{-1}.$$

Dejamos como ejercicio demostrar que $\ker\rho$ es el mayor subgrupo normal de G contenido en H.

Podemos utilizar el ejemplo anterior para dar una aplicación. Daremos una tercera demostración del corolario 5.23 en la página 32.

Sea p el menor número primo que divide al orden de un grupo finito G y sea H un subgrupo de G índice p. Entonces H es normal en G.

Hacemos actuar a G en G/H por multiplicación a izquierda y tenemos un morfismo $\rho\colon G \to \mathbb{S}_p$ que tiene núcleo

$$K = \ker\rho = \bigcap_{x\in G} xHx^{-1} \subseteq H.$$

Por el primer teorema de isomorfismos, $G/K \simeq \rho(G) \lesssim \mathbb{S}_p$ (aquí la notación nos dice que $\rho(G)$ es isomorfo a un subgrupo de $\mathbb{S}_p$). Luego $|G/K|$ divide a $p!$. Sea $m = (H : K)$. Por el teorema de Lagrange,

$$(G : K) = (G : H)(H : K) = pm$$

y luego pm divide a $p!$, lo que implica que m divide a $(p-1)!$. Si q es un primo que divide a m, entnoces $q \geq p$, por la minimalidad de p. Además los factores primos de $(p-1)!$ son todos $< p$. En consecuencia, $m = 1$ y luego $H = K$.

Una acción de un grupo en un conjunto permite definir una relación de equivalencia. Si G actúa en X, sobre el conjunto X definimos $x \sim y$ si y sólo si existe $g \in G$ tal que $g \cdot x = y$.

Definición 11.13. Sea G un grupo que actúa en un conjunto X. Si $x \in X$, la órbita de x es el conjunto

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

Las órbitas de la acción de G en X son entonces las clases de equivalencia de la relación inducida por la acción. En particular, dos órbitas cualesquiera serán disjuntas o iguales. Además X podrá descomponerse como unión disjunta de órbitas.

Definición 11.14. Sea G un grupo que actúa en un conjunto X. Si $x \in X$, el estabilizador de x en G es el subgrupo

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

Queda como ejercicio demostrar que el estabilizador es un subgrupo.

El ejemplo anterior es un ejemplo típico de **acción transitiva**, esto significa que dados $xH, yH \in G/H$, existe $g \in G$ tal que $(gx)H = yH$ (basta tomar $g = yx^{-1}$). Veamos la definición general.

Definición 11.15. Diremos que una acción de un grupo G en un conjunto X es **transitiva** si dados $x, y \in X$ existe $g \in G$ tal que $g \cdot x = y$.

Ejemplo 11.16. Por evaluación, el grupo simétrico $\mathbb{S}_n$ actúa transitivamente en el conjunto $\{1,\dots,n\}$.

En la definición de acción transitiva, no hay condiciones sobre la cantidad de g tales que $g\cdot x = y$.

Definición 11.17. Diremos que una acción de un grupo G en un conjunto X es **fiel** si $\{g \in G : g\cdot x = x \text{ para todo } x \in X\} = \{1\}$.

La definición anterior equivale a pedir que el morfismo inducido por la acción sea inyectivo.

Teorema 11.18 (principio fundamental del conteo). *Sea G un grupo finito que actúa en un conjunto finito X. Si $x \in X$, entonces $|G\cdot x| = (G : G_x)$.*

Demostración. Sea $\varphi\colon G/G_x \to G\cdot x$, $gG_x \mapsto g\cdot x$. La función φ está bien definida pues

$$gG_x = hG_x \implies h^{-1}g \in G_x \implies h^{-1}g\cdot x = x \implies g\cdot x = h\cdot x.$$

La función φ es inyectiva pues

$$\varphi(gG_x) = \varphi(hG_x) \implies g\cdot x = h\cdot x \implies h^{-1}g \in G_x \implies gG_x = hG_x.$$

La función φ es trivialmente sobreyectiva. En consecuencia, $|G/G_x| = |G\cdot x|$. □

Si G es un grupo y X e Y son G-conjuntos, diremos que una función $\varphi\colon X \to Y$ es un **morfismo** de G-conjuntos si $\varphi(g\cdot x) = g\cdot\varphi(x)$ para todo $g \in G$ y $x \in X$. La biyección φ que construimos en la demostración del teorema anterior es en realidad un morfismo de G-conjuntos, donde la acción de G en G/G_x es por multiplicación a izquierda, pues

$$\varphi(g\cdot hG_x) = \varphi((gh)G_x) = (gh)\cdot x = g\cdot(h\cdot x) = g\cdot\varphi(hG_x).$$

Luego $G\cdot x \simeq G/G_x$ como G-conjuntos.

Ejemplo 11.19. Si G actúa en G por conjugación, es decir $g\cdot x = gxg^{-1}$, las órbitas de esta acción son las **clases de conjugación** del grupo, es decir los conjuntos de la forma

$$G\cdot x = \{gxg^{-1} : g \in G\}.$$

Los estabilizadores son los centralizadores pues

$$G_x = \{g \in G : g\cdot x = x\} = \{g \in G : gxg^{-1} = x\} = C_G(x).$$

Luego $|G\cdot x| = (G : C_G(x))$.

Ejemplo 11.20. Sea H un subgrupo de G y sea X el conjunto de subconjuntos de G. Hacemos actuar a G en X por conjugación, es decir si $S \in X$, entonces $g\cdot S = gSg^{-1}$. La órbita de H es entonces

$$G \cdot H = \{g \cdot H : g \in G\} = \{gHg^{-1} : g \in G\},$$

el conjunto de conjugados de H. El estabilizador de H en G es

$$G_H = \{g \in G : g \cdot H = H\} = \{g \in G : gHg^{-1} = H\} = N_G(H),$$

el normalizador de H en G. Luego H tiene exactamente $(G : N_G(H))$ conjugados en G. Observemos que, en particular, la cantidad de conjugados de H en un grupo finito G es un divisor del orden de G.

Como aplicación daremos una demostración de la fórmula que vimos en el teorema 6.6, que permite calcular el tamaño del conjunto HK si H y K son subgrupos de un grupo G.

Ejemplo 11.21. Si G es un grupo y H y K son subgrupos de G, entonces el grupo $L = H \times K$ actúa en $X = HK$ por

$$(h,k) \cdot x = hxk^{-1}, \quad x \in X, h \in H, k \in K.$$

Observemos que $1 \in HK$ y que la acción de K en X tiene una única órbita, pues $(h,k^{-1}) \cdot 1 = hk$. Como además

$$L_1 = \{(h,k) \in H \times K : (h,k) \cdot 1 = 1\} = \{(h,k) \in H \times K : h = k\},$$

entonces $|L_1| = |H \cap K|$, pues L_1 y $H \cap K$ están en biyección. Luego el principio teorema fundamental del conteo nos dice que

$$|HK| = (L : L_1) = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}.$$

El ejemplo anterior puede generalizarse, lo que nos da una descomposición de un grupo como unión disjunta de **coclases dobles**. Veremos más adelante demostraciones alternativas de los teoremas de Sylow basadas en coclases dobles.

Ejemplo 11.22. Sea G un grupo y sean H y K subgrupos de G. Hacemos que el grupo $L = H \times K$ actúe en G por

$$(h,k) \cdot g = hgk^{-1}.$$

Las órbitas son los conjuntos de la forma

$$HgK = \{hgk : h \in H, k \in K\},$$

estos conjuntos se llaman (H,K)-coclases dobles. En particular, dos (H,K)-coclases dobles son disjuntas o iguales. Más aún, G se descompone como unión disjunta

$$G = \bigcup_{i \in I} Hg_iK,$$

para algún conjunto I, es decir G es unión disjunta de (H,K)-coclases dobles. Calculamos ahora

$$L_g = \{(h,k) \in H \times K : hgk^{-1} = g\} = \{(h, g^{-1}hg) \in H \times K\}$$

y vemos que $|L_g| = |H \cap gKg^{-1}|$, pues los conjuntos L_g y $H \cap gKg^{-1}$ están en biyección. Luego, gracias al principio fundamental del conteo,

$$|HgK| = (L : L_g) = \frac{|H \times K|}{|H \cap gKg^{-1}|} = \frac{|H||K|}{|H \cap gKg^{-1}|}.$$

Veamos otra aplicación. Calculemos ahora el orden del grupo $\mathbf{GL}_n(p)$ para $n \in \mathbb{N}$ y p un número primo. El mismo argumento nos permite calcular $\mathbf{GL}_n(q)$ para q una potencia del primo p.

Ejemplo 11.23. Sea $K = \mathbb{Z}/p$. Vamos a demostrar que

$$|\mathbf{GL}_n(p)| = (p^n - 1)p^{n-1}|\mathbf{GL}_{n-1}(p)|,$$

lo que implica que

$$|\mathbf{GL}_n(p)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

La fórmula es cierta en el caso $n = 1$ y por lo tanto también cuando $n = 2$. Supongamos entonces que vale para $n - 1 \geq 1$. El grupo $G = \mathbf{GL}_n(p)$ actúa en K^n por multiplicación a izquierda y hay dos órbitas, es decir

$$X = \{0\} \cup (K^n \setminus \{0\}),$$

pues si $v, w \in K^n \setminus \{0\}$, entonces existe $g \in G$ tal que $gv = w$. El principio fundamental del conteo nos dice que

$$p^{n+1} - 1 = |K^{n+1} \setminus \{0\}| = (G : G_{e_1}),$$

donde $e_1 = (1,0,\ldots,0)^T$. Si $g = (g_{ij}) \in G$ es tal que $ge_1 = e_1$, entonces

$$g = \begin{pmatrix} 1 & g_{12} & \cdots & g_{1n} \\ 0 & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & g_{n1} & \cdots & g_{nn} \end{pmatrix}.$$

Luego $|G_{e_1}| = p^{n-1}|\mathbf{GL}_{n-1}(p)|$, ya que la submatriz $(g_{ij})_{2 \leq i,j \leq n}$ es inversible y los g_{1j} pueden elegirse arbitrariamente para todo $j \in \{2,\ldots,n\}$. Luego

$$p^n - 1 = \frac{|G|}{|G_{e_1}|} = \frac{|\mathbf{GL}_n(p)|}{p^{n-1}|\mathbf{GL}_{n-1}(p)|},$$

que es esencialmente la fórmula que queríamos demostrar.

Capítulo 12
El teorema de Cauchy

Si X es un G-conjunto finito, sabemos que X puede descomponerse como unión disjunta de órbitas. Sea

$$\mathrm{Fix}(X) = \{x \in X : g \cdot x = x \text{ para todo } g \in G\}$$

el **conjunto de puntos fijos** de X. Al tomar cardinal en la descomopsición que tenemos del conjunto X, agrupar las órbitas que tienen únicamente un elemento y utilizar el principio fundamental del conteo para las órbitas con ≥ 2 elementos, obtenemos

$$|X| = |\mathrm{Fix}(X)| + \sum_{i=1}^{k} |G \cdot x_i| = |\mathrm{Fix}(X)| + \sum_{i=1}^{k} (G : G_{x_i}), \tag{12.1}$$

donde los x_j son los representantes de las órbitas que tienen ≥ 2 elementos. La fórmula (12.1) es muy útil y se conoce como **ecuación de clases**.

Ejemplo 12.1. Si un grupo finito G actúa en G por conjugación, un cálculo directo nos muestra que $\mathrm{Fix}(G) = Z(G)$ y luego la ecuación de clases queda

$$|G| = |Z(G)| + \sum_{i=1}^{k} (G : C_G(x_i)),$$

para ciertos $x_1, \ldots, x_k \in G$ tales que $(G : C_G(x_i)) \geq 2$ para todo $i \in \{1, \ldots, k\}$.

Definición 12.2. Sea p un número primo. Diremos que G es un p-grupo si $|G| = p^m$ para algún $m \in \mathbb{N}_0$.

Teorema 12.3. *Sea p un número primo y sea G un p-grupo. Si $\{1\} \neq N \trianglelefteq G$, entonces $N \cap Z(G) \neq \{1\}$.*

Demostración. Como N es normal en G, G actúa en N por conjugación. El teorema fundamental del conteo nos dice que cada órbita de la acción es una potencia del primo p. Escribamos

$$N = \underbrace{\mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k}_{\text{órbitas de un elemento}} \cup \underbrace{\mathcal{O}_{k+1} \cup \cdots \cup \mathcal{O}_m}_{\text{órbitas de tamaño} > 1},$$

Como $N \cap Z(G) = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k$, los números $k = |N \cap Z(G)|$ y $|N \setminus (N \cap Z(G))|$ son divisibles por el primo p. Luego $|N| \equiv |N \cap Z(G)|$ mód p. Como $1 \in N \cap Z(G)$, entonces $|N \cap Z(G)| > 1$. En particular, $N \cap Z(G) \neq \{1\}$. □

Corolario 12.4. *Sea p un número primo. Si G es un p-grupo, entonces $Z(G) \neq \{1\}$.*

Demostración. Tomar $N = G$ en el teorema anterior. □

Corolario 12.5. *Sea p un número primo. Si $|G| = p^2$, entonces G es abeliano.*

Demostración. Por el teorema de lagrange, $|Z(G)| \in \{1, p, p^2\}$. Además, como G es un p-grupo, $Z(G) \neq \{1\}$. Si $|Z(G)| = p$, entonces $Z(G)$ es cíclico y luego G es abeliano (es un ejercicio que hicimos en la página...), una contradicción. Luego $|Z(G)| = p^2$ y en consecuencia $G = Z(G)$. □

Teorema 12.6 (Cauchy). *Si G es finito y p es un primo que divide al orden de G, entonces existe $g \in G$ de orden p.*

Demostración. Sea $C = \mathbb{Z}/p$ y sea

$$X = \{(x_1, \ldots, x_p) \in G \times \cdots \times G : x_1 \cdots x_p = 1\}.$$

Entonces C actúa en X por $k \cdot (x_1, \ldots, x_p) = (x_{k+1}, \ldots, x_{k+p})$, donde los índices se toman módulo p. Para ver que esto es realmente una acción alcanza con observar que

$$x_{i_1} \cdots x_{i_p} = 1 \implies (x_{i_1}^{-1} x_{i_1}) x_{i_2} \cdots x_{i_p} = x_{i_1}^{-1} \implies x_{i_2} \cdots x_{i_p} x_{i_1} = 1.$$

Una vez que $x_1, \ldots, x_{p-1}$ están fijos, $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$ es la única posibilidad para x_p. Luego $|X| = |G|^{p-1}$. Cada C-órbita tiene 1 o p elementos pues $|C| = p$. Escribamos

$$X = \underbrace{\mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k}_{\text{órbitas de un elemento}} \cup \underbrace{\mathcal{O}_{k+1} \cup \cdots \cup \mathcal{O}_m}_{\text{órbitas de tamaño } p}.$$

Entonces $0 \equiv |G|^{p-1} = |X| \equiv k$ mód p, es decir p divide a k. Como además $(1, 1, \ldots, 1) \in X$, $k \geq 1$. Luego $p \leq k$. En particular, existe $x \in G \setminus \{1\}$ tal que $(x, x, \ldots, x) \in X$. Luego $|x| = p$. □

Corolario 12.7. *Sea p un primo y G un grupo finito. Entonces G es un p-grupo si y sólo si todo elemento de G tiene orden una potencia de p.*

Demostración. Si G es un p-grupo, entonces todo elemento tiene orden una potencia de p por el teorema de Lagrange. Recíprocamente, si q es un primo que divide al orden de G, el teorema de Cauchy nos dice que existe $g \in G$ de orden q. Luego $q = p$. □

Corolario 12.8. *Si p es un primo impar y G es un grupo de orden $2p$, entonces $G \simeq \mathbb{Z}/2p$ o bien $G \simeq \mathbb{D}_p$.*

Demostración. Por el teorema de Cauchy sabemos que existen $r,s \in G$ tales que $|r| = p$ y $|s| = 2$. Sea $H = \langle r \rangle$. Entonces $(G : H) = 2$ y luego $H \trianglelefteq G$. Escribimos $G = H \cup Hs$ (unión disjunta) pues $s \notin H$. En particular,

$$G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}.$$

Como $srs^{-1} \in H$, entonces $srs^{-1} = r^k$ para algún $k \in \{0, 1, \ldots, p-1\}$. Como $s^2 = 1$,

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = sr^k s^{-1} = r^{k^2}.$$

Luego $k^2 \equiv 1$ mód p y entonces $k \equiv 1$ mód p o bien $k \equiv -1$ mód p. Si $k \equiv -1$ mód p, entonces $srs^{-1} = r^{-1}$ y luego $G \simeq \mathbb{D}_p$. Si $k \equiv 1$ mód p, entonces $rs = sr$ y luego, como G es abeliano, $G \simeq \mathbb{Z}/2p$. □

Teorema 12.9. *Un grupo de orden p^m tiene un subgrupo normal de orden p^n para todo $n \leq m$.*

Demostración. Procederemos por inducción en m. El caso $m = 1$ es trivial. Supongamos entonces que el resultado vale para los grupos de orden p^m y sea G un grupo de orden p^{m+1}. Queremos ver que si $n \leq m$, entonces G contiene un subgrupo normal de orden p^n. Como $Z(G) \neq \{1\}$, existe $g \in Z(G) \setminus \{1\}$ de orden p. Sea $N = \langle g \rangle \trianglelefteq G$. El grupo G/N tiene orden p^m y entonces, por la hipótesis inductiva, existe un subgrupo normal Y de G/N de orden p^n. El teorema de la correspondencia nos permite afirmar entonces que G contiene un subgrupo normal K de G que contiene a N, es decir $N \leq K \leq G$. En efecto, $Y = \pi(K)$ y además $(G : K) = (\pi(G) : \pi(K)) = p^{m-n}$. En consecuencia, $|K| = p^n$. □

Capítulo 13
Los teoremas de Sylow

Definición 13.1. Sea G un grupo de orden $p^\alpha m$, donde p es un primo coprimo con m. Un subgrupo S de G es un p-subgrupo de Sylow de G si $|S| = p^\alpha$.

Observemos que un subgrupo S de G será entonces un p-subgrupo de Sylow de G si y sólo si S es un p-grupo y además p no divide a $(G : S)$.

Ejemplos 13.2.

1) Si p no divide a $|G|$, entonces $\{1\}$ es un p-subgrupo de Sylow de G.
2) Si G es un p-grupo, entonces G es un p-subgrupo de Sylow de G.

Ejemplo 13.3. Sea $G = \mathbb{S}_3$. Entonces $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$ son los 2-subgrupos de Sylow de G. Además $\langle(123)\rangle$ es el único 3-subgrupo de Sylow de G.

Ejemplo 13.4. Si $G = \mathbb{S}_4$, el subgrupo $\langle(1234),(13)\rangle$ es un 2-subgrupo de Sylow de G y el subgrupo $\langle(123)\rangle$ es un 3-subgrupo de Sylow de G.

Ejemplo 13.5. Si $G = \mathbb{Z}/18$, el subgrupo $\langle 2\rangle = \{0,2,4,6,8,10,12,14,16\}$ es el único 3-subgrupo de Sylow de G y el subgrupo $\langle 9\rangle = \{0,9\}$ es el único 2-subgrupo de Sylow de G.

Ejemplo 13.6. Sea p un número primo y sea $G = \mathbf{GL}_n(p)$. Como

$$\begin{aligned} |\mathbf{GL}_n(p)| &= (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) \\ &= p^{1+2+\cdots+n}(p^n-1)(p^{n-1}-1)\cdots(p-1), \end{aligned}$$

podemos escribir $|\mathbf{GL}_n(p)| = p^\alpha m$, donde $\alpha = 1+2+\cdots+n$ y m es un entero no divisible por p. El subgrupo de matrices de la forma

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

es decir el conjunto de matrices (g_{ij}) con

$$g_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i > j, \end{cases}$$

tiene orden p^α y luego es un p-subgrupo de Sylow de $\mathbf{GL}_n(p)$.

El primer objetivo del capítulo es demostrar el primer teorema de Sylow, que garantiza la existencia de p-subgrupos de Sylow para todo primo p. Antes de ir al teorema, necesitamos un resultado auxiliar.

Lema 13.7. *Si p es un primo, $\alpha \geq 0$ y $m \geq 1$, entonces*

$$\binom{p^\alpha m}{p^\alpha} \equiv m \text{ mód } p.$$

Demostración. Por el teorema del binomio,

$$(1+X)^p = \sum_{j=0}^{p} \binom{p}{j} X^{p-j} \equiv 1 + X^p \text{ mód } p,$$

ya que $\binom{p}{j}$ es divisible por p para todo $j \in \{1, \ldots, p-1\}$. Por inducción, demostramos ahora que

$$(1+X)^{p^j} \equiv 1 + X^{p^j} \text{ mód } p$$

vale para todo j. Luego

$$(1+X)^{p^\alpha m} \equiv (1+X^{p^\alpha})^m \text{ mód } p.$$

Al comparar el coeficiente de X^{p^α} en ambos miembros de la fórmula anterior, obtenemos el resultado que queríamos demostrar. □

Teorema 13.8 (primer teorema de Sylow). *Si G es un grupo finito y p es un número primo, existe un p-subgrupo de Sylow de G.*

Demostración. Escribimos $|G| = p^\alpha m$, con $\text{mcd}(p,m) = 1$ y $\alpha \geq 1$. Sea

$$X = \{S : S \subseteq G \text{ subconjunto de tamaño } p^\alpha\}.$$

Hacemos actuar a G en X por multiplicación a izquierda, pues $|g \cdot S| = |gS| = |S|$ para todo $g \in G$ y todo $S \in X$. Descomponemos a X en G-órbitas y observamos que, gracias al lema anterior,

$$|X| = \binom{p^\alpha m}{p^\alpha} \equiv m \not\equiv 0 \text{ mód } p,$$

lo que implica que existe una órbita $\mathscr{O}$ de tamaño no divisible por p. Si $S \in \mathscr{O}$, sea G_S el estabilizador de S en G. Como $|\mathscr{O}| = (G : G_S)$ y $|\mathscr{O}|$ no es divisible por p,

tenemos que p^α divide a $|G_S|$. En particular, $p^\alpha \leq |G_S|$. Si $g \in G_S$, entonces $gS = S$. Si $x \in S$, entonces $G_S x \subseteq S$. Luego

$$|G_S| = |G_S x| \leq |S| = p^\alpha$$

pues $S \in X$. En conclusión G_S es un p-subgrupo de Sylow de G. □

Nos resultará conveniente introducir la siguiente notación. Si G es un grupo finito y p es un número primo que divide al orden de G, escribiremos

$$\mathrm{Syl}_p(G) = \{p\text{-subgrupos de Sylow de } G\}.$$

Veamos una demostración alternativa del primer teorema de Sylow que utiliza coclases dobles. Primero demostraremos un resultado auxiliar. Si $P \in \mathrm{Syl}_p(G)$ y $H \leq G$, entonces existe un $g \in G$ tal que $H \cap gPg^{-1} \in \mathrm{Syl}_p(H)$. En efecto, supongamos que $|H| = p^\beta t$ con p coprimo con t. Si descomponemos a G en (H,P)-coclases dobles,

$$|G| = \sum_{i=1}^{k} \frac{|H||P|}{|H \cap x_i P x_i^{-1}|}.$$

Al simplificar $|P| = p^\alpha$, tenemos que $m = \sum_{i=1}^{k} (H : H \cap x_i P x_i^{-1})$, lo que nos dice que existe $i \in \{1,\ldots,k\}$ tal que $(H : H \cap x_i P x_i^{-1})$ no es divisible por p. Esto significa que que p^β divide a $|H \cap x_i P x_i^{-1}|$ y en consecuencia $H \cap x_i P x_i^{-1} \in \mathrm{Syl}_p(H)$. Por el teorema de Cayley podemos suponer que nuestro subgrupo G es un subgrupo de $\mathbf{GL}_n(p)$ para algún $n \in \mathbb{N}$ y algún primo p. Sea P un subgrupo de Sylow del grupo $\mathbf{GL}_n(P)$. La observación que demostramos aplicada al grupo G nos dice que existe $g \in \mathbf{GL}_n(p)$ tal que $G \cap gPg^{-1}$ es un subgrupo de Sylow de G.

Antes de demostrar el segundo teorema de Sylow, vamos a demostrar un resultado similar, aunque levemente más técnico.

Teorema 13.9. *Si P es un p-subgrupo de G y $S \in \mathrm{Syl}_p(G)$, entonces $P \subseteq gSg^{-1}$ para algún $g \in G$.*

Demostración. Sea $X = \{xS : x \in G\}$ el conjunto de coclases de S en G. Entonces $|X| = (G : S)$ no es divisible por el primo p. Si hacemos actuar a G en X por multiplicación a izquierda, en particular, el subgrupo P también actuará en X por multiplicación a izquierda. Si descomponemos entonces a X en P-órbitas, existirá una P-órbita $\mathscr{O}$ de tamaño no divisible por p, pues $|X|$ no es divisible por p. Como $|\mathscr{O}|$ divide al orden de P y p no divide al tamaño de $\mathscr{O}$, necesariamente se tiene $|\mathscr{O}| = 1$, es decir $\mathscr{O} = \{gS\}$ para algún $g \in G$. Como entonces $P(gS) = gS$, en particular, $xg \in gS$ para todo $x \in P$, es decir: si $x \in P$, entonces $x \in gSg^{-1}$. Luego $P \subseteq gSg^{-1}$. □

Corolario 13.10. *Sea p un número primo. Si G es un grupo finito y P es un p-subgrupo de G, entonces P está contenido en algún p-subgrupo de Sylow de G.*

Demostración. Si $S \in \mathrm{Syl}_p(G)$, entonces $gSg^{-1} \in \mathrm{Syl}_p(G)$ pues $|gSg^{-1}| = |S|$. El teorema anterior nos da el corolario pues $P \subseteq gSg^{-1}$ para algún $g \in G$ □

Ahora sí, el segundo teorema de Sylow, que afirma que dos p-subgrupos de Sylow siempre serán conjugados.

Teorema 13.11 (segundo teorema de Sylow). *Sea G un grupo finito y p un número primo. Si $S,T \in \mathrm{Syl}_p(G)$, entonces existe $g \in G$ tal que $gSg^{-1} = T$.*

Demostración. Utilizamos el teorema anterior con $P = T$ y entonces $T \subseteq gSg^{-1}$ para algún $g \in G$. Como $|S| = |T|$ y además $|T| \leq |gSg^{-1}| = |S|$, se concluye que $T = gSg^{-1}$. □

Corolario 13.12. *Sea G un grupo finito, p un número primo y $S \in \mathrm{Syl}_p(G)$. Si S es normal en G, entonces* $\mathrm{Syl}_p(G) = \{S\}$.

Demostración. Si $T \in \mathrm{Syl}_p(G)$, entonces $T = gSg^{-1} = S$ para algún $g \in G$. □

Veamos una demostración alternativa del segundo teorema de Sylow que usa coclases dobles. Si $P,Q \in \mathrm{Syl}_p(G)$ y descomponemos a G en (P,Q)-coclases dobles, tenemos

$$p^\alpha m = \sum_{i=1}^{k} \frac{|P||Q|}{|P \cap x_i Q x_i^{-1}|} \implies m = \sum_{i=1}^{k} \frac{|P|}{|P \cap x_i Q x_i^{-1}|}$$

para ciertos $x_1, \ldots, x_k \in G$. Como m no es divisible por p, existe algún $i \in \{1, \ldots, k\}$ tal que $|P| = |P \cap x_i Q x_i^{-1}|$, lo que implica que $P = x_i Q x_i^{-1}$ para algún $i \in \{1, \ldots, k\}$.

Antes de enunciar y demostrar el tercer teorema de Sylow introduciremos la siguiente notación. Si p es un número primo y G es un grupo finito de orden $p^\alpha m$ con $\mathrm{mcd}(p,m) = 1$, entonces $n_p(G) = |\mathrm{Syl}_p(G)|$. Observar que entonces

$$n_p(G) = (G : N_G(P))$$

para cualquier $P \in \mathrm{Syl}_p(G)$. Veremos que además $n_p(G)$ divide a m.

Teorema 13.13 (tercer teorem de Sylow). *Sea G un grupo finito y p un número primo. Entonces $n_p(G) \equiv 1$ mód p.*

Demostración. Supongamos que $|G| = p^\alpha m$ con m un entero no divisible por p. Sea $P \in \mathrm{Syl}_p(G)$, que sabemos que existe por el primer teorema de Sylow, y sea $n = n_p(G)$, Consideramos el conjunto

$$X = \{gPg^{-1} : g \in G\} = \{P = P_1, P_2, \ldots, P_n\}.$$

El segundo teorema de Sylow implica que $|X| = n$.

Si hacemos actuar a G en X por conjugación, P también actúa en X por conjugación. Entonces todas las P-órbitas tiene tamaño una potencia del primo p.

Afirmamos que $\{P\}$ es la única P-órbita de tamaño 1. En efecto, como $xPx^{-1} = P$ si $x \in P$, tenemos que $\{P\}$ es una P-órbita. Sea $\{P_i\}$ una P-órbita de tamaño 1. Entonces $xP_ix^{-1} = P_i$ para todo $x \in P$ y luego $P \subseteq N_G(P_i)$. El grupo $N_G(P_i)/P_i$ tiene orden no divisible por p, pues $P_i \in \mathrm{Syl}_p(G)$. Si $xP_i \in N_G(P_i)/P_i$ con $x \in P$, entonces $xP_i = P_i$, es decir $x \in P_i$, pues como $(xP_i)^{p^\alpha} = x^{p^\alpha} P_i = P_i$, entonces $|xP_i|$ divide a p^α.

Luego $|xP_i| = 1$, pues $N_G(P_i)/P_i$ tiene orden coprimo con p, y entonces $x \in P_i$. Esto implica que $P \subseteq P_i$ y luego $P = P_i$ ya que ambos conjuntos tienen tamaño p^α. Ahora tenemos

$$X = \{P\} \cup \underbrace{\mathscr{O}_1 \cup \mathscr{O}_2 \cup \cdots \cup \mathscr{O}_k}_{\text{de tamaño} > 1 \text{ divisible por } p},$$

de donde obtenemos $n_p(G) = |X| \equiv 1 \text{ mód } p$. □

Una demostración alternativa del tercer teorema de Sylow basada en coclases dobles. Sean $P \in \mathrm{Syl}_p(G)$ y $N = N_G(P)$. Recordemos que $n_p(G) = (G : N)$. Si descomponemos a G en (P,N)-coclases dobles,

$$|G| = \sum_{i=1}^{k} \frac{|P||N|}{|N \cap x_i P x_i^{-1}|}$$

para ciertos $x_1, \ldots, x_k \in G$. Sin perder generalidad podemos suponer que $x_1 = 1$, entonces la fórmula anterior queda

$$n_p(G) = 1 + \sum_{i=2}^{k} \frac{|P|}{|N \cap x_i P x_i^{-1}|},$$

pues $(G : N) = n_p(G)$. El teorema quedará demostrado si vemos que la suma del miembro de la derecha es divisible por p. Si esto no pasa, es decir si existe $i \in \{2, \ldots, k\}$ tal que $|N \cap x_i P x_i^{-1}| = |P|$, entonces $x_i P x_i^{-1} = N \cap x_i P x_i^{-1} \subseteq N$. Como entonces P y también $x_i P x_i^{-1}$ son ambos p-subgrupos de Sylow de N, el segundo teorema de Sylow afirma que estos subgrupos tienen que ser conjugados en N. Por definición del normalizador, P es normal en N. En consecuencia, $x_i P x_i = P$, es decir $x_i \in N$, una contradicción pues como $i > 1$ se tiene que Px_iN y $Px_1N = PN$ son coclases dobles disjuntas.

Veamos algunas aplicaciones sencillas de los teoremas de Sylow.

Ejemplo 13.14. Si G es un grupo de orden 15, entonces G es cíclico.

Sean $n_3 = n_3(G)$ y $n_5 = n_5(G)$. Sabemos que $n_3 \equiv 1$ mód 3 y que además n_3 divide a 5, luego $n_3 = 1$. Esto nos dice que existe un único $H \in \mathrm{Syl}_3(G)$, que resulta ser normal en G e isomorfo a $\mathbb{Z}/3$. Similarmente, $n_5 = 1$ y existe entonces un único $K \in \mathrm{Syl}_5(G)$ tal que $K \trianglelefteq G$ y $K \simeq \mathbb{Z}/5$. Como $H \cap K = \{1\}$ por el teorema de Lagrange, tenemos

$$|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = 15 = |G|.$$

Luego $G = HK \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \simeq \mathbb{Z}/15$.

El siguiente ejemplo, es bastante más difícil que el anterior.

Ejemplo 13.15. Si G es un grupo de orden 455, entonces G es cíclico.

Para cada primo p que divide al orden de G, sea $n_p = n_p(G)$. Como n_5 divide a 7×13 y $n_5 \equiv 1$ mód 5, entonces $n_5 \in \{1{,}91\}$. En cambio, un cálculo sencillo nos da $n_7 = n_{13} = 1$. Sea $P \in \mathrm{Syl}_7(G)$ y sea $Q \in \mathrm{Syl}_{13}(G)$, ambos son subgrupos normales en G. Como P y Q tienen órdenes coprimos, el teorema de Lagrange implica que $P \cap Q = \{1\}$.

Estudiaremos ahora los subgrupos de Sylow de los cocientes G/P y G/Q. Sea $m_5 = n_5(G/P)$ y $m_{13} = n_{13}(G/P)$. Como m_5 divide a 13 y además $m_5 \equiv 1$ mód 5, entonces $m_5 = 1$. Similarmente, $m_{13} = 1$ y entonces $G/P \simeq \mathbb{Z}/5 \times \mathbb{Z}/13$. De la misma forma vemos que $G/Q \simeq \mathbb{Z}/5 \times \mathbb{Z}/7$ y entonces G/P y G/Q son ambos abelianos. Esto significa que $[G,G] \subseteq P \cap Q = \{1\}$ y luego G también es un grupo abeliano. En particular, $n_5 = 1$ y luego

$$G \simeq \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/13 \simeq \mathbb{Z}/455.$$

Ejemplo 13.16. Si G es un grupo de orden 21, entonces

$$G \simeq \mathbb{Z}/21 \text{ o bien } G \simeq \langle x, y : x^7 = y^3 = 1, yx = x^2 y \rangle.$$

Sean $n_3 = n_3(G)$ y $n_7 = n_7(G)$. Como $n_7 \equiv 1$ mód 7 y n_3 divide a 3, entonces $n_7 = 1$. Existe entonces un único $H \in \mathrm{Syl}_7(G)$. Ese subgrupo H es tal que $H \trianglelefteq G$ y $H \simeq \mathbb{Z}/7$. Entonces $H = \langle x \rangle$ donde $x^7 = 1$. Sea $K \in \mathrm{Syl}_3(G)$. Como n_3 divide a 7 y $n_3 \equiv 1$ mód 3, entonces $n_3 \in \{1,7\}$. En cualquier caso, $K \simeq \mathbb{Z}/3$ y entonces $K = \langle y \rangle$ donde $y^3 = 1$. Por el teorema de Lagrange, $H \cap K = \{1\}$ y luego $G = HK$. En particular,

$$G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2\}.$$

Como H es normal en G, $yxy^{-1} \in H$, es decir $yxy^{-1} = x^i$ para algún $i \in \{1, \ldots, 6\}$. Tenemos entonces que $x^7 = y^3 = 1$ y además $yx = x^i y$ para un cierto $i \in \{1, \ldots, 6\}$. Para ver qué podemos decir de ese i observamos que

$$x = y^3 x y^{-3} = y^2 (yxy^{-1}) y^{-2} = y^2 x^i y^{-2} = y (x^i)^2 y^{-1} = (x^i)^3$$

y luego $i^3 \equiv 1$ mód 7, es decir $i \in \{1,2,4\}$. Tenemos entonces tres casos para analizar.

(a) Si $yxy^{-1} = x$, entonces $xy = yx$ y luego $K \trianglelefteq G$. Esto implica que $G \simeq H \times K \simeq \mathbb{Z}/21$.

(b) Si $yxy^{-1} = x^2$, entonces tenemos todo lo que necesitamos para conocer G. De hecho, no solamente tenemos la descripción prometida sino que podemos escribir la tabla de multiplicación e intentar reconocer este grupo. Para poder tener una idea más concreta del grupo G que encontramos en este caso, mencionamos que puede presentarse como un cierto subgrupo de $\mathbf{GL}_2(\mathbb{Z}/7)$. En efecto,

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad G \simeq \langle x, y \rangle \leq \mathbf{GL}_2(\mathbb{Z}/7).$$

(c) Si $yxy^{-1} = x^4$, entonces $y^2 x y^{-2} = x^2$. Como $|y^2| = |y| = 3$, si $z = y^2$, entonces $H = \langle y \rangle = \langle z \rangle$, lo que nos dice que, en realidad, estamos en el caso anterior.

Ejemplo 13.17. Si G es un grupo de orden $5 \cdot 7 \cdot 17$, entonces G es cíclico.

Si $p \in \{5,7,17\}$, sea $n_p = n_p(G)$. Como $n_5 \equiv 1$ mód 5 y n_5 divide a $7 \cdot 17$, entonces $n_5 = 1$. Sea $H \in \mathrm{Syl}_5(G)$. Al ser el único 5-subgrupo de Sylow de G, H es normal en G. Sean además $K \in \mathrm{Syl}_7(G)$ y $L \in \mathrm{Syl}_{17}(G)$. Como H es normal en G,

HK es un subgrupo de G. Por el teorema de Lagrange, $H \cap K = \{1\}$ pues H y K tienen órdenes coprimos. Entonces $|HK| = 5 \cdot 7$.

Usaremos ahora la teoría de Sylow pero en el grupo HK. Si $m_7 = n_7(HK)$, entonces $m_7 = 1$. En particular, $K \in \mathrm{Syl}_7(HK)$ y además K es normal en HK, es decir $HK \subseteq N_G(K)$, lo que implica que $|HK| \leq |N_G(K)|$. Como

$$n_7 = (G : N_G(K)) = \frac{|G|}{|N_G(K)|} \leq \frac{|G|}{|HK|} = \frac{5 \cdot 7 \cdot 17}{5 \cdot 7} = 17$$

y además $n_7 \in \{1, 5 \cdot 17\}$, se concluye que $n_7 = 1$. Dejamos como ejercicio utilizar la misma técnica para demostrar que $n_{17} = 1$. En conclusión, K y L son ambos normales en G. El teorema de Lagrange implica que $L \cap H = H \cap K = L \cap K = \{1\}$ y entonces

$$L \cap (HK) = H \cap (LK) = K \cap (LH) = \{1\}.$$

Luego $G = HKL \simeq \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/17 \simeq \mathbb{Z}/5 \cdot 7 \cdot 17$.

Ejemplo 13.18. Si G es un grupo de orden 12 tal que $n_3(G) \neq 1$, entonces $G \simeq \mathbb{A}_4$.

Sea $P \in \mathrm{Syl}_3(G)$ y sea $n_3 = n_3(G) = 4$. Claramente P no es normal en G. Hacemos actuar a G en el conjunto de coclases G/P por multiplicación a izquierda y obtenemos un morfismo

$$\rho : G \to \mathbb{S}_{G/P} \simeq \mathbb{S}_4.$$

Afirmamos que ρ es inyectivo. Primero vemos que $\ker \rho \subseteq P$ pues

$$x \in \ker \rho \implies \rho_x = \mathrm{id} \implies xP \subseteq P \implies x \in P.$$

Como P no es normal en G, $P \neq \ker \rho$. Luego $\ker \rho$ es un subgrupo propio de P. En consecuencia, $\ker \rho = \{1\}$ pues $|P| = 3$.

Sean $S, T \in \mathrm{Syl}_3(G)$. Como $S \simeq T \simeq \mathbb{Z}/3$, el teorema de Lagrange implica que $S \cap T = \{1\}$. Esto implica que G contiene exactamente ocho elementos de orden tres. Como los elementos de orden tres de $\mathbb{S}_4$ están todos en $\mathbb{A}_4$, el subgrupo $\rho(G) \cap \mathbb{A}_4$ de $\mathbb{S}_4$ contiene al menos ocho elementos. Luego $G \simeq \rho(G) \simeq \mathbb{A}_4$.

Otra aplicación bastante común de los teoremas de Sylow es a la (no) simplicidad de grupos.

Ejemplo 13.19. Si G es un grupo de orden 36, entonces G no es simple.

Si G fuera simple, entonces $n_3 = n_3(G) = 4$. Sea $P \in \mathrm{Syl}_3(G)$. Si hacemos actuar a G en $X = \{gPg^{-1} : g \in G\}$ por conjugación, tenemos un morfismo de grupos

$$\rho : G \to \mathbb{S}_X \simeq \mathbb{S}_4.$$

Como G es simple, $\ker \rho = \{1\}$ o bien $\ker \rho = G$. Si $\ker \rho = G$, P es normal en G, una contradicción. Luego $\ker \rho = \{1\}$ y entonces ρ es inyectivo. En particular, gracias al primer teorema de isomorfismos,

$$G \simeq G/\ker \rho \simeq \rho(G) \lesssim \mathbb{S}_4,$$

que implica que 36 divide a 24, una contradicción.

Ejemplo 13.20. Si G es un grupo de orden 30, entonces G no es simple.

Para cada primo p que divide a 30, sea $n_p = n_p(G)$. Supongamos que $n_2 > 1$, $n_3 > 1$ y que $n_5 > 1$. Entonces $n_3 = 10$. Tenemos así diez 3-subgrupos de Sylow, todos ellos con intersección trivial. En efecto, para ver que la intersección de dos 3-subgrupos de Sylow es trivial procedemos de la siguiente forma: Si $P, Q \in \mathrm{Syl}_3(G)$ son tales que $P \neq Q$, entonces $P \cap Q \leq P$ y luego $|P \cap Q| \in \{1,3\}$. Si $|P \cap Q| = 3$, entonces $P \cap Q = P$ y luego $P = Q$, un contradicción. De la misma forma, tenemos seis 5-subgrupos de Sylow de G, todos con interección trivial. En conclusión,

$$|G| \geq 1 + 10 \times 2 + 6 \times 4 > 30,$$

una contradicción.

Al terminar la demostración del primer teorema de Sylow, usamos coclases dobles para demostrar que si H es un subgrupo de un grupo finito G y $P \in \mathrm{Syl}_p(G)$, entonces $g \in G$ tal que $gPg^{-1} \cap H \in \mathrm{Syl}_p(H)$. Otra demostración puede obtenerse al considerar la acción de H en G/P por multiplicación a izquierda.

Teorema 13.21. *Sea N un subgrupo normal de un grupo finito G y sea $P \in \mathrm{Syl}_p(N)$. Entonces $P \cap N \in \mathrm{Syl}_p(N)$ y todo los p-subgrupos de Sylow de N se obtienen de esa forma.*

Demostración. Como N es normal, sabemos por el teorema anterior que existe un $g \in G$ tal que

$$g(P \cap N)g^{-1} = gPg^{-1} \cap gNg^{-1} = gPg^{-1} \cap N \in \mathrm{Syl}_p(N).$$

Luego $P \cap N$ es un p-subgrupo de Sylow de $g^{-1}Ng = N$.

Sea $Q \in \mathrm{Syl}_p N$ y sea $P \in \mathrm{Syl}_p(G)$ tal que $Q \subseteq P$. Entonces Q está contenido en el p-subgrupo de Sylow $P \cap N$ de N. Luego $Q = P \cap N$. □

Como corolario obtenemos que si N es un subgrupo normal de un grupo finito G, entonces $n_p(N) \leq n_p(G)$.

Teorema 13.22. *Sean N un subgrupo normal de un grupo finito G, $\pi\colon G \to G/N$ el morfismo canónico y $P \in \mathrm{Syl}_p(G)$. Entonces $\pi(G) \in \mathrm{Syl}_p(G/N)$ y todos los p-subgrupos de Sylow de G/N se obtienen de esa forma.*

Demostración. Como $\pi(P) = \pi|_P(P) \simeq P/N \cap P$ por el segundo teorema de isomorfismo, $\pi(P)$ es un p-grupo. Como además $|PN| = |P||N|/|P \cap N|$,

$$(G/N : \pi(P)) = (G : PN)$$

no es divisible por p. Luego $\pi(P) \in \mathrm{Syl}_p(G/N)$.

Si $Q \in \mathrm{Syl}_p(G/N)$, entonces $Q = \pi(H)$ para algún subgrupo H de G tal que $N \subseteq H$. En particular,

$$|Q| = |\pi(H)| = \frac{|H|}{|H \cap N|} = \frac{|H|}{|N|}$$

y luego

$$(G : H) = \frac{|G|/|N|}{|H|/|N|} = (G/N : Q)$$

no es divisible por p. Esto nos dice que si $X \in \mathrm{Syl}_p(H)$, entonces $X \in \mathrm{Syl}_p(G)$. Luego $\pi(X) \subseteq \pi(H) = Q$ y entonces $\pi(X) = Q$ ya que $\pi(X) \in \mathrm{Syl}_p(G/N)$. □

Como corolario, si N es un subgrupo normal de un grupo finito G, entonces $n_p(G/N) \leq n_p(G)$.

Corolario 13.23. *Si un grupo finito G tiene un único p-subgrupo de Sylow para algún primo p, entonces todo subgrupo y todo cociente de G también tienen un único p-subgrupo de Sylow.*

Demostración. Si H es un subgrupo de G, entonces $n_p(H) \leq n_p(G) = 1$. Si N es un subgrupo normal de G, entonces $n_p(G/N) \leq n_p(G) = 1$. □

Capítulo 14
El teorema de Jordan–Hölder

Definición 14.1. Una sucesión de subgrupos $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$ de un grupo G es una **serie de composición** si cada G_{i+1} es normal en G_i y cada cociente G_i/G_{i+1} es simple. En ese caso, el entero r es la **longitud** de la serie de composición y los cocientes son los **factores** de la serie de composición.

Ejemplo 14.2. $\mathbb{S}_5 \supseteq \mathbb{A}_5 \supseteq \{1\}$ es una serie de composición de $\mathbb{S}_5$.

Ejemplo 14.3. $\mathbb{Z}$ no admite una serie de composición pues $\mathbb{Z}$ no es simple y cada subgrupo S de $\mathbb{Z}$ cumple que $S \simeq n\mathbb{Z} \simeq \mathbb{Z}$.

Vimos en el ejemplo anterior que no todo grupo admite una serie de composición. Sin embargo, todo grupo finito sí lo hará. Esa será nuestra primera observación.

Proposición 14.4. *Si G es un grupo finito, entonces G admite una serie de composición.*

Demostración. Procederemos por inducción en el orden de G. Si G es simple, entonces $G \supseteq \{1\}$ es una serie de composición. Si G no es simple, G contiene un subgrupo normal propio $N \neq \{1\}$, que además puede tomarse maximal sobre los subgrupos normales de G. La maximal de N entro los normales de G implica que G/N es un grupo simple. Por hipótesis inductiva, N admite una serie de composición

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}$$

y entonces

$$G \supseteq N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}$$

es una serie de composición para G pues G/N es simple. □

Definición 14.5. Dos series de composición

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}, \qquad G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r = \{1\}$$

de un grupo G se dirán **equivalentes** si existe $\sigma \in \mathbb{S}_r$ tal que

$$G_{i-1}/G_i \simeq H_{\sigma(i)-1}/H_{\sigma(i)}$$

para todo $i \in \{1,\dots,n\}$.

Ejemplo 14.6. Sea $G = \langle x \rangle \simeq \mathbb{Z}/6$. Las series de composición

$$G \supseteq \langle x^2 \rangle = G_1 \supseteq \{1\}, \quad G \supseteq \langle x^3 \rangle = H_1 \supseteq \{1\}$$

son equivalentes por la permutación $\sigma = (12) \in \mathbb{S}_2$. Observar que $G/G_1 \simeq \mathbb{Z}/3$ y $G/H_1 \simeq \mathbb{Z}/2$.

Nuestro objetivo es demostrar el teorema de Jordan–Hölder, que afirma que todo grupo que admita una serie de composición, tendrá esencialmente una única serie de composición módulo equivalencia. Antes de ir directamente al teorema, necesitamos un resultado previo.

Lema 14.7. *Sea $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$ una serie de composición para G y sea N un subgrupo normal de G. Entonces N también admite una serie de composición.*

Demostración. Para cada i, sea $N_i = G_i \cap N$. Como ejercicio, se demuestra que

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}$$

y que además N_{i+1} es normal en N_i para todo i. Como

$$N \cap G_{i+1} = N \cap (G_i \cap G_{i+1}) = (N \cap G_i) \cap G_{i+1}$$

para todo i, entonces

$$\frac{N_i}{N_{i+1}} = \frac{N \cap G_i}{N \cap G_{i+1}} = \frac{N \cap G_i}{(N \cap G_i) \cap G_{i+1}} \simeq \pi(N \cap G_i)$$

donde $\pi\colon G_i \to G_i/G_{i+1}$ es el morfismo canónico. En efecto, la restricción $\pi|_{N_i}$ tiene núcleo $(N_i \cap G_i) \cap G_{i+1} = (N \cap G_{i+1})$ y entonces, por el primer teorema de isomorfismos, $\pi(N_i) = \pi(N \cap G_i) \simeq (N \cap G_i)/(N \cap G_{i+1})$. Como $\pi(N \cap G_i)$ es un subgrupo normal del grupo simple $\pi(G_i) = G_i/G_{i+1}$, se sigue que $N_i = N_{i+1}$ o bien $N_i/N_{i+1} = G_i/G_{i+1}$. Luego de remover las posibles repeticiones obtememos entonces una serie de composición para N. □

Ahora sí, el teorema.

Teorema 14.8 (Jordan–Hölder). *Si G es un grupo que admite una serie de composición, entonces todas las series de composición de G tienen la misma longitud y son además equivalentes.*

Demostración. Sean

$$G = G_0 \supseteq G_1 \supseteq \cdots \subseteq G_r = \{1\}, \qquad G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_s = \{1\}$$

dos series de composición de G. Procederemos por inducción en r. Si $r = 1$, entonces G es simple y el teorema queda demostrado trivialmente. Si $r > 1$, supongamos que el resultado vale para todos los grupos que admiten una series de composición de longitud $< r$.

Si $G_1 = H_1$, entonces G_1 admite dos series de longitudes $r-1$ y $s-1$, respectivamente, y entonces, por hipótesis inductiva, $r = s$ y además las series de composición son equivalentes.

Si $G_1 \neq H_1$, como G_1 y H_1 son ambos normales en G, entonces G_1H_1 es también normal en G (esto es un ejercicio que dejamos en la página ??). Como G/G_1 es simple y $G_1 \trianglelefteq G_1H_1 \trianglelefteq G$, entonces $G_1 = G_1H_1$ o bien $G_1H_1 = G$, pues G_1 es maximal entre todos los subgrupos normales de G. Como G/H_1 es simple, H_1 es maximal entre todos los subgrupos normales de G, y entonces $H_1 = G_1H_1$ o bien $G_1H_1 = G$. En conclusión, $G_1H_1 = G$. Sea $K = G_1 \cap H_1$. Entonces K es normal en G y además

$$G/G_1 = \frac{G_1H_1}{G_1} \simeq H_1/K, \quad G/H_1 = \frac{G_1H_1}{H_1} \simeq G_1/K.$$

Luego H_1/K y G_1/K son ambos grupos simples. Gracias al lema anterior sabemos que K también admite una serie de composición, digamos

$$K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_t = \{1\}.$$

Luego

$$G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}, \quad G_1 \supseteq K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_t = \{1\},$$

son ambas series de composición para G_1. La hipótesis inductiva implica entonces que $r-1 = t+1$, es decir $t = r-2$, y además que estás series de composición son equivalentes. Similarmente,

$$H_1 \supseteq H_2 \supseteq \cdots \supseteq H_s = \{1\}, \quad H_1 \supseteq K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_t = \{1\}$$

son series de composición para H_1 y además $s-1 = t+1 = r-1$, lo que implica que $r = s$. Como las series de composición

$$G = G_0 \supseteq G_1 \supseteq K_0 \supseteq \cdots \supseteq K_t = \{1\}, \quad G = H_0 \supseteq H_1 \supseteq K_0 \supseteq \cdots \supseteq K_t = \{1\},$$

son equivalentes, las series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}, \quad G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r = \{1\},$$

también son equivalentes. □

Veamos un corolario muy simpático.

Corolario 14.9 (teorema fundamental de la aritmética). *Los primos y sus multiplicidades que aparecen en la factorzación de un entero $n \geq 2$ están unívocamente determinados por n.*

Demostración. Escribamos $n = p_1 \cdots p_k$, donde los primos $p_1, \ldots, p_k$ no son necesariamente distintos. Si $G = \langle x \rangle \simeq \mathbb{Z}/n$ es cíclico de orden n, entonces

$$G = \langle x \rangle \supseteq \langle x^{p_1} \rangle \supseteq \langle x^{p_1 p_2} \rangle \supseteq \cdots \supseteq \langle x^{p_1 \cdots p_{k-1}} \rangle \supseteq \{1\}$$

es una serie de composición con factores de orden $p_1 p_2, \ldots, p_k$, respectivamente. Si $n = q_1 \ldots q_l$ es otra factorización de n como producto de primos, entonces

$$G = \langle x \rangle \supseteq \langle x^{q_1} \rangle \supseteq \langle x^{q_1 q_2} \rangle \supseteq \cdots \supseteq \langle x^{q_1 \cdots q_{l-1}} \rangle \supseteq \{1\}$$

es también una serie de composición. Por el teorema de Jordan–Hölder, $k = l$ y además las series son equivalentes, algo que se traduce en poder reordenar los primos $q_1, \ldots, q_k$ y obtener como $p_1, \ldots, p_k$. □

Capítulo 15
Grupos resolubles

Una forma de atacar ciertos aspectos de la estrucura de los grupos se basa en estudiar propiedades de los factores que aparecen en las series de composición. El caso que estudiaremos en este capítulo involucra factores abelianos. Nos concentraremos en el caso de los grupos finitos.

Definición 15.1. Diremos que un grupo finito G es **resoluble** si los factores de su serie de composición son abealianos.

La definición anterior trivialmente implica que todo grupo abeliano finito será resoluble. En cambio, grupos simples finitos no abelianos no serán resolubles.

Ejemplo 15.2. Si p es primo, $\mathbb{D}_p$ es resoluble pues $\mathbb{D}_p \supseteq \langle r \rangle \supseteq \{1\}$ es una serie de composición.

Ejemplo 15.3. El grupo simétrico $\mathbb{S}_3$ es resoluble pues $\mathbb{S}_3 \supseteq \mathbb{A}_3 \supseteq \{\mathrm{id}\}$ es una serie de composición.

Ejemplo 15.4. Si $n \geq 5$ el grupo simétrico $\mathbb{S}_n$ no es resoluble. Una serie de composición para $\mathbb{S}_n$ es $\mathbb{S}_n \supseteq \mathbb{A}_n \supseteq \{\mathrm{id}\}$.

Ejemplo 15.5. Todo grupo G de orden 20 es resoluble. Por el primer teorema de Sylow sabemos que existe $P \in \mathrm{Syl}_2(G)$, es decir $|P| = 4$. Por el teorema de Cauchy sabemos que existe $x \in P$ tal que x tiene orden 2. Entonces G es resoluble pues la serie de composición $G \supseteq P \supseteq \langle x \rangle \supseteq \{1\}$ tiene factores abelianos.

Vamos a dar una caracterización de la resolubilidad de un grupo G. Para eso definimos la siguiente sucesión de conmutadores:

$$G^{(0)} = G, \quad G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

para $k \geq 0$. La sucesión $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots$ se conoce como la **serie derivada** de G o sucesión de conmutadores de G.

Teorema 15.6. *Sea G un grupo finito. Las siguientes afirmaciones son equivalentes:*

1) G es resoluble.
2) G admite una sucesión $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ de subgrupos tal que $G_i \trianglelefteq G_{i-1}$ para todo i y además G_{i-1}/G_i es abeliano para todo i.
3) $G^{(n)} = \{1\}$ para algún $n \in \mathbb{N}$.

Demostración. La implicación $(1) \implies (2)$ es trivial, solamente basta con utilizar una serie de composición para el grupo.

Demostremos ahora que $(2) \implies (3)$. Veamos por inducción que $G^{(i)} \subseteq G_i$ para todo $i \geq 0$. El caso $i = 0$ es trivial. Si el resultado vale para algún $i \geq 0$, entonces, como G_i/G_{i+1} es abeliano, $[G_i, G_i] \subseteq G_{i+1}$ y luego

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}.$$

En particular, $G^{(n)} \subseteq G_n = \{1\}$.

La implicación $(3) \implies (2)$ es trivial.

Por último, demostraremos que $(2) \implies (1)$. Sea

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\} \tag{15.1}$$

una sucesión de subgrups de G tal que $H_i \trianglelefteq H_{i-1}$ para todo i y además H_{i-1}/H_i es abeliano para todo i, donde n se tomará lo mayor posible. Entonces cada cociente H_{i-1}/H_i es simple, pues de lo contrario existirá $N \trianglelefteq H_{i-1}$ tal que $H_i \subsetneq N \subsetneq H_{i-1}$ y la sucesión

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_{i-1} \supseteq N \supseteq H_i \supseteq \cdots \supseteq H_n = \{1\}$$

tendrá longitud $> n$, ya que N/H_i es abeliano por ser un subgrupo de H_{i-1}/H_i y

$$H_{i-1}/N \simeq \frac{H_{i-1}/H_i}{N/H_i}$$

es también abeliano, una contradicción. En conclusión, la sucesión (15.1) es una serie de composición con factores abelianos. □

Un grupo infinito se dirá resoluble si se satisface el segundo o tercer ítem del teorema anterior. El teorema siguiente ya no requiere la finitud del grupo G.

Teorema 15.7. *Sea G un grupo y H un subgrupo de G.*

1) Si G es resoluble, H es resoluble.
2) Si $K \trianglelefteq G$. Entonces G es resoluble si y sólo si K y G/K son resolubles.

Demostración. La primera afirmación se obtiene de la inclusión $H^{(i)} \subseteq G^{(i)}$ para todo $i \geq 0$. Para demostrar la segunda, sea $Q = G/K$ y sea $\pi\colon G \to Q$ el morfismo canónico.

Afirmamos que $\pi(G^{(i)}) = Q^{(i)}$ para todo $i \geq 0$. El caso $i = 0$ es fácil pues π es sobreyectivo. Si el resultado vale para un cierto $i \geq 0$, entonces

$$\pi(G^{(i+1)}) = \pi([G^{(i)}, G^{(i)}]) = [\pi(G^{(i)}), \pi(G^{(i)})] = [Q^{(i)}, Q^{(i)}] = Q^{(i+1)}$$

Supongamos primero que K y Q son resolubles. Entonces que $Q^{(n)} = \{1\}$ para algún $n \in \mathbb{N}$. Como $\pi(G^{(n)}) = Q^{(n)} = \{1\}$, entonces $G^{(n)} \subseteq K = \ker \pi$. Como K es resoluble, existe $m \in \mathbb{N}$ tal que $K^{(m)} = \{1\}$. Luego

$$G^{(n+m)} \subseteq \left(G^{(n)}\right)^{(m)} \subseteq K^{(m)} = \{1\}.$$

Supngamos ahora que G es resoluble, es decir $G^{(n)} = \{1\}$ para algún $n \in \mathbb{N}$. Entonces $Q^{(n)} = \pi(G^{(n)}) = \pi(\{1\}) = \{1\}$ y luego Q es resoluble. La resolubiildad del subgrupo K se obtiene a partir del primer ítem del teorema. □

La siguiente proposición nos da muchos ejemplos de grupos resolubles.

Proposición 15.8. *Sea p un número primo. Si G es un p-grupo, entonces G es resoluble.*

Demostración. Procederemos por inducción en el order de G. Si $|G| = 1$, el resultado es trivialmente cierto. Supongamos entonces que la proposición vale para todos los p-grupos de tamaño $< |G|$. Si G es abeliano, G es resoluble. De lo contrario, $1 < |Z(G)| < |G|$ pues $Z(G) \neq \{1\}$ porque G es un p-grupo. Como $Z(G)$ es resoluble (por ser abeliano) y $G/Z(G)$ es resoluble (por hipótesis inductiva), G es resoluble gracias al teorema anterior. □

Parte II
Anillos

Capítulo 16
Anillos

En esta parte trataremos sobre algunas propiedades básicas de ciertas estructuras que se conocen como anillos conmutativos. Si bien los anillos no conmutativos tienen gran importancia dentro de la matemática, las aplicaciones que daremos en este curso, estarán basadas en la teoría de anillos conmutativos.

Definición 16.1. Un anillo es un conjunto R con dos operaciones binarias, una suma $(x,y) \mapsto x+y$ y un producto $(x,y) \mapsto xy$ de forma tal que se cumplen las siguientes propiedades:

1) $(R,+)$ es un grupo abeliano (escrito aditivamente).
2) $(xy)z = x(yz)$ para todo $x,y,z \in R$.
3) Existe $e \in R$ tal que $xe = ex = x$ para todo $x \in R$.
4) $x(y+z) = xy+xz$ para todo $x,y,z \in R$.
5) $(x+y)z = xz+yz$ para todo $x,y,z \in R$.

Definición 16.2. Un anillo R se dirá **conmutativo** si $xy = yx$ para todo $x,y \in R$.

Ejemplos 16.3. $\mathbb{N}$ no es un anillo. En cambio, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ sí son anillos conmutativos.

Ejemplo 16.4. $\mathbb{Z}/n$ es un anillo conmutativo.

Ejemplo 16.5. Si R es un anillo, entonces

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}_0, a_0, \ldots, a_n \in R \right\}$$

es un anillo con las operaciones usuales. Un polinomio es una expresión formal de la forma

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

no una función $R \to R$. Por ejemplo, si $R = \mathbb{Z}/2$ hay cuatro funciones $R \to R$ pero infintios polinomios con coeficientes en R. Veamos un polinomio concreto que además nos recuerda cuál es la notación que utilizaremos:

$$1x^3 + 0x^2 + x - 5 = x^3 + x - 5 \in \mathbb{R}[X].$$

Como dijimos al principio del capítulo, los anillos no conmutativos tienen gran importancia dentro de la matemática. Para convencernos, tenemos el siguiente ejemplo. Si $n \geq 2$, entonces $M_n(\mathbb{R}) = \mathbb{R}^{n\times n}$ es un anillo no conmutativo con las operaciones usuales.

Ejercicio 16.6. Si A es un grupo abeliano, entonces $\mathrm{End}(A)$ es un anillo conmutativo con las operaciones

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(g(x)).$$

Si R es un anillo, es fácil verificar las siguientes propiedades:

1) $x0 = 0x = 0$ para todo $x \in R$.
2) $-x = (-1)x = x(-1)$ para todo $x \in R$.
3) $x(-y) = -xy = (-x)y$ para todo $x, y \in R$.
4) $(-x)(-y) = xy$ para todo $x, y \in R$.
5) Si $1 = 0$, entonces $|R| = 1$. Este anillo se conoce como el **anillo nulo**.

Si R es un anillo y S es un subconjunto de R, diremos que S es cerrado por multiplicación si $S \cdot S \subseteq S$, es decir $st \in S$ si $s, t \in S$.

Definición 16.7. Sea R un anillo. Un **subanillo** de R es un subconjunto S de R tal que $(S, +)$ es un subgrupo de $(R, +)$, S es cerrado por multiplicación y además $1 \in S$.

Ejemplos 16.8.

1) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ son subanillos.
2) $\mathbb{Z}$ es un subanillo de $\mathbb{Z}$.
3) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$.
4) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es un subanillo de $\mathbb{R}$.

Ejemplo 16.9. Si R es un anillo, $Z(R) = \{x \in R : xy = yx \text{ para todo } y \in R\}$ es un subanillo de R. Se denomina el **centro** de R.

Ejercicio 16.10. Si S es un subanillo de R, entonces $0_S = 0_R$. Además si $x \in S$, el inverso aditivo de x en S coincide con el inverso aditivo de x en R.

Ejercicio 16.11. Si S y T son subanillos de R, entonces $S \cap T$ es también un subanillo de R.

El resultado del ejercicio anterior puede generalizarse a una intersección arbitraria de subanillos.

Ejercicio 16.12. Si $R_1 \subseteq R_2 \subseteq \cdots$ es una sucesión de subanillos de un anillo R, entonces $\cup_{i\geq 1} R_i$ es un subanillo de R.

Definición 16.13. Sea R es un anillo. Un elemento $x \in R$ es una **unidad** si existe $y \in R$ tal que $xy = yx = 1$.

Si un elemento x es una unidad, entonces el inverso y tal que $xy = yx = 1$ es único. Esto nos permite escribir $y = x^{-1}$. El **grupo de unidades** de R se define como

$$\mathscr{U}(R) = \{x \in R : x \text{ es una unidad}\},$$

que forma un grupo con la multiplicación de R.

En anillos no conmutativos conviene distinguir unidades, unidades a derecha y unidades a izquierda, ya que todos estos conceptos son diferentes. Veamos un ejemplo. Sea $R = \mathrm{End}(V)$, donde V es un espacio vectorial con base $e_1, e_2, \ldots$. Sea $f \in R$ tal que $f(e_i) = e_{i+1}$ para todo i y sea $g \in R$ tal que

$$g(e_i) = \begin{cases} 0 & \text{si } i = 1, \\ e_{i-1} & \text{si } i > 1. \end{cases}$$

Entonces $g \circ f = \mathrm{id}$ pero $f \circ g \neq \mathrm{id}$ pues $f(g(e_1)) = f(0) = 0$. Luego f no es una unidad. En caso contrario, existe $h \in R$ tal que $f \circ h = h \circ f = \mathrm{id}$ y entonces

$$g = g \circ \mathrm{id} = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id} \circ h = h,$$

una contradicción.

Definición 16.14. Diremos que un anillo R es de **división** si $\mathscr{U}(R) = R \setminus \{0\}$.

Ejemplo 16.15. Sea

$$R = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Entonces R es un anillo de división no conmutativo con la suma usual y la multiplicación inducida por $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$.

Definición 16.16. Un **cuerpo** es un anillo de división conmutativo tal que $1 \neq 0$.

Ejemplos 16.17. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos. Si p es un número primo, entonces $\mathbb{Z}/p$ es un cuerpo.

Ejemplo 16.18. $\mathbb{Q}[\sqrt{2}] = \{x + \sqrt{2}y : x, y \in \mathbb{Q}\}$ es un cuerpo con las operaciones usuales.

Capítulo 17
Ideales

Definición 17.1. Sea R un anillo. Un subconjunto I de R es un **ideal a izquierda** de R si $(I,+) \leq (R,+)$ y además $RI \subseteq I$ (es decir $xu \in I$ para todo $x \in R$ y $u \in I$).

Análogamente pueden definirse ideales a derecha, simplemente hay que reemplazar la condición $RI \subseteq I$ por $IR \subseteq I$.

Ejemplo 17.2. Si $R = M_2(\mathbb{R})$, entonces

$$I = \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} : x, y \in \mathbb{R} \right\}$$

es un ideal a derecha de R que no es un ideal a izquierda.

Dejamos como ejercicio encontrar un ideal a izquierda de $M_2(\mathbb{R})$ que no sea un ideal a derecha.

Definición 17.3. Sea R un anillo. Un **ideal** es un subconjunto I de R tal que I es simultáneamente un ideal a derecha y a izquierda.

Los ideales de la definición anterior también se llaman **ideales biláteros**.

Ejemplo 17.4. Si $g(X) \in \mathbb{R}[X]$, entonces el conjunto

$$(g(X)) = \{f(X)g(X) : f(X) \in \mathbb{R}[X]\}$$

de múltiplos de $g(X)$ es un ideal de $\mathbb{R}[X]$.

Dejamos como ejercicio verificar los siguientes ejemplos.

Ejemplos 17.5.

1) $\{0\}$ y R son siempre ideales de R.
2) $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.
3) Si $\{I_\lambda : \lambda\}$ es una colección de ideales de R, entonces $\cap_\lambda I_\lambda$ es un ideal de R.
4) Si $I_1 \subseteq I_2 \subseteq \cdots$ es una sucesión de ideales de R, entonces $\cup_{i \geq 1} I_i$ es un ideal de R.

Ejercicio 17.6. Sean R un anillo conmutativo y J, P y Q ideales de R. Pruebe que si $J \subseteq P \cup Q$ entonces $J \subseteq P$ o bien $J \subseteq Q$.

Tal como hicimos para grupos, pueden definirse ideales generados por un subconjunto del anillo R. Por ejemplo, podemos definir el ideal a izquierda generado por el subconjunto X como

$$(X)_L = \bigcap \{I : X \subseteq I, I \text{ ideal a izquierda}\}.$$

Análogamente se define el ideal a derecha $(X)_R$ generado por X. Puede demostrarse que

$$(X)_L = \left\{ \sum_{i=1}^{n} r_i x_i : n \in \mathbb{N}_0, r_1, \ldots, r_n \in R, x_1, \ldots, x_n \in X \right\}.$$

De la misma forma podemos definir el ideal (X) generado por X. En este caso,

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i s_i : n \in \mathbb{N}_0, r_1, \ldots, r_n, s_1, \ldots, s_n \in R, x_1, \ldots, x_n \in X \right\}$$

Ejemplo 17.7. Veamos que los ideales de $\mathbb{Z}/n$ son de la forma (d) con d un divisor de n. En efecto, si d es un divisor de n, entonces (d) es un ideal de $\mathbb{Z}/n$. Demostremos entonces que todo ideal I de $\mathbb{Z}/n$ es de la forma (d) para algún divisor d de n. Como I es en particular un subgrupo del grupo aditivo de $\mathbb{Z}/n$, el teorema de Lagrange nos dice que $m = |I|$ es un divisor de n. Como además el grupo aditivo de $\mathbb{Z}/n$ es cíclico, digamos $\mathbb{Z}/n = \langle 1 \rangle$, el grupo aditivo de I también será cíclico, digamos $I = \langle n/m \rangle$. Luego $I = (n/m)$, donde $d = n/m$ es un divisor de n.

Usaremos ideales para poder definir cocientes. Antes de proceder a explicar esta construcción es conveniente repasar nociones básicas sobre morfismos de anillos.

Definición 17.8. Si R y S son anillos, diremos que una función $f\colon R \to S$ es un morfismo de anillos si $f(1) = 1$, $f(x+y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$ para todo $x, y \in R$.

Si $f\colon R \to S$ es una función tal que $f(x+y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$ para todo $x, y \in R$, no es necesariament cierto que $f(1) = 1$. Se pide esta condición en la definición para evitar patologías. Veremos otra posible explicación en el capítulo 24.

Ejemplo 17.9. Sea $f\colon \mathbb{Z}/6 \to \mathbb{Z}/6$, $f(x) = 3x$. Un cálculo sencillo muestra que $f(x+y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$ para todo $x, y \in \mathbb{Z}/6$, pero $f(1) = 3 \neq 1$.

Tal como hicimos en el caso de grupos, podemos definir el núcleo de un morfismo $f\colon R \to S$ como

$$\ker f = \{x \in R : f(x) = 0\}.$$

Queda como ejercicio demostrar que $\ker f$ es un ideal de R. Además f es inyectivo si y sólo si $\ker f = \{0\}$.

Ejemplos 17.10. Las siguientes funciones son ejemplos de morfismos de anillos:

1) La identidad $\mathrm{id}\colon R \to R$.
2) Las inclusiones $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$.
3) $\mathbb{Z} \to R$, $k \mapsto k1_R$.
4) La evaluación $\mathrm{ev}_{x_0}\colon R[X] \to R$, $f \mapsto f(x_0)$, donde $x_0 \in R$ es un elemento fijo.

Ejemplo 17.11. La función $f\colon \mathbb{Z}[i] \to \mathbb{Z}/5$, $f(a+bi) = a+2b$ mód 5, es un morfismo de anillos. El núcleo de f es el conjunto

$$\ker f = \{a+bi : a+2b \text{ es divisible por } 5\}.$$

Ejercicio 17.12. Sea R un anillo conmutativo y sea $d \in \mathbb{Z}$ libre de cuadrados. Demuestre que $\mathrm{Hom}(\mathbb{Z}[\sqrt{d}], R)$ está en biyección con $\{r \in R : r^2 = d1_R\}$.

El ejercicio anterior nos dice por ejemplo que $\mathrm{Hom}(\mathbb{Z}[i], \mathbb{Z}) = \emptyset$.

Ejemplo 17.13. La función $\mathbb{C} \to \mathbb{R}^{2\times 2}$, $a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, es un morfismo inyectivo de anillos.

La idea del ejemplo anterior nos permite también encontrar un morfismo de anillos $\mathbb{Z}[i] \to \mathbb{Z}^{2\times 2}$.

Ejemplo 17.14. La función $\mathbb{Z} \to 2\mathbb{Z}$, $x \mapsto 2x$, es un morfismo de grupos abelianos pero no es un morfismo de anillos.

Ejemplo 17.15. Sean D un anillo de división y R un anillo no trivial. Si $f\colon D \to R$ es un morfismo de anillos, entonces, como $f(1) = 1 \neq 0$, el núcleo $\ker f$ es un ideal propio de D. Luego f resulta ser inyectivo.

Ejercicio 17.16. Demuestre que los anillos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ no son isomorfos.

Ejercicio 17.17. Demuestre que no hay morfismos de anillos $\mathbb{Z}/6 \to \mathbb{Z}/15$.

Ejercicio 17.18. Demuestre que si $f\colon \mathbb{Q} \to \mathbb{Q}$ es un morfismo de anillos, entonces $f = \mathrm{id}$.

Ejercicio 17.19. Demuestre que si $f\colon \mathbb{R}[X_1, \ldots, X_n] \to \mathbb{R}$ es un morfismo de anillos tal que la restricción $f|_{\mathbb{R}}$ es la identidad, entonces $f = \mathrm{ev}_p$ para algún $p \in \mathbb{R}^n$.

Para definir cocientes de anillos utilizaremos ideales. Si I es un ideal de R, entonces $(I,+)$ es un subgrupo normal de $(R,+)$, pues el grupo aditivo de R es abeliano. Esto implica que R/I es un grupo abeliano con la operación

$$(x+I)+(y+I) = (x+y)+I.$$

Hasta acá, solamente se necesita que $(I,+)$ sea un subgrupo normal de $(R,+)$. Si queremos que R/I sea un anillo, necesitamos determinar cómo tiene que ser el producto. La estrucuturea de anillo sobre R/I tiene que ser tal que el morfismo canónico

$\pi\colon R \to R/I$, $\pi(x) = x+I$, sea un morfismo de anillos. Esto nos dice que la multiplicación tiene que estar dada por

$$(x+I)(y+I) = (xy)+I.$$

Veamos cómo demostrar que esta operación está bien definida.

Usaremos que I es un ideal. Sean $x+I = x_1+I$ e $y+I = y_1+I$. Queremos demostrar que $xy - x_1y_1 \in I$. Como $x - x_1 \in I$ y además I es un ideal a derecha,

$$xy - x_1y = (x-x_1)y \in I. \tag{17.1}$$

Similarmente, como $y - y_1 \in I$ y además I es un ideal a izquierda,

$$x_1y - x_1y_1 = x_1(y-y_1) \in I. \tag{17.2}$$

Entonces, al combinar las fórmula (17.2) con (17.1) y que I es un subgrupo aditivo de R, obtenemos que la multiplicación de R/I está bien definida pues

$$xy - x_1y_1 = xy - x_1y + x_1y - x_1y_1 \in I.$$

Teorema 17.20. *Sea R un anillo. Si I es un ideal de R, entonces existe una única estructura de anillo en R/I tal que $\pi\colon R \to R/I$ es un morfismo de anillos sobreyectivo.*

Demostración. Ya sabemos que las operaciones

$$(x+I)+(y+I) = (x+y)+I, \qquad (x+I)(y+I) = (xy)+I$$

están bien definidas gracias a que I es un ideal de R. Sabemos también que $(R/I,+)$ es un grupo abeliano. Nos queda por demotrar entonces que R/I es un anillo, algo que dejaremos como ejercicio. □

Ejemplo 17.21. Sea $R = (\mathbb{Z}/3)[X]$ y sea $I = (2X^2+X+2)$. Sabemos que todo $f \in R$ se escribe como

$$f = (2X^2+2X+2)q + r,$$

donde $q, r \in R$ y $r = 0$ o bien $\deg r < 2$. Podemos escribir entonces $r = aX+b$ para ciertos $a, b \in \mathbb{Z}/3$. Esto nos dice que entonces

$$f+I = ((2X^2+2X+2)q+r)+I = (aX+b)+I.$$

Como $a, b \in \mathbb{Z}/3$, tenemos entonces nueve posibilidades. Luego $|R/I| = 9$.

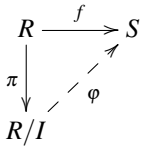
Como ejemplo, calculemos $((2X+1)+I)((X+1)+I)$. En efecto, si usamos el algoritmo de división,

$$(2X+1)(X+1) = 2X^2+3X+1 = 2X^2+1 = (2X^2+X+2)\cdot 1 + (2X+2)$$

y luego $(2X^2+1)+I = (2X+2)+I$.

Valen además los teoremas de isomorfismos. Dado que no hay mucha diferencia entre lo que se hizo en el caso de grupos y lo que debe hacerse en el caso de anillos, enunciaremos los teoremas más importantes y dejaremos las demostraciones como ejercicio.

Teorema 17.22. *Sea $f\colon R \to S$ un morfismo de anillos y I un ideal de R tal que $I \subseteq \ker f$. Existe entonces un único morfismo $\varphi\colon R/I \to S$ tal que el diagrama*



es conmutativo, lo que significa que $\varphi \circ \pi = f$, donde $\pi\colon R \to R/I$ es el morfismo canónico. Más aún, $\ker \varphi = \ker f/I$ *y* $\varphi(R/I) = f(R)$. *En particular, φ es inyectiva si y sólo si* $\ker f = I$ *y φ es sobreyectiva si y sólo si f es sobreyectiva.*

Demostración. Queda como ejercicio, ya que es muy similar a la demostración hecha en el caso de grupos. □

Como corolario obtenemos:

Corolario 17.23 (primer teorema de isomorfismos). *Si $f\colon R \to S$ es un morfismo de anillos, entonces* $R/\ker f \simeq f(R)$.

Veamos algunas aplicaciones del primer teorema de isomorfismos.

Ejemplo 17.24. Con el morfismo $\mathbb{R}[X] \to \mathbb{C}$, $f \mapsto f(i)$, se demuestra que

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}.$$

Ejemplo 17.25. Con el morfismo $\mathbb{Z}[X] \to (\mathbb{Z}/7)[X]$, $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a_i} X^i$, donde $\overline{a}$ es a módulo 7, se demuestra que

$$\mathbb{Z}[X]/(7) \simeq (\mathbb{Z}/7)[X].$$

Ejemplo 17.26. Sea R el anillo de funciones continuas $[0,2] \to \mathbb{R}$. Veamos que el conjunto $I = \{f \in R : f(1) = 0\}$ es un ideal de R y calculemos el cociente R/I. Para ver que I es un ideal consideramos la evaluación $\varphi\colon R \to \mathbb{R}$, $\varphi(f) = f(1)$. Sabemos que φ es un morfismo de anillos y además podemos verificar que

$$\ker \varphi = \{f \in R : \varphi(f) = 0\} = \{f \in R : f(1) = 0\} = I.$$

Como φ es sobreyectiva (basta tomar funciones constantes), el teorema de isomorfismos implica que $R/I \simeq \mathbb{R}$.

Ejemplo 17.27. Sea R el anillo de matrices de la forma $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, donde $a, b \in \mathbb{Q}$. La función

$$f\colon R \to \mathbb{Q}, \quad \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a,$$

es un morfismo sobreyectivo de anillos tal que $I = \ker f$ es el ideal formado por las matrices de la forma $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, donde $b \in \mathbb{Q}$. Entonces $R/I \simeq \mathbb{Q}$.

Ejemplo 17.28. Sea $R = \mathbb{Z}[\sqrt{10}]$ y sea

$$I = (2, \sqrt{10}) = \{a + b\sqrt{10} : a \equiv 0 \text{ mód } 2\}.$$

La función

$$f\colon R \to \mathbb{Z}/2, \quad a + b\sqrt{10} \mapsto a \text{ mód } 2,$$

es un morfismo sobreyectivo tal que $\ker f = I$. Luego $R/I \simeq \mathbb{Z}/2$.

Ejemplo 17.29. Si I es un ideal de R, entonces $M_n(I)$ es un ideal de $M_n(R)$ y además $M_n(R)/M_n(I) \simeq M_n(R/I)$. Un cálculo sencillo muestra que $M_n(I)$ es un subgrupo de $M_n(R)$. Además si $a = (a_{ij}) \in M_n(R)$ y $y \in M_n(I)$, entonces

$$(ay)_{ij} = \sum_{k=1}^{n} a_{ik} y_{kj} \in I$$

para todo $i, j \in \{1, \ldots, n\}$. Similarmente vemos que $ya \in M_n(I)$. Sea $\pi\colon R \to R/I$ el morfismo canónico y sea $\varphi\colon M_n(R) \to M_n(I)$, $(a_{ij}) \mapsto (\pi(a_{ij}))$. Entonces φ es un morfismo sobreyectivo de anillos tal que

$$\ker \varphi = \{(a_{ij}) \in M_n(R) : a_{ij} \in I \text{ para todo } i, j \in \{1, \ldots, n\}\}.$$

Por el primer teorema de isomorfismos, $M_n(R)/M_n(I) \simeq M_n(R/I)$.

Ejemplo 17.30. Vamos a demostrar que $\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/10$. Sea f la composición

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[i] \xrightarrow{\pi} \mathbb{Z}[i]/(1+3i),$$

donde π es el morfimso canónico. Claramente f es morfismo de anillos por ser composición de morfismos.

Veamos que f es sobreyectiva. Para eso, alcanza con encontrar un entero $b \in \mathbb{Z}$ tal que $f(b) = i$, es decir: queremos $b \in \mathbb{Z}$ tal que $b - i \in (1+3i)$. Observemos que

$$b - i \in (1+3i) \iff b - i = (1+3i)(x+yi) = (x-3y) + i(3x+y)$$

para $x, y \in \mathbb{Z}$. Si tomamos $x = 1$, $y = -4$ y $b = 13$, entonces vemos que f es sobreyectiva pues $f(a+13b) = f(a) + f(b)f(13) = a + bi$.

Calculemos ahora el núcleo de f. Afirmamos que $\ker f = (10)$. Primero observamos que, como $10 = (1+3i)(1-3i)$, entonces $f(10) = \pi(1+3i)\pi(1-3i) = 0$ y luego $(10) \subseteq \ker f$. Recíprocamente, si $m \in \ker f$, entonces $m \in (1+3i)$, es decir

$$m = (1+3i)(x+iy) = (x-3y) + i(3x+y)$$

para ciertos $x, y \in \mathbb{Z}$. Pero entonces $3x + y = 0$, lo que implica que $y = -3x$ y que entonces $m = x - 3(-x) = 10x$, es decir $m \in (10)$. En conclusión, por el primer teorema de isomorfismos de anillos, $\mathbb{Z}/(1+3i) \simeq \mathbb{Z}/10$.

Ejercicio 17.31. Demuestre que $\mathbb{Z}[i]/(2+3i) \simeq \mathbb{Z}/13$.

Ejercicio 17.32. Demuestre que no existe un ideal I de $\mathbb{Z}[i]$ tal que $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

Teorema 17.33. *Si $f\colon R \to S$ es un morfismo sobreyectivo de anillos con $K = \ker f$, existe una correspondencia biyectiva entre los ideales de R que contienen a K y los ideales de S. La correspondencia está dada por $I \mapsto f(I)$ y $f^{-1}(J) \hookleftarrow J$. Más aún, si $f(I) = J$, entonces $R/I \simeq S/J$.*

Bosquejo de la demostración. Hay que demostrar las siguientes afirmaciones:

1) $f(I) \subseteq S$ es un ideal.
2) $f^{-1}(J) \subseteq R$ es un ideal que contiene a K.
3) $f(f^{-1}(J)) = J$ y además $f^{-1}(f(I)) = I$.
4) Si $f(I) = J$, entonces $R/I \simeq S/J$.

Las primeras tres afirmaciones quedarán como ejercicio. Demostremos (4). Primero obervamos que la tercera afirmación implica que $f(I) = J$ si y sólo si $I = f^{-1}(J)$. Sea $\pi\colon S \to S/J$ el morfismo canónico y sea $g = \pi \circ f$. Como

$$\ker g = \{x \in R : g(x) = 0\} = \{x \in R : f(x) \in J\} = \{x \in R : x \in f^{-1}(J) = I\} = I,$$

existe un morfismo de anilos $h\colon R/I \to S/J$ tal que $h \circ p = g$, donde $p\colon R \to R/I$ es el morfismo canónico. Dejamos como ejercicio verificar que h es biyectivo. □

Definición 17.34. Un ideal I de R se dice **principal** si existe $x \in R$ tal que $I = (x)$.

Análogamente pueden definirse ideales a izquierda principales e ideales a derecha principales.

Ejemplo 17.35. Todo ideal de $\mathbb{Z}$ es principal.

Ejercicio 17.36. Sea I un ideal (a izquierda) de R. Demuestre que $I = R$ si y sólo si existe $x \in I \cap \mathscr{U}(R)$.

El ejercicio anterior nos permite demostrar que un anillo R es de división si y sólo si R admite únicamente dos ideales a izquierda.

Observación 17.37. $u \in \mathscr{U}(R) \iff (u) = R$.

Capítulo 18
Polinomios

Sea R un anillo conmutativo. Un polinomio con coeficientes en R es una expresión de la forma

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^{n} a_n X^i,$$

donde $n \in \mathbb{N}_0$. El conjunto de polinomios en una variable con coeficientes en R será denotado por $R[X]$.

Diremos que f y $g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$ son iguales si y sólo si $a_i = b_i$ para todo $i \in \{0, 1, \ldots, n\}$.

El grado de un polinomio $f = \sum_{i=0}^{n} a_i X^i$ se define como el menor entero positivo tal que $a_n \neq 0$. Un polinomio de grado cero será denominado **polinomio constante**.

Un polinomio $f = \sum_{i=0}^{n} a_i X^i$ de grado n se dice **mónico** si su **coeficiente principal** es igual a uno, es decir $a_n = 1$. Si

$$f = \sum a_i X^i, \quad g = \sum b_j X^j,$$

donde omitimos los índices de la sumatoria para aliviar un poco la notación, se definen la suma y el producto como

$$f + g = \sum (a_k + b_k) X^k, gh = \sum \sum a_i b_j X^{i+j}.$$

Con estas operaciones, $R[X]$ es un anillo conmutativo. Además R puede pensarse como un subanillo de $R[X]$ pues existe un morfismo inyectivo de anillos $R \to R[X]$.

Ejemplo 18.1. Si f es un polinomio mónico y g es un polinomio, existen entonces únicos $q \in R[X]$ y $r \in R[X]$ tales que

$$g = fq + r,$$

donde $r = 0$ o bien $\deg r < \deg f$. Por ejemplo, si

$$f = X^5 + X^4 - 3X^3 + 4X^2 + 2X, \quad g = X^4 + 3X^3 - X^2 - 6X - 2$$

entonces $q = X - 2$ y $r = 4X^3 + 8X^2 - 8X - 4$ pues

$$f = (X-2)g + (4X^3 + 8X^2 - 8X - 4).$$

El algoritmo de división podrá hacerse siempre que el coeficiente principal de f sea una unidad del anillo R. En particular, siempre podremos utilizar el algoritmo de división cuando el anillo R es en realidad un cuerpo y $f \neq 0$.

Proposición 18.2. *Si $g \in R[X]$ y $\alpha \in R$, el resto de dividir al polinomio g por $X - \alpha$ es $g(\alpha)$. En particular, $X - \alpha$ divide al polinomio g en $R[X]$ si y sólo si $g(\alpha) = 0$.*

Demostración. Hay que evaluar en α la expresión $g = (X - \alpha)q + r$. □

Como corolario puede demostrarse que todo $f \in R[X]$ no nulo tiene a lo sumo $\deg f$ raíces en R.

Proposición 18.3. *Sea $\varphi\colon R \to S$ un morfismo de anillos y sea $\alpha \in S$. Existe un único morfismo de anillos $\Phi\colon R[X] \to S$ tal que $\Phi(X) = \alpha$ y tal que Φ coincide con φ en los polinomios constantes.*

Bosquejo de la demostración. Si $f = \sum a_i X^i$, definimos

$$\Phi(f) = \Phi(\sum a_i X^i) = \sum \Phi(a_i)\Phi(X)^i = \sum \Phi(a_i)\alpha^i,$$

y así Φ quedaría unívocamente determinado. Dejamos como ejercicio demostrar que Φ es un morfismo de anillos. □

Ejemplo 18.4. Sea $\varphi\colon \mathbb{R}[X] \to \mathbb{R}$, $X \mapsto 2$. Entonces $\ker\varphi$ es el ideal $(X-2)$ de $\mathbb{R}[X]$ generado por $X - 2$ pues

$$\ker\varphi = \{g \in \mathbb{R}[X] : g(2) = 0\} = \{g \in \mathbb{R}[X] : g = (X-2)q \text{ para algún } q \in \mathbb{R}[X]\}.$$

El resultado que sigue es análogo al teorema 1.32.

Teorema 18.5. *Sea K un cuerpo. Todo ideal de $K[X]$ es principal. Más aún, todo ideal I no nulo de $K[X]$ está generado por el único polinomio mónico de menor grado que está contenido en I.*

Demostración. Sea I un ideal de $K[X]$. Si $I = \{0\}$, entonces I es principal. Supongamos que $I \neq \{0\}$ y sea $f \in I \setminus \{0\}$ de grado mínimo. Sin perder generalidad, podemos suponer que f es mónico pues si no lo fuera, digamos $f = a_n X^n + \cdots$ con $a_n \neq 0$, entonces solamente hay que reemplaar a f por el polinomio $a_n^{-1} f$.

Veamos que $I = (f)$. Vamos a demostrar la inclusión no trivial. Sea $g \in I$. Escribimos $g = fq + r$ para ciertos $q, r \in K[X]$, donde $r = 0$ o bien $\deg r < \deg f$. Si $r \neq 0$, entonces $r = g - fq \in I$, una contradicción a la minimalidad del grado de f. Luego $r = 0$ y entonces f divide a g, es decir $g \in (f)$. □

Diremos que un polionomio $f \in \mathbb{Z}[X]$ se dice **irreducible** si f no es constante y $f = gh$ implica que g o h son constantes. De la misma forma podemos definir polinomios irreducibles en $\mathbb{Q}[X]$.

Los polinomios de grado uno son irreducibles.

Ejemplo 18.6. , Sea $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ y sea $a \in K$. Entonces f es irreducible si y sólo si $f(X+a) = \sum_{i=0}^{n} a_i (X+a)^i$ es irreducible, pues

$$T_a \colon K[X] \to K[X], g \mapsto g(X+a),$$

es isomorfismo de anillos y manda irreducibles en irreducibles.

Un polinomio $f \in \mathbb{Z}[X]$ se dice **primitivo** si el máximo común divisor de sus coeficientes es igual a uno.

Lema 18.7 (Gauss). *Sean $f, g \in \mathbb{Z}[X]$. Si f y g son primitivos, entonces fg es primitivo.*

Demostración. Sean $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$. Supongamos que fg no es primitivo y sea p un primo que divide a todos los coeficientes de fg. Como f y g son primitivos, p no divide a los coeficientes de f ni divide a los coeficientes de g. Sean $i \in \{0, \ldots, n\}$ y $j \in \{0, \ldots, m\}$ minimales tales que $p \nmid a_i$ y $p \nmid b_j$. Si c_{i+j} es el coeficiente de X^{i+j} en fg, entonces

$$c_{i+j} = \sum_{k>i} a_k b_{i+j-k} + \sum_{k<i} a_k b_{i+j-k} + a_i b_j.$$

Luego p divide a $\sum_{k>i} a_k b_{i+j-k} + \sum_{k<i} a_k b_{i+j-k}$ pero no divide al entero $a_i b_j$, es decir no divide a c_{i+j}, una contradicción. □

Teorema 18.8 (Gauss). *Sea $f \in \mathbb{Z}[X]$ un polinomio no constante y primitivo. Entonces f es irreducible en $\mathbb{Z}[X]$ si y sólo si f es irreducible en $\mathbb{Q}[X]$.*

Demostración. Demostremos la implicación no trivial. Vamos a demostrar que f es reducible en $\mathbb{Z}[X]$. Supongamos que $f = gh$ con $g, h \in \mathbb{Q}[X]$ de grado positivo. Al multiplicar por un número racional adecuado, podemos suponer que

$$f = \frac{a}{b} g_1 h_1,$$

donde $\mathrm{mcd}(a,b) = 1$ y $g_1, h_1 \in \mathbb{Z}[X]$ son polinomios primitivos, es decir $bf = ag_1h_1$. Luego el máximo común divisor de los coeficientes de bf es b. Como g_1h_1 es primitivo por el lema de Gauss, el máximo común divisor de los coeficientes de ag_1h_1 es a. Luego $a = b$ o $a = -b$, es decir $f = g_1h_1$ o $f = -g_1h_1$ en $\mathbb{Z}[X]$. □

Teorema 18.9 (Eisenstein). *Sea $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ primitivo de grado n. Si existe un primo p tal que $p \mid a_j$ para $j \in \{0, \ldots, n-1\}$, $p \nmid a_n$ y $p^2 \nmid a_0$, entonces f es irreducible en $\mathbb{Z}[X]$.*

Demostración. Escribimos $f = gh$ con $g = \sum_{i=0}^{k} b_i X^i$ y $h = \sum_{i=0}^{l} c_i X^i$, donde suponemos que $b_k \neq 0$ y $c_l \neq 0$. Como $p \mid a_0$, $p^2 \nmid a_0$ y $a_0 = b_0 c_0$, entonces p divide a b_0 o p divide a c_0, pero no a ambos. Supongamos que $p \mid b_0$ y que $p \nmid c_0$. Como $n = k + l$ y $p \nmid a_n = b_k c_l$, entonces $p \nmid b_k$. Sea $j \in \{1, \ldots, k\}$ maximal tal que $p \mid b_i$ para todo $i < j$ y $p \nmid b_j$. Entonces

$$a_j = b_j c_0 + \underbrace{b_{j-1}c_1 + \cdots + b_0 c_j}_{\text{divisible por } p}$$

se concluye que $p \nmid b_j c_0$ y luego $p \nmid a_j$. En conclusión, $j = n$ y entonces $k = n$ y h es constante. □

Ejemplo 18.10. El polinomio $X^5 + 16X + 2 \in \mathbb{Z}[X]$ es irreducible.

Ejemplo 18.11. Sea p un número primo. Veamos que $f = X^{p-1} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$. Escribimos $(X-1)f = X^p - 1$ y aplicamos el isomorfismo de anillos $T_1 : g \mapsto g(X+1)$ que vimos en el ejemplo 18.6,

$$XT_1(f) = (X+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i$$

y luego $T_1(f) = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$. Como $p \mid \binom{p}{i}$ para todo $i \in \{1, \ldots, p-1\}$ y además $p^2 \nmid \binom{p}{1} = p$, entonces el criterio de Eisenstein implica que $T_1(f)$ es irreducible. Luego f es también irreducible.

Nos interesará también estudiar anillos de polinomios en varias variables. Un **monomio** en las variables $X_1, \ldots, X_n$ es un producto de la forma

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

donde $i_1, \ldots, i_n \geq 0$. A veces conviene utilizar la siguiente notación: si $i = (i_1, \ldots, i_n)$, entonces

$$X^i = X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}.$$

El monomio X^0, donde $0 = (0, 0, \ldots, 0)$, será denotado por 1.

Un polinomio en las variables $X_1, \ldots, X_n$ con coeficientes en R es una combinación lineal (sobre R) de finitos monomios, es decir

$$f = f(X_1, \ldots, X_n) = \sum a_i X^i,$$

donde la suma se recorre sobre todos los multi-índices $i = (i_1, \ldots, i_n)$, los coeficientes a_i son elementos del anillo R y solamente finitos de esos coeficientes son distintos de cero. El conjunto de los polinomios en las variables $X_1, \ldots, X_n$ con coeficientes en R será denotado por $R[X_1, \ldots, X_n]$.

Ejercicio 18.12. Demuestre que la proposición 18.3 vale también en el caso de polinomios en varias variables.

Ejemplo 18.13. Si R es un anillo, $R[X]$ es un anillo. Podemos considerar entonces el anillo de polinomios $R[X,Y] = (R[X])(Y) = R[X][Y]$. Sabemos que si utilizamos las identificaciones pertinentes, podemos pensar que $R \subseteq R[X] \subseteq (R[X])[Y]$ son subanillos. Si $\varphi \colon R \to R[X][Y]$ la inclusión, existe entonces un único morfismo de anillos $\Psi \colon R[X,Y] \to R[X][Y]$ que extiende a φ y tal que $\Psi(X) = X$ y $\Phi(Y) = Y$. Puede demostrarse que Ψ es biyectivo y luego, en consecuencia,

$$R[X,Y] \simeq R[X][Y].$$

Ejemplo 18.14. Veamos que $\mathbb{R}[X,Y]/(X) \simeq \mathbb{R}[Y]$. Consideramos el morfismo sobreyectivo $\varphi\colon \mathbb{R}[X,Y] \to \mathbb{R}[Y]$, $\varphi(f(X,Y)) = f(0,Y)$. Afirmamos que $\ker\varphi = (X)$. En efecto, para probar que $\ker\varphi \subseteq (X)$ observamos que si

$$f(X,Y) = f_0(Y) + f_1(Y)X + \cdots + f_n(Y)X^n,$$

donde $f_i(Y) \in \mathbb{R}[Y]$ para todo $i \in \{0,1,\ldots,n\}$, entonces

$$0 = \varphi(f(X,Y)) = f(0,Y) = f_0(Y).$$

Luego $f(X,Y) = f_1(Y)X + \cdots + f_n(Y)X^n = X(f_1(Y) + \cdots + f_n(Y)X^{n-1}) \in (X)$. La otra inclusión es trivial. El primer teorema de isomorfismos, entonces, implica que $\mathbb{R}[X,Y]/(X) \simeq \mathbb{R}[Y]$.

Ejercicio 18.15. Demuestre que $\mathbb{R}[X]/(X^2-1) \simeq \mathbb{R} \times \mathbb{R}$.

Ejercicio 18.16. Demuestre que $\mathbb{Q}[X]/(X-2) \simeq \mathbb{Q}$.

Capítulo 19
El teorema chino del resto

En este capítulo veremos una generalización del conocido teorema chino del resto válida para anillos conmutativos. Empezaremos con algunas observaciones básicas. Primero observamos que si I y J son ideales de R, entonces

$$I+J=\{u+v : u\in I,\, v\in J\}$$

es también un ideal de R.

Definición 19.1. Sea R un anillo conmutativo y sean I y J ideales de R. Diremos que I y J son **coprimos** si $I+J=R$.

La terminología está justificada por la siguiente observación.

Ejemplo 19.2. Si $R=\mathbb{Z}$, $I=(a)$ y $J=(b)$, entonces I y J serán coprimos si y sólo si existen $r,s\in\mathbb{Z}$ tales que $ra+sb=1$, es decir si y sólo si $\mathrm{mcd}(a,b)=1$.

Si I y J son ideales de R, entonces

$$IJ=\left\{\sum_{i=1}^{m} u_i v_i : m\in\mathbb{N}_0,\, u_i\in I,\, v_i\in J\right\}$$

es también un ideal de R. Vale además que $IJ\subseteq I\cap J$. La igualdad no siempre vale, tal como nos muestra el siguiente ejemplo.

Ejemplo 19.3. Si $R=\mathbb{Z}$ y además $I=J=(2)$, entonces $IJ=(4)\subsetneq(2)=I\cap J$.

Sin embargo, si I y J son ideales coprimos de un anillo conmutativo R, entonces $IJ=I\cap J$. En efecto, para demostrar la inclusión no trivial, sea $x\in I\cap J$. Entonces $1=u+v$ para ciertos $u\in I$ y $v\in J$ pues los ideales son coprimos, y luego

$$x=x1=x(u+v)=xu+xv\in IJ.$$

Teorema 19.4 (teorema chino del resto). *Sea R un anillo conmutativo y sean I y J ideales coprimos de R. Si $u,v\in R$, existe $x\in R$ tal que $\pi_I(x)=\pi_I(u)$ y $\pi_J(x)=\pi_J(v)$, donde $\pi_I\colon R\to R/I$ y $\pi_J\colon R\to R/J$ son los morfismos canónicos.*

Demostración. Como I y J son coprimos, existen $a \in I$ y $b \in J$ tales que $1 = a+b$. Si $x = av+bu$, entonces

$$x-u = av+(b-1)u = av-au = a(v-u) \in I.$$

Similarmente, $x-v \in J$. Luego $\pi_I(x-u) = 0$ y entonces $\pi_I(x) = \pi_I(u)$. Análogamente, como $\pi_J(x-v) = 0$, se tiene que $\pi_J(x) = \pi_J(v)$. □

Si escribimos $x \equiv u$ mód $I \iff x-u \in I$ y $x \equiv v$ mód $J \iff x-v \in J$, entonces el teorema chino del resto garantinza la existencia de $x \in R$ tal que

$$\begin{cases} x \equiv u \text{ mód } I, \\ x \equiv v \text{ mód } J. \end{cases}$$

Corolario 19.5. *Si R es un anillo conmutativo y I y J son ideales coprimos de R, entonces $R/(I \cap J) \simeq (R/I) \times (R/J)$.*

Demostración. Sea $f\colon R \to (R/I) \times (R/J)$, $f(a) = (\pi_I(a), \pi_J(a))$. Claramente, f es un morfismo tal que $\ker f = I \cap J$. Gracias al teorema anterior, f es sobreyectivo. En efecto, Si $(u+I, v+J) \in R/I \times R/J$, entonces existe $x \in R$ tal que $x-u \in I$ y $x-v \in J$, es decir $f(x) = (u+I, v+J)$. El primer teorema de isomorfismos concluye la demostración. □

Veamos qué pasa con el resultado anterior en el caso particular $R = \mathbb{Z}$. Sean $a, b \in \mathbb{Z}$ tales que $\text{mcd}(a,b) = 1$. Si $u, v \in \mathbb{Z}$, entonces, al utilizar el corolario con $I = (a)$ y $J = (b)$, tenemos garantizada la existencia de $x \in \mathbb{Z}$ tal que

$$\begin{cases} x \equiv u \text{ mód } a, \\ x \equiv v \text{ mód } b, \end{cases}$$

para todo $u, v \in \mathbb{Z}$.

Ejercicio 19.6. Si $I_1, \ldots, I_n$ son ideales de un anillo conmutativo R, entonces

$$I_1 \cdots I_n = \left\{ \sum_{j=1}^{m} a_{1j} \cdots a_{nj} : m \in \mathbb{N}_0, a_{ij} \in I_i, 1 \leq j \leq m, 1 \leq i \leq n \right\}$$

es un ideal de R. Puede demostrarse además que si I_1 es un ideal coprimo con I_j para todo $j \in \{2, \ldots, n\}$ entonces I_1 y $I_2 \cdots I_n$ son también ideales coprimos.

El ejercicio anterior nos permite extender el teorema chino del resto a finitos ideales. Supongamos que R es un anillo conmutativo y que $I_1, \ldots, I_n$ son ideales de R tales que I_i e I_j son coprimos siempre que $i \neq j$. Si $x_1, \ldots, x_n \in R$, puede demostrarse que entonces existe $x \in R$ tal que $\pi_i(x_i) = \pi_i(x)$ para todo $i \in \{1, \ldots, n\}$, donde $\pi_i\colon R \to R/I_i$ es el morfismo canónico. En este caso, además,

$$R/(I_1 \cap \cdots \cap I_n) \simeq (R/I_1) \times \cdots \times (R/I_n).$$

Un hecho sorprendente. El teorema de interpolación de Lagrange es en realidad un caso particular del teorema chino del resto en el anillo de polinomios $R = \mathbb{R}[X]$. En efecto, si $x_1, \ldots, x_k \in \mathbb{R}$ son tales que $x_i \neq x_j$ y fijamos elementos $y_1, \ldots, y_k \in \mathbb{R}$, entonces, gracias a la versión abstracta del teorema chino del resto aplicado a los ideales coprimos $I_j = (X - x_j)$ para $j \in \{1, \ldots, k\}$, se garantizará la existencia de una solución f (única módulo el ideal generado por $(X - x_1) \cdots (X - x_k)$) del sistema

$$\begin{cases} f \equiv y_1 \text{ mód } (X - x_1), \\ f \equiv y_1 \text{ mód } (X - x_2), \\ \quad \vdots \\ f \equiv y_1 \text{ mód } (X - x_k). \end{cases}$$

El sistema tendrá en particular una única solución de grado $k - 1$, que es lo que conocemos como el polinomio interpolador de Lagrange.

Capítulo 20
Anillos noetherianos

Definición 20.1. Sea R un anillo. Diremos que R es **noetheriano** si toda sucesión de ideales $I_1 \subseteq I_2 \subseteq \cdots$ de R se estabiliza, es decir que existe $m \in \mathbb{N}$ tal que $I_n = I_m$ para todo $n \geq m$.

Análogamente se definen anillos noetherianos a izquierda y a derecha.

Ejemplo 20.2. $\mathbb{Z}$ es noetheriano.

Ejemplo 20.3. Sea R el anillo de funciones $[0,1] \to \mathbb{R}$ con las operaciones

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x), \quad f,g \in R, x \in [0,1].$$

Para cada $n \in \mathbb{N}$ sean

$$I_n = \{f \in R : f|_{[0,1/n]} = 0\}.$$

Como $I_1 \subsetneq I_2 \subsetneq \cdots$ no se estabiliza, R no es noetheriano.

Teorema 20.4. *Sea R un anillo. Entonces R es noetheriano si y sólo si todo ideal de R es finitamente generado.*

Demostración. Vamos a demostrar primero que vale $\implies$. Sea I un ideal de R que no es finitamente generado. En particular, $I \neq \{0\}$. Existe entonces $x_1 \in I \setminus \{0\}$. Si $I_1 = (x_1)$, entonces $\{0\} \subsetneq I_1 \subsetneq I$. Si los ideales $I_0, I_1, \ldots, I_{k-1}$ fueron construidos, sea $x_k \in I \setminus I_{k-1}$ y sea $I_k = (x_1, \ldots, x_k)$. De esta forma pudimos construir una sucesión

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

que no se estabiliza.

Demostremos ahora la recíproca. Supongamos que tenemos una sucesión

$$I_0 \subsetneq I_1 \subsetneq I_2 \cdots$$

de ideales de R. Vimos que entonces $I = \cup_{i \geq 0} I_i$ es un ideal de R. Como por hipótesis todo ideal es finitamente generado, podemos escribir $I = (x_1, \ldots, x_n)$ para ciertos

$x_1,\dots,x_n \in R$. Sin perder generalidad podemos suponer además que $x_j \in I_{i_j}$ para todo $j \in \{1,\dots,n\}$. Si $N = \max\{i_1,\dots,i_n\}$ y $n \geq N$, entonces $I_N \subseteq I \subseteq I_N \subseteq I_n$ y el resultado queda demostrado. □

Ejemplo 20.5. Todo anillo de ideales principales es noetheriano. En particular, $\mathbb{Z}$, $\mathbb{Z}/n$ y $\mathbb{R}[X]$ son noetherianos.

Ejercicio 20.6. Sea R un anillo noetheriano. Si I es un ideal de R, entonces R/I también es noetheriano.

Teorema 20.7 (Hilbert). *Si R es noetheriano entonces $R[X]$ también lo es.*

Demostración. Tenemos que demostrar que todo ideal I de $R[X]$ es finitamente generado. Supongamos entonces que existe un ideal I que no es finitamente generado. En particular, I es no nulo. Sea $f_1 \in I$ de grado mínimo. Como I no es finitamente generado, para $i > 1$ existe $f_i \in I$ de menor grado tal que $f_i \notin (f_1,\dots,f_{i-1})$. Para cada i, sea a_i el coeficiente principal del polinomio f_i, es decir

$$f_i = a_i X^{n_i} + \cdots \text{ (términos de grado menor)},$$

lo que implica que $a_i \neq 0$ y que $\deg f_i = n_i$. Sea $J = (a_1, a_2, \dots)$ el ideal generado por los coeficientes principales de los f_i. Como R es noetheriano, podemos suponer sin perder generalidad que $J = (a_1,\dots,a_m)$ para algún m. Luego

$$a_{m+1} = \sum_{i=1}^{m} u_i a_i$$

para ciertos $u_1,\dots,u_m \in R$. En particular, el coeficiente principal del polinomio

$$g = \sum_{i=1}^{m} u_i f_i X^{\deg(f_{m+1})-n_i} \in (f_1,\dots,f_m).$$

es entonces a_{m+1} y además $\deg(g) = \deg(f_{m+1})$ pues

$$g = \sum_{i=1}^{m} u_i (a_i X^{n_i} + \cdots) X^{\deg(f_{m+1})-n_i} = \sum_{i=1}^{m} u_i a_i (X^{\deg(f_{m+1})} + \cdots)$$

donde los puntos suspensivos representantes un polinomio de grado $< n_i$. Observemos que $g - f_{m+1} \notin (f_1,\dots,f_m)$, pues por construcción $f_{m+1} \notin (f_1,\dots,f_m)$. Además $\deg(g - f_{m+1}) < \deg(f_{m+1})$, una contradicción a la minimalidad del grado de f_{m+1}. □

Corolario 20.8. *Si R es un anillo noetheriano, entonces $R[X_1,\dots,X_n]$ también es noetheriano.*

Bosquejo de la demostración. La demostración quedará como ejercicio, hay que utilizar inducción y que $R[X_1,\dots,X_{n-1}][X_n] \simeq R[X_1,\dots,X_n]$. □

Veamos algunas aplicaciones sencillas.

Ejemplo 20.9. $\mathbb{Z}[\sqrt{N}]$ es noetheriano pues $\mathbb{Z}[\sqrt{N}] \simeq \mathbb{Z}[X]/(X^2 - N)$ y $\mathbb{Z}[X]$ es noetheriano gracias al teorema de Hilbert.

Ejemplo 20.10. $\mathbb{Z}[X, X^{-1}] \simeq \mathbb{Z}[X,Y]/(XY - 1)$ es noetheriano ya que $\mathbb{Z}[X,Y]$ es noetheriano por el teorema de Hilbert.

Proposición 20.11. *Si R es noetheriano y $f\colon R \to R$ es un morfismo de anillos sobreyectivo, entonces f es un isomorfismo.*

Demostración. Si escribimos $f^n = f \circ \cdots \circ f$ (n-veces), entonces f^n es sobreyectivo. Para cada n sea $K_n = \ker(f^n)$. Entonces

$$K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

es una sucesión de ideales de R. Como R es noetheriano, $K_m = K_{m+1}$ para algún m. Sea $y \in \ker f = K_1$. Como f^m es sobreyectivo, $y = f^m(x)$ para algún $x \in R$. Entonces $0 = f(y) = f(f^m(x))$ y luego

$$x \in \ker(f^{m+1}) = K_{m+1} = K_m = \ker f^m,$$

es decir $y = 0$ y luego $\ker f = \{0\}$. □

Veamos ahora un ejemplo de ideal no finitamente generado.

Ejemplo 20.12. Sea $R = \mathbb{C}[X_1, X_2, \dots]$ es anillo de polinomios en infinitas variables. Vamos a demostrar que el ideal $I = (X_1, X_2, \dots)$ generado por esas infinitas variables no es finitamente generado. Observemos que I es el conjunto de polinomios con término constante nulo.

Si I fuera finitamente generado, digamos $I = (f_1, \dots, f_n)$ para ciertos f_i, hay que observar que cada f_i involucra únicamente una cantidad finita de variables, por lo que entonces existe $m \in \mathbb{N}$ tal que todas las X_i aparecen en alguno de los $f_1, \dots, f_n$ con $i < m$. Sea $\varphi\colon R \to \mathbb{C}$ dado por

$$\varphi(X_i) = \begin{cases} 0 & \text{si } i < m, \\ 1 & \text{si } i \geq m. \end{cases}$$

Entonces $\varphi(f_i) = 0$ para todo $i \in \{1, \dots, n\}$, lo que implica que $\varphi(I) = 0$. Por otro lado, $\varphi(X_m) = 1$, lo que implica que $X_m \notin I$, una contradicción.

Ejercicio 20.13. Si R es noetheriano, entonces $R[[X]]$ es noetheriano.

Capítulo 21
Factorización

Nuestro objetivo es utilizar ciertos aspectos de la teoría de anillos conmutativos para demostrar algunos resultados de la teoría de números. La idea básica será intentar reconocer similitudes entre ciertos anillos conmutativos y $\mathbb{Z}$. Comenzaremos entonces estudiando divisibilidad en anillos conmutativos.

Definición 21.1. Un anillo conmutativo R será un **dominio íntegro** si $xy = 0 \implies x = 0$ o bien $y = 0$.

Ejemplo 21.2. $\mathbb{Z}$ es un dominio íntegro y $\mathbb{Z}/4$ no lo es.

Ejemplo 21.3. $\mathbb{Z}[i]$ es un dominio íntegro. Este anillo se conoce como el anillo de **enteros de Gauss**.

Sea R un dominio íntegro. Vamos a extender algunas nociones de la divisibilidad en $\mathbb{Z}$ en el contexto del dominio íntegro R. Diremos que x **divide** al elemento y si y sólo si $y = xz$ para algún $z \in R$, lo que resulta ser equivalente a pedir $(y) \subseteq (x)$. Diremos además que x es un **divisor propio** de y si y sólo si $(y) \subsetneq (x) \subsetneq R$. Tal como se hace en el caso de los enteros, a veces utilizaremos la notación $x \mid y$ para referirnos a que el elemento y es divisible por x. Escribiremos $x \nmid y$ cuando y no es divisible por x.

Ejemplo 21.4. Sea $R = \mathbb{Z}[i]$ y sean $d \in \mathbb{Z}$ y $a + bi \in R$. Entonces $d \mid a + bi$ si y sólo si $d \mid a$ y $d \mid b$ en $\mathbb{Z}$. En efecto, si existen $e, f \in \mathbb{Z}$ tales que

$$a + bi = d(e + fi) = de + dfi,$$

entonces $a = de$ y $b = df$, es decir $d \mid a$ y $d \mid b$.

Las siguientes definiciones extienden propiedades que conocemos de $\mathbb{Z}$.

Definición 21.5. Sea R un dominio íntegro y sean $x, y \in R$. Diremos que x e y son **asociados** si y sólo si $(x) = (y)$.

Observar que x e y son asociados si y sólo si $x = yu$ para alguna unidad u.

Ejemplos 21.6. En $\mathbb{Z}$ los enteros 2 y -2 son asociados. En $\mathbb{R}[X]$ los polinomios $f \neq 0$ y λf, donde $\lambda \in \mathbb{R}^\times$, son asociados.

Ejemplo 21.7. En $\mathbb{Z}[i]$ los elementos $2+5i$ y $-5+2i = (2+5i)i$ son asociados.

Definición 21.8. Sea R un dominio íntegro y sea $x \in R \setminus \{0\}$. Diremos que x es **irreducible** si y sólo si $(x) \neq R$ y (x) es maximal en el conjunto de ideales principales de R, es decir que no existe ningún ideal principal (y) tal que $(x) \subsetneq (y) \subsetneq R$.

Para entender mejor la definición de elementos irreducibles observemos que en un dominio íntegro R, los divisores de un irreducible son sus asociados y las unidades de R. En efecto, si z es irreducible y $x \mid z$, entonces $(z) \subseteq (x)$. Esto nos da dos posibilidades, $(z) = (x)$ o bien $(x) = R$, es decir x y z son asociados o bien $x \in \mathscr{U}(R)$.

Ejemplo 21.9. Si K es un cuerpo y $f \in K[X]$ de grado $n > 0$. Entonces f es irreducible en $K[X]$ si y solo si los únicos divisores de f son de la forma $g = \lambda$ o bien $g = \lambda f$ para $\lambda \in K^\times = K \setminus \{0\}$, es decir cuando los divisores de f son unidades de $K[X]$ o los asociados a f.

Del ejemplo anterior se desprende que un polinomio f será reducible (es decir, no irreducible) si $\deg(f) > 0$ y además f tiene algún divisor $g \in K[X]$ no nulo tal que $0 < \deg(g) < \deg(f)$.

Definición 21.10. Sea R un dominio íntegro y sea $p \in R \setminus \{0\}$. Diremos que p es **primo** si y sólo si $(p) \neq R$ y además $xy \in (p) \implies x \in (p)$ o bien $y \in (p)$.

En $\mathbb{Z}$ primos e irreducibles coinciden, algo que no pasará en otros anillos. Más adelante caracterizaremos todos los primos en $\mathbb{Z}[i]$.

Proposición 21.11. *En un dominio íntegro, todo elemento primo es irreducible.*

Demostración. Como p es primo, $p \neq 0$ y $p \notin \mathscr{U}(R)$. Sea x un divisor de p, digamos $p = xy$ para $y \in R$. Como $xy \in (p)$ y p es primo, entonces $x \in (p)$ o $y \in (p)$. Si $x \in (p)$, entonces $x = pz$ y luego

$$p = xy = (pz)y = p(yz) \implies p(1-yz) = 0.$$

Como $p \neq 0$ y R es un dominio, $y, z \in \mathscr{U}(R)$ y luego $x = pz$ es asociado a p. Si $y \in (p)$, una cuenta similar a la anterior nos muestra que $x \in \mathscr{U}(R)$. □

Veremos que la afirmación recíproca no vale con total generalidad, aunque sí en el caso de dominios principales. Para poder hacer algunas cuentas con mayor facilidad, utilizaremos la siguiente herramienta sobre el anillo $R = \mathbb{Z}[\sqrt{d}]$, donde d es un entero libre de cuadrados. Utilizaremos la siguiente notación: si $n \in \mathbb{N}$, entonces $\sqrt{-n} = \sqrt{n}i$.

Lema 21.12. *Sea $d \in \mathbb{Z}$ libre de cuadrados. Para cada $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ sea $N(\alpha) = |a^2 - db^2|$.*

1) $N(\alpha)=0 \iff \alpha=0$.
2) $N(\alpha\beta)=N(\alpha)N(\beta)$ *para todo* $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$.
3) $\alpha\in\mathbb{Z}[\sqrt{d}]$ *es una unidad* $\iff N(\alpha)=1$.
4) Si $N(\alpha)$ *es primo, entonces* α *es irreducible en* $\mathbb{Z}[\sqrt{d}]$.

Demostración. Dejamos las primeras dos afirmaciones como ejercicio. Demostremos (3). Si $\alpha\in\mathscr{U}(\mathbb{Z}[\sqrt{d}])$, entonces $\alpha\beta=1$ para algún $\beta\in\mathbb{Z}[\sqrt{d}]$. Como

$$1=N(1)=N(\alpha\beta)=N(\alpha)N(\beta),$$

entonces $N(\alpha)=1$. Recíprocamente, si $\alpha\neq 0$, entonces α es una unidad con inversa $\alpha^{-1}=\overline{\alpha}/N(\alpha)$, donde $\overline{a+b\sqrt{d}}=a-b\sqrt{d}$.

Demostremos ahora (4). Si $\alpha=\beta\gamma$, entonces $N(\alpha)=N(\beta\gamma)=N(\beta)N(\gamma)$ y luego $N(\beta)=1$ o bien $N(\gamma)=1$ (pues $N(\alpha)$ es primo). Luego $\beta\in\mathscr{U}(\mathbb{Z}[\sqrt{d}])$ o bien $\gamma\in\mathscr{U}(\mathbb{Z}[\sqrt{d}])$ por el ítem anterior. □

Ejemplo 21.13. Sea $R=\mathbb{Z}[i]$.

1) $\mathscr{U}(R)=\{-1,1,i,-i\}$ pues si $a+bi\in R$ es una unidad, entonces, gracias al lema anterior, $N(a+bi)=a^2+b^2=1$.
2) 3 es irreducible en R. Si $3=\alpha\beta$, entonces $9=N(\alpha\beta)=N(\alpha)N(\beta)$. Luego $N(\alpha)\in\{1,3,9\}$. Supongamos que $\alpha=a+bi$. Si $N(\alpha)=3$, entonces $|a^2+b^2|=3$, una contradicción pues $a,b\in\mathbb{Z}$. Luego $N(\alpha)\in\{1,9\}$. Si $N(\alpha)=1$, entonces α es una unidad. Si no, $N(\beta)=1$ y β es una unidad.
3) $2\in R$ no es irreducible. En efecto, alcanza con observar que $2=(1+i)(1-i)$, que $1+i$ y $1-i$ no son unidades pues $N(1+i)=N(1-i)=2\neq 1$.

Ejemplo 21.14. Sea $R=\mathbb{Z}[\sqrt{-5}]$.

1) $1+\sqrt{-5}$ es irreducible en R. Dejamos como ejercicio verificar que $1+\sqrt{-5}$ no es una unidad. Si $1+\sqrt{-5}=\alpha\beta$ para ciertos $\alpha,\beta\in R$, entonces

$$6=N(1+\sqrt{-5})=N(\alpha)N(\beta).$$

Esto implica que $N(\alpha)\in\{1,2,3,6\}$. Si $N(\alpha)\in\{1,6\}$, entonces α es una unidad o bien β es una unidad. Si $\alpha=x+y\sqrt{-5}$, entonces $x^2+5y^2=N(\alpha)\in\{2,3\}$, una contradicción. De la misma forma puede demostrarse que $1-\sqrt{-5}$ es irreducible.
2) 2, 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ no son asociados en R. En efecto, 2, 3 y $1+\sqrt{-5}$ no son asociados pues tienen todos distinta norma. Tampoco son asociados $1+\sqrt{-5}$ y $1-\sqrt{-5}$, pues $1+\sqrt{-5}=u(1-\sqrt{-5})$ para $u\in\mathscr{U}(R)$ da una contradicción.

Ejemplo 21.15. Sea $R=\mathbb{Z}[\sqrt{-3}]$ y sea $x=1+\sqrt{-3}$. Entonces x es irreducible. En efecto, si $1+\sqrt{-3}=\alpha\beta$, entonces $4=N(\alpha)N(\beta)$. Supongamos que $N(\alpha)=2$. Si $\alpha=a+b\sqrt{-3}$, entonces $a^2+3b^2=2$. Obviamente, los enteros a y b tienen que tener la misma paridad. Si $a\equiv b\equiv 0$ mód 2, digamos $a=2k$ y $b=2l$, entonces

$$2=a^2+3b^2=(2k)^2+3(2l)^2=4k^2+12l^2$$

es divisible por 4, una contradicción. Si $a \equiv 1$ mód 2 y además $b \equiv 1$ mód 2, digamos $a = 2k+1$ y $b = 2l+1$, entonces

$$2 = a^2 + 3b^2 = (2k+1)^2 + 3(2l+1)^2 = 4k^2 + 4k + 12l^2 + 12l + 4$$

es un múltilo de 4, una contradicción.

Sin embargo, x no es primo. Como

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 4,$$

x divide a $4 = 2 \times 2$, pero $1+\sqrt{-3}$ no divide a 2 pues

$$(1+\sqrt{-3})(a+b\sqrt{-3}) = 2 \implies (a-3b) + (a+b)\sqrt{-3} = 2$$

que implica que $a-3b = 2$ y además $a+b = 0$. En conclusión, $a = 1/2 \notin \mathbb{Z}$, una contradicción.

Ejercicio 21.16. Demuestre que $1+\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ es un irreducible que no es primo.

Definición 21.17. Un dominio íntegro R se dirá un **dominio de ideales principales** (o simplemente dominio principal) si todo ideal de R es principal.

Vimos que $\mathbb{Z}$ es un dominio de ideales principales. Si K es un cuerpo, entonces $K[X]$ es también un dominio de ideales principales.

Ejemplo 21.18. Veamos que $\mathbb{Z}[X]$ no es principal. Sea $I = (X, 2)$. Primero observemos que $I \neq \mathbb{Z}[X]$. En efecto, si $I = \mathbb{Z}[X]$, entonces

$$1 = 2f + Xg$$

para ciertos $f, g \in \mathbb{Z}[X]$. En particular, $-1/2 = f(0) \in \mathbb{Z}$, una contradicción. Si existe $h \in \mathbb{Z}[X]$ tal que $I = (h)$, entonces, en particular, $2 = hg$ y además $X = hf$ para ciertos $f, h \in \mathbb{Z}[X]$. En particular, $\deg h = 0$ y luego h es la constante $h(1)$. Como $2 = h(1)g(1)$, tenemos $h = h(1) \in \{-1, 1, 2, -2\}$. Como I es un ideal propio, $h = h(1) \notin \{-1, 1\}$. Luego $X = \pm 2f$. Si escribimos

$$f = a_0 + a_1 X + \cdots + a_n X^n,$$

donde $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, entonces, al comparar el coeficiente de X en $X = \pm 2f$ vemos que $1 = \pm 2a_1$, una contradicción pues $a_1 \in \mathbb{Z}$.

Ejemplo 21.19. Veamos que $\mathbb{Z}[\sqrt{-5}]$ no es principal. Sea $I = (2, 1+\sqrt{-5})$. Primero observamos que $I \neq \mathbb{Z}[\sqrt{-5}]$. En efecto, si $I = \mathbb{Z}[\sqrt{-5}]$, entonces

$$1 = 2(x+\sqrt{-5}y) + (1+\sqrt{-5})(u+\sqrt{-5}v) = (2x+u-5v) + \sqrt{-5}(2y+u+v)$$

para ciertos $x, y, u, v \in \mathbb{Z}$. Luego

$$1 = 2x + u - 5v, \quad 0 = 2y + u + v,$$

que implica que $1 = 2(x+y+u-2v)$, una contradicción pues $x+y+u-2v \in \mathbb{Z}$. Si $I = (\alpha)$, entonces $N(\alpha) \mid N(2)$, pues $\alpha \mid 2$, y además $N(\alpha) \mid N(1+\sqrt{-5})$, pues $\alpha \mid 1+\sqrt{-5}$. Observemos que entonces se tiene que $N(\alpha) \in \{1,2\}$, pues $N(2) = 4$ y $N(1+\sqrt{-5}) = 6$. Si $\alpha = a+b\sqrt{-5}$, entonces, como $N(\alpha) = a^2+5b^2$, se concluye que $N(\alpha) = 1$. Luego α es una unidad y entonces $I = \mathbb{Z}[\sqrt{-5}]$, una contradicción.

Proposición 21.20. *Sea R un dominio principal y sea $x \in R$. Entonces x es irreducible si y sólo si x es primo.*

Demostración. Vimos en la proposición anterior que todo primo es irreducible. Supongamos entonces que x es irreducible y que $x \mid yz$. Sea $I = (x,y)$ el ideal generado por x e y. Como R es principal, existe $a \in R$ tal que $I = (a)$. En particular, $x = ab$ para algún $b \in R$. La irreducibilida de x implica que $a \in \mathscr{U}(R)$ o bien $b \in \mathscr{U}(R)$. Si $a \in \mathscr{U}(R)$, entonces $I = R$ y luego $1 = xr+ys$ para ciertos $r,s \in R$, lo que implica que

$$z = z1 = z(xr+ys) = xzr+yzs$$

y entoces $x \mid z$. Si $b \in \mathscr{U}(R)$, entonces $I = (x) = (a)$ y luego, como $y \in I$, existe $t \in R$ tal que $xt = y$, es decir $x \mid y$. □

Ejemplo 21.21. $\mathbb{Z}[\sqrt{-3}]$ no es principal ya que existen irreducibles que no son primos.

Ejemplo 21.22. Como $\mathbb{Z}$ es principal, en $x \in \mathbb{Z}$ es primo si y sólo si $x \in \mathbb{Z}$ es irreducible.

Definición 21.23. Sea R un dominio íntegro. Diremos que R es un **dominio euclidiano** si existe una función $\varphi\colon R \setminus \{0\} \to \mathbb{N}_0$ tal que para cada $x,y \in R$ con $y \neq 0$ existen $q,r \in R$ tales que $x = yq+r$, donde $r = 0$ o bien $\varphi(r) < \varphi(y)$.

Es importante remarcar que en la definición de dominio euclidiano no pedimos la unicidad que tenemos en $\mathbb{Z}$. En muchos libros de texto, en la definición de dominio euclidiano, a la función φ se le pide además que cumpla $\varphi(x) \leq \varphi(xy)$ para todo $x,y \in R \setminus \{0\}$. Esta condición no se usa para demostrar los resultados básicos, por eso no se incluye. Además, si R es euclidiano (con nuestra definición y nuestro φ), siempre puede reemplazarse φ por una función $\psi(x) = \min_{y \neq 0} \varphi(xy)$ y esta ψ satisface $\psi(x) \leq \psi(xy)$ para todo $x,y \in R \setminus \{0\}$.

Ejemplos 21.24.

1) $\mathbb{Z}$ es un dominio euclidiano con $\varphi(x) = |x|$. Cuidado que acá tampoco tenemos unicidad.
2) Si K es un cuerpo, $K[X]$ es euclidiano con $\varphi(f) = \deg f$. Este ejemplo es el que motiva que la función φ de la definición de dominio euclidiano esté definida para elementos no nulos del anillo.

Veamos otro ejemplo de dominio euclidiano.

Ejemplo 21.25. Sea $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$. Dejamos como ejercicio demostrar que $\mathbb{Z}[i]$ es un dominio íntegro.

Sea $N(x+iy) = x^2+y^2$. Veamos que N es un función multiplicativa: Si $\alpha = x+iy$ y $\beta = u+iv$, entonces

$$\alpha\beta = (xu-yv)+i(xv+yu)$$

y luego

$$N(\alpha\beta) = (xu-yv)^2-(xv+yu)^2 = (x^2+y^2)(u^2+v^2) = N(\alpha)N(\beta).$$

Vamos a demostrar ahora que $\mathbb{Z}[i]$ es un dominio euclidiano con $\varphi(\alpha) = N(\alpha)$. Sean $\alpha = a+ib$ y $\beta = c+id \neq 0$. Entonces

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = r+is,$$

donde $r = (ac+bd)/(c^2+d^2)$ y $s = (bc-ad)/(c^2+d^2)$. Sean $m,n \in \mathbb{Z}$ tales que $|r-m| \leq 1/2$ y $|s-n| \leq 1/2$. Si $\delta = m+in$ y $\gamma = \alpha - \beta\delta$, entonces $\delta, \gamma \in \mathbb{Z}[i]$ y además $\alpha = \beta\delta+\gamma$. Si $\gamma \neq 0$, entonces

$$\begin{aligned}\varphi(\gamma) &= \varphi\left(\beta\left(\frac{\alpha}{\beta}-\delta\right)\right) = \varphi(\beta)\varphi\left(\frac{\alpha}{\beta}-\delta\right)\\ &= \varphi(\beta)\varphi((r-m)+i(s-n)) = \varphi(\beta)\left((r-m)^2+(s-n)^2\right)\\ &\leq \varphi(\beta)\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{1}{2}\varphi(\beta) < \varphi(\beta).\end{aligned}$$

En $\mathbb{Z}[i]$ hay algoritmo de división pero no tenemos unicidad. De hecho, por ejemplo, podemos escribir

$$1+8i = (2-4i)(-1+i)+(-1+2i) = (2-4i)(-2+i)+(1-2i)$$

y entonces $N(1-2i) = N(-1+2i) = 5 < 20 = N(2-4i)$.

Ejemplo 21.26. Si $\omega = \frac{-1+\sqrt{3}i}{2}$, entonces $\mathbb{Z}[\omega]$ es un dominio euclidiano. Primero observamos que

$$\mathbb{Z}[\omega] = \left\{\frac{a}{2}+\frac{b}{2}\sqrt{-3} : a,b \in \mathbb{Z},\, a \equiv b \text{ mód } 2\right\}$$

pues $a+b\omega = \frac{2a+b}{2}+\frac{b}{2}\sqrt{-3}$.

Veamos que $\mathbb{Z}[\omega]$ es euclidiano con la norma $N(a+b\sqrt{-3}) = a^2+3b^2$, donde $a,b \in \frac{1}{2}\mathbb{Z}$. Sean $\alpha = a_1+a_2\omega$ y $\beta = b_1+b_2\omega \neq 0$, donde $a_1,a_2,b_1,b_2 \in \frac{1}{2}\mathbb{Z}$. Queremos ver que existen $\gamma, \delta \in \mathbb{Z}[\omega]$ tales que $\alpha = \beta\gamma+\delta$, donde $N(\delta) < N(\beta)$. En $\mathbb{Q}[\sqrt{-3}]$ podemos dividir, entonces

$$\frac{\alpha}{\beta} = c_1+c_2\sqrt{-3},$$

para ciertos $c_1, c_2 \in \mathbb{Q}$. Sea $q_2 \in \mathbb{Z}$ tal que $|2c_2 - q_2| \leq 1/2$ y sea $t \in \mathbb{Z}$ el entero más cercano al número $c_1 - \frac{q_2}{2}$. Si $q_1 = 2t + q_2$, entonces $|c_1 - \frac{q_1}{2}| \leq 1/2$. Si

$$\gamma = \frac{q_1}{2} + \frac{q_2}{2}\sqrt{-3},$$

entonces $\gamma \in \mathbb{Z}[\omega]$ pues $q_1 - q_2 = 2t$ es par. Si

$$\delta = \beta\left((c_1 - \frac{q_1}{2}) + (c_2 - \frac{q_2}{2})\sqrt{-3}\right),$$

entonces $\alpha = \gamma\beta + \delta$. Como

$$N\left((c_1 - \frac{q_1}{2}) + (c_2 - \frac{q_2}{2})\sqrt{-3}\right) \leq (c_1 - \frac{q_1}{2})^2 + 3(c_2 - \frac{q_2}{2})^2 \leq \frac{1}{4} + 3\frac{1}{16} < 1,$$

se concluye que $N(\delta) < N(\beta)$ pues N es multiplicativa.

Ejercicio 21.27. Demuestre que $\mathbb{Z}[\sqrt{d}]$ es euclidiano si $|d| \leq 2$.

El siguiente ejemplo no es sencillo. Simplemente lo mencionamos para mayor completitud en la presentación. Para más información ver [1, 7, 6].

Ejemplo 21.28. Si $\theta = \frac{1+\sqrt{-19}}{2}$, entonces $\mathbb{Z}[\theta]$ no es euclidiano. Sin embargo, $\mathbb{Z}[\theta]$ es un dominio de ideales principales.

Tal como pasa en $\mathbb{Z}$ y $K[X]$, el tener algoritmo de división nos permite demostrar que todo ideal es principal.

Teorema 21.29. *Si R es euclidiano, entonces R es principal.*

Demostración. Sea I un ideal no nulo de R y sea $y \in I$ no nulo donde la función $x \mapsto \varphi(x)$ alcanza su mínimo. Si $z \in I$, entonces $z = yq + r$ donde $r = 0$ o bien $\varphi(r) < \varphi(y)$. La minimalidad de y implica que $r = 0$ y luego $z = yq$. Tenemos entonces $I \subseteq Ry \subseteq (y) \subseteq I$ y luego $I = (y)$. □

Ejemplo 21.30. El anillo $\mathbb{Z}[\sqrt{-5}]$ no es euclidiano ya que no es principal.

Nos interesa poder reconocer anillos de la forma $\mathbb{Z}[\sqrt{d}]$, con d libre de cuadrados, que se parezcan al anillo $\mathbb{Z}$. Ya vimos que hay muchas similitudes, pero en $\mathbb{Z}[\sqrt{d}]$ no siempre valdrá el teorema de la factorización única.

Definición 21.31. Diremos que un dominio íntegro R es un **dominio factorización única** si valen las siguientes propiedades:

1) Cada $x \neq 0$ que no es una unidad puede escribirse como $x = c_1 \dots c_n$ para ciertos irreducibles $c_1, \dots, c_n$.
2) Si $x = c_1 \cdots c_n = d_1 \cdots d_m$ con los c_i y los d_j irreducibles, entonces $n = m$ y además existe una permutación $\sigma \in \mathbb{S}_n$ tal que c_i y $d_{\sigma(i)}$ son asociados para todo $i \in \{1, \dots, n\}$.

El ejemplo típico de domino de factorización única es $\mathbb{Z}$.

Intentaremos explicar mejor la diferencia entre tener factorización y tener factorización única. Supongamos que R es un dominio íntegro noetheriano. Podemos demostrar entonces que R tendrá factorización, aunque no necesariamente única. Sea $x \in R$ no nulo tal que $x \notin \mathscr{U}(R)$. Si x es irreducible, no hay nada para demostrar. En caso contrario, podemos escribir $x = x_1x_2$ con $x_1, x_2 \notin \mathscr{U}(R)$. Si x_1 y x_2 son ambos irreducibles, significa que x pudo factorizarse en irreducibles. En caso contrario, digamos si x_1 no es irreducible, entonces podemos escribir $x_1 = x_{11}x_{12}$ para $x_{11}, x_{12} \notin \mathscr{U}(R)$. Nos interesa demostrar que este procedimiento en algún momento tiene que terminarse en una cantidad finita de pasos y eso pasa porque, así como la factorización $x = x_1x_2$ nos da la sucesión $(x) \subsetneq (x_1) \subsetneq (x_{11})$, el procedimiento general nos da la sucesión $(x) \subsetneq (x_1) \subsetneq (x_{11}) \subseteq \cdots$, que tiene que estabilizarse pues R es noetheriano.

Ejemplo 21.32. Gracias al teorema de Hilbert sabemos que $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-6}]$ son ambos noetherianos, lo que nos dice que en en esos anillos existirá factorización. Sin embargo, veremos que en $\mathbb{Z}[i]$ hay factorización única y que en $\mathbb{Z}[\sqrt{-6}]$ no.

Teorema 21.33. *Sea R un dominio de ideales principales. Entonces R es un dominio de factorización única.*

Demostración. Primero demostraremos que R es noetheriano. Como todos los ideales de R son principales, toda sucesión de ideales es de la forma $(a_1) \subsetneq (a_2) \subsetneq \cdots$. Fijada esa sucesión, la unión $J = \cup_{i \geq 1}(a_i)$ es un ideal de R. Como R es principal, $J = (x)$ para algún $x \in R$. En particular, como $x \in (a_i)$ para algún $i \geq 1$, podemos concluir que $(a_k) \subseteq J = (x) \subseteq (a_i)$ para todo k.

Como R es noetheriano, R admite factorización en irreducibles.

Nos falta demostrar la unicidad. Sea $x \in R$ y supongamos que

$$x = c_1 \cdots c_n = d_1 \cdots d_m$$

son factorizaciones de x en irreducibles, donde $n \leq m$. Si $m = 1$, entonces $n = 1$ y luego $c_1 = d_1$. Si $m > 1$, como c_1 es primo (pues sabemos que en R los irreducibles son primos) y además $c_1 \mid d_1 \cdots d_m$, entonces c_1 divide a alguno de los d_j, digamos $c_1 \mid d_1$, sin perder generalidad. Como d_1 es irreducible y $c_1 \notin \mathscr{U}(R)$, c_1 y d_1 son asociados, es decir $c_1 = ud_1$ para algún $u \in \mathscr{U}(R)$. Como entonces

$$c_1c_2 \cdots c_n = (ud_1)c_2 \cdots c_n = d_1d_2d_3 \cdots d_m,$$

se sigue que

$$d_1(c_2 \cdots c_n - u^{-1}d_2 \cdots d_m) = 0.$$

Como R es un dominio y además $d_1 \neq 0$, después de reemplazar, sin perder generalidad, $u^{-1}d_2$ por d_2, nos quedamos con $c_2 \cdots c_n = d_2 \cdots d_m$. Por inducción, queda entonces demostrada la implicación que queríamos probar. □

Ejemplo 21.34. $\mathbb{Z}[\sqrt{-6}]$ no es un dominio de factorización única. En efecto, primero observamos que

$$10 = 2 \cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6}).$$

Recordemos que $N(a+b\sqrt{-6}) = a^2+6b^2$. Primero veamos que 2 es irreducible. Si $2 = \alpha\beta$ con $\alpha, \beta \notin \mathscr{U}(R)$, entonces

$$4 = N(2) = N(\alpha)N(\beta)$$

y luego $N(\alpha) = N(\beta) = 2$, una contradicción pues $a^2+6b^2 \neq 2$ para todo $a,b \in \mathbb{Z}$. De la misma forma se demuestra que 5 es también irreducible en $\mathbb{Z}[\sqrt{-6}]$.

Queda como ejercicio demostrar que $2+\sqrt{-6}$ y $2-\sqrt{-6}$ son irreducibles,.

Terminamos el capítulo con una aplicación a la teoría de números.

Teorema 21.35 (Fermat). *Para p un número primo, son equivalentes:*

1) $p = 2$ o bien $p \equiv 1$ mód 4.
2) Existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1$ mód p.
3) p no es irreducible en $\mathbb{Z}[i]$.
4) p es suma de dos cuadrados.

Demostración. Veamos primero que (1) $\implies$ (2). Si $p = 2$, entonces $a = 1$. Si $p = 4k+1$, el pequeño teorema de Fermat nos dice que las raíces del polinomio $X^{p-1}-1$ con coeficientes en $\mathbb{Z}/p$ son $1, 2, \ldots, p-1$. Escribimos

$$X^{p-1}-1 = X^{4k}-1 = (X^{2k}-1)(X^{2k}+1) = (X-1)(X-2)\cdots(X-(p-1))$$

en $(\mathbb{Z}/p)[X]$. Como p es primo, $\mathbb{Z}/p$ es un cuerpo y luego $(\mathbb{Z}/p)[X]$ es un dominio de factorización única, pues $(\mathbb{Z}/p)[X]$ es un dominio de ideales principales por ser un dominio euclidiano. Existe entonces $\alpha \in \mathbb{Z}/p$ tal que $\alpha^{2k}+1 = 0$ y para terminar la demostración alcanza con tomar $a = \alpha^{2k}$.

Demostremos ahora que (2) $\implies$ (3). Si $a^2 \equiv -1$ mód p, entonces $a^2+1 = kp$ para algún $k \in \mathbb{Z}$. Como $(a-i)(a+i) = a^2+1 = kp$, entonces $p \mid (a-i)(a+i)$. Afirmamos que $p \nmid a+i$ en $\mathbb{Z}[i]$. Si $p \mid a+i$, entonces $a+i = p(e+fi)$ para ciertos $e, f \in \mathbb{Z}$. Luego $1 = pf$, una contradicción. De la misma forma se demuestra que $p \nmid a-i$. Sabemos entonces que $p \mid (a-i)(a+i)$ pero $p \nmid a-i$ y $p \nmid a+i$, es decir p no es un primo de $\mathbb{Z}[i]$, por lo que tampoco será un irreducible de $\mathbb{Z}[i]$ (recordemos que $\mathbb{Z}[i]$ es un dominio de ideales principal y en dominios de ideales principales primos e irreducibles son equivalentes).

Veamos ahora que (3) $\implies$ (4). Como p no es irreducible en $\mathbb{Z}[i]$, escribimos $p = (a+bi)(c+di)$ con $a+bi \notin \mathscr{U}(\mathbb{Z}[i])$ y $c+di \notin \mathscr{U}(\mathbb{Z}[i])$, es decir $N(a+bi) \neq 1$ y $N(c+di) \neq 1$, y entonces

$$p^2 = N(p) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2).$$

Como $\mathbb{Z}$ es un dominio de factorización única y p es irreducible en $\mathbb{Z}$, $p = a^2+b^2$.

Para finalizar, demostremos que (4) $\implies$ (1). Como p es un número primo, entonces $p = 2$, $p \equiv 1$ mód 4 o bien $p \equiv 3$ mód 4. Si $p \equiv 3$ mód 4 y $p = a^2+b^2$, entonces $a^2+b^2 \equiv 3$ mód 4, una contradicción pues los únicos casos posibles son $a^2+b^2 \equiv 0$ mód 4, $a^2+b^2 \equiv 1$ mód 4 o bien $a^2+b^2 \equiv 2$ mód 4. □

Veamos ahora como aplicación que $\mathbb{Z}[i]$ puede utilizarse para resolver ecuaciones en $\mathbb{Z}$.

Proposición 21.36. *La ecuación $y^3 - 1 = x^2$ tiene únicamente una solución en $\mathbb{Z}$.*

Demostración. Si x es impar, entonces $x^2 \equiv 1$ mód 4. Luego $2 \mid x^2+1$, pero además $4 \nmid x^2+1$. Como además y es par, tenemos que $y^3 = x^2+1$ es divisible por 8, una contradicción. Luego x es par e y es impar. Escribimos

$$y^3 = x^2 + 1 = (x-i)(x+i)$$

Observemos que $x-i$ y $x+i$ no tienen factores en común pues si $d \in \mathbb{Z}[i]$ es tal que $d \mid x+i$ y $d \mid x-i$, entonces $d = 1$ por lo que vimos en el ejemplo 21.4 de la página 125. La factorización única del anillo $\mathbb{Z}[i]$ implica que $x+i = ((a+bi)u)^3$ para ciertos $a, b \in \mathbb{Z}$ y $u \in \mathscr{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. Como entonces $u^3 \in \{-1, 1, i, -i\}$, sin perder generalidad podemos suponer que

$$x + i = (a+bi)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3).$$

En particular, $1 = 3a^2b - b^3 = b(3a^2 - b^2)$, lo que implica que $b = 1$ y $a = 0$, es decir $(x, y) = (0, 1)$. □

Capítulo 22
El lema de Zorn

Un conjunto no vacío R se dirá **parcialmente ordenado** si posee una relación X en R (es decir, $X \subseteq R \times R$) tal que

1) $(r,r) \in X$ para todo $r \in R$,
2) $(r,s) \in X$ y $(s,t) \in X$ implican que $(r,t) \in X$, y además
3) $(r,s) \in X$ y $(s,r) \in X$ implican que $r = s$.

La notación que utilizaremos es la siguiente: $(r,s) \in X \iff r \leq s$. Un conjunto parcialmente ordenado será denotado entonces como el par $(R, \leq)$. Las tres condiciones anteriores pueden reescribirse así:

1) $r \leq r$ para todo $r \in R$.
2) $r \leq s$ y $s \leq t$ implican que $r \leq t$.
3) $r \leq s$ y $s \leq r$ implican que $r = s$.

Otra notación que utilizaremos frecuentemente: $r < s \iff r \leq s$ y además $r \neq s$.

Sea $(R, \leq)$ un conjunto parcialmente ordenado y sean $r, s \in R$. Diremos que r y s son **comparables** si $r \leq s$ o bien $s \leq r$.

Ejemplo 22.1. Sea $U = \{1,2,3,4,5\}$ y sea T el conjunto de subconjuntos de U. Definimos la relación $C \leq D \iff C \subseteq D$. Luego T es un conjunto parcialmente ordenado. Los subconjuntos $\{1,2\}$ y $\{3,4\}$ no son comparables.

Si $(R, \leq)$ es un conjunto parcialmente ordenado, diremos que un elemento $r \in R$ es **maximal** en R si para todo $t \in R$ comparable con r, se tiene que $t \leq r$, es decir: para todo $t \in R$ tal que $r \leq t$ se tiene $r = t$.

Ejemplo 22.2. $(\mathbb{Z}, \leq)$ no tiene elementos maximales.

Ejemplo 22.3. Sea $R = \{(x,y) \in \mathbb{R}^2 : y \leq 0\}$. Definimos la relación de orden parcial

$$(x_1, y_1) \leq (x_2, y_2) \iff x_1 = x_2 \text{ y además } y_1 \leq y_2.$$

Entonces $(R, \leq)$ es un conjunto parcialmente ordenado. Cada elemento de la forma $(x,0)$ es un elemento maximal, pues si $(x,0) \leq (x_1, y_1)$, entonces $x = x_1$ y además $y_1 = 0$. En conclusión, R tiene una infinidad de elementos maximales.

Si R es un conjunto parcialmente ordenado, una **cota superior** de un subconjunto no vacío S de R será un elemento $u \in R$ tal que $s \leq u$ para todo $s \in S$.

Ejemplo 22.4. El conjunto $S = \{6\mathbb{Z}, 12\mathbb{Z}, 24\mathbb{Z}\}$ de subgrupos de $\mathbb{Z}$ es totalmente ordenado con la inclusión. El elemento $6\mathbb{Z} = 6\mathbb{Z} \cup 12\mathbb{Z} \cup 24\mathbb{Z}$ es cota superior de S.

Un subconjunto no vacío S de R será una **cadena** si dos elementos cualesquiera de S son comparables. El **lema de Zorn** afirma lo siguiente:

> Si R es un conjunto parcialmente ordenado tal que toda cadena en R admite una cota superior en R, entonces R contiene un elemento maximal.

Como se ve, el lema de Zorn nada tiene de intuitivo. Curiosamente, es lógicamente equivalente al axioma de elección y al principio de buena ordenación. En realidad, el lema de Zorn es un axioma y no un resultado que debe demostrare.

En vez de profundizar más en los aspectos lógicos del lema de Zorn y sus equivalencias, nos contentaremos con dar una aplicación.

Definición 22.5. Sea R un anillo. Diremos que un ideal $I \neq R$ es **maximal** si dado un ideal J de R tal que $I \subseteq J$, entonces $I = J$ o bien $J = R$.

Ejemplo 22.6. Si p es un número primo, entonces $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.

Ejercicio 22.7. Sea R un anillo. Entonces R es un cuerpo si y sólo si $\{0\}$ es un ideal maximal.

Ejercicio 22.8. Sea R un anillo. Un ideal I de R es maximal si y sólo si R/I es un cuerpo.

Ahora sí, el teorema.

Teorema 22.9. *Sea R un anillo no nulo. Todo ideal $I \neq R$ está contenido en un ideal maximal. En particular, todo anillo no nulo tiene ideales maximales.*

Demostración. Sea

$$X = \{J \subseteq R : J \text{ es un ideal tal que } I \subseteq J \subsetneq R\}.$$

Como $I \in X$, entonces X es no vacío. Luego X es un conjunto parcialmente ordenado con la inclusión. Si C es una cadena en X, entonces $\cup_{J \in C} J \in X$ es una cota superior para C, pues $\cup_{J \in C} J$ es un ideal de R y $1 \notin \cup_{J \in C} J$, lo que implica que $\cup_{J \in C} J \neq R$. Por el lema de Zorn, existe entonces $M \in X$ un elemento maximal.

Afirmamos que M es un ideal maximal de R. En efecto, si M_1 es un ideal propio de R tal que $M \subseteq M_1$, entonces $I \subseteq M_1$ y luego $M_1 \in X$, lo que implica que $M = M_1$ pues M es maximal en X. □

En el teorema anterior, el hecho crucial es la existencia de la unidad del anillo. De hecho, el álgebra no conmutativa nos muestra que existen anillos (no son anillos unitarios, obviamente) que no poseen ideales maximales.

Ejemplo 22.10. Sea K un cuerpo. Los ideales maximales de $K[X]$ son los ideales principales generados por los polinomios mónicos irreducibles. En efecto, si I es un ideal maximal, entonces $I = (f)$ para algún $f \in K[X]$, pues sabemos que $K[X]$ es principal. Si $\deg f = n$ y a es el coeficiente principal de f, entonces $g = a^{-1}f$ es un polinomio mónico tal que

$$(a^{-1}f) = (f).$$

Podemos suponer entonces, sin perder generalidad, que f es mónico. Si f es irreducible y $(f) \subseteq J \subseteq K[X]$, escribimos $J = (g)$ para algún $g \in K[X]$. Entonces $f = gh$ para algún $h \in K[X]$, lo que implica que g o h son constantes. Si g es constante, entonces $(g) = K[X]$. Si h es constante, digamos $h = a \in K$, entonces $f = ga$, lo que implica que $g = a^{-1}f \in (f)$ y luego $I = J$.

Ejercicio 22.11. Sea R un dominio de ideales principales. Demuestre que $p \in R$ es irreducible si y sólo si (p) es un ideal maximal.

Un caso particular del ejercicio anterior. Si K es un cuerpo, $f \in K[X]$ es irreducible si y sólo si el ideal (f) es maximal.

Ejemplo 22.12. Sean K un cuerpo y S un dominio íntegro. Si $\varphi \in K[X] \to S$ es un morfismo de anillos, entonces $\ker\varphi = \{0\}$ o bien $\ker\varphi$ es maximal. En efecto, como $K[X]$ es principal, sabemos que $\ker\varphi = (f)$ para algún $f \in K[X]$. Si $\ker\varphi = 0$, no hay nada que demostrar. Si f es irreducible, entonces (f) es maximal. En caso contrario, digamos $f = gh$, tenemos

$$0 = \varphi(f) = \varphi(gh) = \varphi(g)\varphi(h).$$

Como S es un dominio íntegro, $\varphi(g) = 0$ o bien $\varphi(h) = 0$. Sin perder generalidad, podemos suponer que $\varphi(g) = 0$, es decir $g \in \ker\varphi$. Luego $(f) \subseteq (g) = \ker\varphi$ y entonces h es una unidad, una contradicción.

Ejemplo 22.13. El ideal $(X^2 + 2X + 2)$ es maximal en $\mathbb{Q}[X]$ pues

$$X^2 + 2X + 2 = (X+1)^2 + 1 > 0$$

es irreducible en $\mathbb{Q}[X]$, por ser un polinomio de grado dos sin raíces racionales.

Ejercicio 22.14. Demuestre que R/I es un cuerpo si y sólo si I es un ideal maximal.

Ejemplo 22.15. Sea $R = (\mathbb{Z}/2)[X]$. Como $X^2 + X + 1$ es irreducible en R, el ideal $I = (X^2 + X + 1)$ es maximal. Luego R/I es un cuerpo.

Ejercicio 22.16. Sea R un anillo conmutativo y sea $J(R)$ la intersección de todos los ideales maximales de R. Pruebe que $x \in J(R)$ si y sólo si $1 - xy \in \mathscr{U}(R)$ para todo $y \in R$.

Ejercicio 22.17. Los ideales maximales de $\mathbb{Z}/n$ son de la forma $I = \mathbb{Z}/p$ donde p es un primo que divide a n.

Veamos ahora una aplicación a la teoría de grupos.

Un subgrupo propio M de un grupo G se dice **maximal** si $M \subseteq H \subseteq G$ para algún subgrupo H de G implica que $M = H$ o $H = G$, es decir que el subgrupo M es maximal con respecto a la inclusión entre los subgrupos propios de G. Quizá sería mejor definir estos subgrupos como maximal-propio, pero, tal como se hace en la literatura, nos quedaremos con la terminología estándar.

Ejercicio 22.18. Demuestre que $M \leq \mathbb{Z}$ es maximal si y sólo si $M = p\mathbb{Z}$ para algún primo p.

Ejercicio 22.19. Demuestre que $\mathbb{Q}$ no tiene subgrupos maximales.

Ejercicio 22.20. Demuestre que todo subgrupo propio de un grupo finito está contenido en algún subgrupo maximal.

El resultado del ejercicio anterior puede extenderse a grupos finitamente generados gracias al lema de Zorn.

Teorema 22.21. *Sea G un grupo no trivial y finitamente generado. Todo subgrupo propio de G está contenido en un subgrupo maximal.*

Demostración. Supongamos que $G = \langle g_1, \ldots, g_n \rangle$ y sea K un subgrupo propio de G. Para cada $j \in \{0, \ldots, n\}$ se define $G_j = \langle K, g_1, \ldots, g_j \rangle$. Como

$$K = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G,$$

existe entonces $l = \text{máx}\{j : 0 \leq j \leq n-1, G_j \neq G\}$. Luego $G_{l+1} = \langle G_l, g_{l+1} \rangle = G$ y además $g_{l+1} \notin G_l$. Sea

$$S = \{H : H \leq G, G_l \subseteq H, g_{l+1} \notin H\}$$

ordenado parcialmente con la inclusión. Como $G_l \in S$, entonces $S \neq \emptyset$. Dejamos como ejercicio demostrar que si $\{H_i : i \in I\} \subseteq S$ es totalmente ordenado, entonces $H = \cup_{i \in I} H_i$ es una cota superior de S. Por el lema de Zorn sabemos entonces que S tiene un elemento maximal, digamos M, es decir que M es maximal con respecto a las siguientes propiedades: $M \leq G$, $G_l \subseteq M$ y $g_{l+1} \notin M$.

Vamos a demostrar ahora que M es un subgrupo maximal de G que contiene a K. Como $K \subseteq G_l \subseteq M$, entonces M contiene a K. Para ver que M es maximal, supongamos que $M \leq L \leq G$. Si $g_{l+1} \notin L$, entonces, por definición, $L \in S$, pero esto contradice la maximalidad del conjunto M. Luego $g_{l+1} \in L$, lo que implica que $\langle M, g_{l+1} \rangle \subseteq L$. Como $G_l \subseteq M$, entonces

$$G = G_{l+1} = \langle G_l, g_{l+1} \rangle \subseteq \langle M, g_{l+1} \rangle.$$

En consecuencia, $G \subseteq L$ y luego $L = G$. □

Capítulo 23
Álgebras

En este capítulo veremos cierto tipo de anillos que además son espacios vectoriales de forma que la acción por escalares y la estructura de anillo son compatibles. Este concepto es de gran importancia en álgebra.

Definición 23.1. Un espacio vectorial A sobre un cuerpo K es un **algebra** sobre K (o una K-álgebra) si posee una multiplicación asociativa $A \times A \to A$, $(a,b) \mapsto ab$, tal que $(\lambda a+\mu b)c = \lambda(ac)+\mu(bc)$ y $a(\lambda b+\mu c) = \lambda(ab)+\mu(ac)$ para todo $a,b,c \in A$ y $\lambda,\mu \in K$. Existe además un elemento $1_A \in A$ tal que $1_A a = a1_A = a$ para todo $a \in A$.

Un álgebra A se dirá **conmutativa** si $ab = ba$ para todo $a,b \in A$.

La **dimensión** de un álgebra A es la dimensión de A como K-espacio vectorial. Justamente esta es quizá una de las claves de la definición, un álgebra es en particular un espacio vectorial y cuando sea necesario podremos utilizar argumentos que involucren el concepto de dimensión.

Ejemplo 23.2. Todo cuerpo K es una K-álgebra.

Ejemplo 23.3. Si K es un cuerpo, $K[X]$ es una K-álgebra.

Similarmente, el anillo de polinomios $K[X,Y]$ y el anillo $K[[X]]$ de series de potencias son ejemplos de álgebras sobre el cuerpo K.

Ejemplo 23.4. Si A es un álgebra, entonces $M_n(A)$ es un álgebra.

Ejemplo 23.5. El conjunto de funciones continuas $[0,1] \to \mathbb{R}$ es un álgebra sobre $\mathbb{R}$ con las operaciones usuales, $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$.

Un **morfismo de álgebras** es un morfismo de anillos $f\colon A \to B$ que es además una transformación lineal. Observemos que es necesario pedir que un morfismo de álgebras sea una transformación lineal, por ejemplo, la conjugación $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$, es un morfismo de anillos que no es un morfismo de álgebras sobre $\mathbb{C}$.

Definición 23.6. Un **ideal** de un álgebra es un ideal del anillo que además es un subespacio.

Análogamente se definen ideales a izquierda y a derecha de un álgebra.

Si A es un álgebra, entonces todo ideal a izquierda del anillo A es un ideal a izquierda del álgebra A. Si L es un ideal de A y $\lambda \in K$ y $x \in L$, entonces

$$\lambda x = \lambda(1_A x) = (\lambda 1_A)x$$

y luego, como $\lambda 1_A \in A$, se concluye que $\lambda L = (\lambda 1_A)L \subseteq L$. Análogamente se demuestra que todo ideal a derecha del anillo unitario A es también un ideal de A como álgebra.

Ejercicio 23.7. Demuestre que si A es un álgebra, entonces todo ideal a derecha del anillo A es un ideal a derecha del álgebra A.

Puede demostrarse que si A es un álgebra e I es un ideal de A, entonces el anillo cociente A/I tiene una única estructura de álgebra que hace que el morfismo canónico $A \to A/I$, $a \mapsto a+I$, sea un morfismo de álgebras.

Ejemplo 23.8. Si $n \in \mathbb{N}$, entonces $K[X]/(X^n)$ es un álgebra de dimensión finita, se conoce como el **álgebra de polinomios truncados**.

Sea A un álgebra. Un elemento $a \in A$ se dice **algebraico** sobre A si existe un polinomio no nulo $f \in K[X]$ tal que $f(a) = 0$. Si todo elemento de A es algebraico, A se dice **algebraica**. Por ejemplo, sabemos que en la $\mathbb{Q}$-álgebra $A = \mathbb{R}$ el elemento $\sqrt{2}$ es algebraico, pues $\sqrt{2}$ es raíz del polinomio $X^2 - 2 \in \mathbb{Q}[X]$, y que π no lo es. Todo elemento de $\mathbb{R}$ como $\mathbb{R}$-álgebra es algebraico.

Proposición 23.9. *Toda álgebra de dimensión finita es algebraica.*

Demostración. Sea A un álgebra de dimensión finita n y sea $a \in A$. Como el conjunto $\{1, a, a^2, \ldots, a^n\}$ es linealmente dependendiente, existe un polinomio no nulo $f \in k[X]$ tal que $f(a) = 0$. □

Sea K un cuerpo y sea G un grupo finito. El **álgebra de grupo** $K[G]$ es el K-espacio vectorial con base $\{g : g \in G\}$ con la estructura de álgebra dada por el producto

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{g,h\in G} \lambda_g \mu_h (gh).$$

Observemos que el álgebra $K[G]$ es conmutativa si y sólo si G es abeliano. Además $\dim K[G] = |G|$.

Ejemplo 23.10. Sea $G = \{1, g, g^2\}$ el grupo cíclico de orden tres y sea $A = \mathbb{C}[G]$ el álgebra (compleja) del grupo G. Si $\alpha = a_1 1 + a_2 g + a_3 g^2$ y $\beta = b_1 1 + b_2 g + b_3 g^2 \in A$, donde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{C}$, entonces la suma de A está dada por

$$\alpha + \beta = (a_1 + b_1)1 + (a_2 + b_2)g + (a_3 + b_3)g^2$$

y el producto por

$$\alpha\beta = (a_1b_1 + a_2b_3 + a_3b_2)1 + (a_1b_2 + a_2b_1 + a_3b_3)g + (a_1b_3 + a_2b_2 + a_3b_1)g^2.$$

Si G es un grupo finito no trivial, entonces $K[G]$ posee ideales propios no triviales. Esto es porque el conjunto

$$I(G) = \left\{ \sum_{g\in G} \lambda_g g \in K[G] : \sum_{g\in G} \lambda_g = 0 \right\}$$

es un ideal propio y no nulo de $K[G]$ (pues $\dim I(G) = \dim K[G] - 1$). Este conjunto se conoce como el **ideal de aumentación** de $K[G]$.

Ejercicio 23.11. Sea $G = C_n$ el grupo ciclico de orden n (escrito multiplicativamente). Demuestre que $K[G] \simeq K[X]/(X^n - 1)$.

Proposición 23.12. *Si G es un grupo finito no trivial, entonces $K[G]$ tiene divisores de cero.*

Demostración. Sea $g \in G \setminus \{1\}$ y sea n el orden de g. Para ver que $K[G]$ tiene divisores de cero alcanza con observar que $(1-g)(1+g+\cdots+g^{n-1}) = 0$. □

Si A es un álgebra, entonces $\mathscr{U}(A)$ es el grupo de unidades del anillo A. La proposición que sigue se conoce como la propiedad universal del álgebra de grupo.

Proposición 23.13. *Sean A un álgebra y G un grupo finito. Si $f\colon G \to \mathscr{U}(A)$ es un morfismo de grupos, entonces existe un único morfismo $\varphi\colon K[G] \to A$ de álgebras tal que la restricción $\varphi|_G$ de φ al grupo G es igual a f, es decir $\varphi|_G = f$.*

Demostración. Como G es base de $K[G]$, puede verificarse que el morfismo φ de álgebras queda unívocamente determinado por

$$\varphi\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} \lambda_g f(g).$$ □

La proposición anterior nos dice que si G es un grupo finito y A es un álgebra, para definir un morfismo de álgebras $K[G] \to A$ alcanza con tener un morfismo de grupos $G \to \mathscr{U}(A)$.

Parte III
Módulos

Capítulo 24
Módulos

Un módulo sobre un anillo R será un grupo aditivo junto con un morfismo de anillos $R \to \mathrm{End}(M)$, que será la acción de R en M. Al traducir qué significa tener tal morfismo de anillos, obtenemos la siguiente definición:

Definición 24.1. Sea R un anillo. Un grupo abeliano aditivo M junto con una operación $R \times M \to M$, $(x,m) \mapsto x \cdot m$, será un **módulo** (a izquierda) sobre R (o también R-módulo a izquierda) si se cumplen las siguientes propiedades:

1) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ para todo $r_1, r_2 \in R$ y $m \in M$.
2) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ para todo $r \in R$ y $m_1, m_2 \in M$.
3) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ para todo $r_1, r_2 \in R$ y $m \in M$.
4) $1 \cdot m = m$ para todo $m \in M$.

Similarmente uno puede definir módulos a derecha.

Tabajaremos con módulos a izquierda, por lo tanto los llamaremos simplemente módulos y no habrá peligro de confusión. Muchas veces no haremos referencia al anillo sobre el que se define el módulo.

Ejemplo 24.2. Si R es un cuerpo, entonces un R-módulo es un espacio vectorial.

Ejemplo 24.3. Todo grupo abeliano es un $\mathbb{Z}$-módulo.

Ejemplo 24.4. Si R es un anillo, entonces R es un R-módulo con $x \cdot m = xm$. Este módulo es la **representación regular (a izquierda)** de R. La notación que utilizaremos para este módulo será $M = {}_R R$.

Ejemplo 24.5. Si R es un anillo, $R^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in R\}$ es un R-módulo con $r \cdot (x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$.

Ejemplo 24.6. Si R es un anillo, $M_{m,n}(R)$ es un R-módulo.

El siguiente ejemplo explica por qué es útil pedir que un morfismo f de anillos cumpla con la condición $f(1) = 1$.

Ejemplo 24.7. Si $f\colon R \to S$ es un morfismo de anillos y M es un S-módulo con la acción $(s,m) \mapsto sm$, entonces M es un R-módulo con $r \cdot m = f(r)m$ para $r \in R$ y $m \in M$. En efecto,

$$1 \cdot m = f(1)m = 1m = m,$$
$$r_1 \cdot (r_2 \cdot m) = f(r_1)(r_2 \cdot m) = f(r_1)(f(r_2)m) = (f(r_1)f(r_2))m = f(r_1r_2)m$$

para todo $r_1, r_2 \in R$ y $m \in M$.

El ejemplo siguiente es particularmente importante.

Ejemplo 24.8. Sean $R = \mathbb{R}[X]$, $T\colon \mathbb{R}^n \to \mathbb{R}^n$ una transformación lineal y $M = \mathbb{R}^n$, entonces M es un R-módulo con

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Ejemplo 24.9. Si $\{M_i | i \in I\}$ es una familia de módulos, entonces

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i \text{ para todo } i \in I\}$$

es un módulo con la operación $x \cdot (m_i)_{i\in I} = (x \cdot m_i)_{i\in I}$, donde el símbolo $(m_i)_{i\in I}$ denota a la función $I \to M_i$, $i \mapsto m_i$. Este módulo se conoce como el **producto directo** de los M_i.

Ejemplo 24.10. Si $\{M_i | i \in I\}$ es una familia de módulos, entonces

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i \text{ para todo } i \in I \text{ y } m_i = 0 \text{ salvo finitos } i \in I\}$$

es un módulo con la operación $x \cdot (m_i)_{i\in I} = (x \cdot m_i)_{i\in I}$. Este módulo se conoce como la **suma directa** de los M_i.

Ejercicio 24.11. Si M es un módulo, entonces

1) $0 \cdot m = 0$ para todo $m \in M$,
2) $x \cdot 0 = 0$ para todo $x \in R$ y además
3) $-m = (-1) \cdot m$ para todo $m \in M$.

Ejemplo 24.12. $M = \mathbb{Z}/6$ es un $\mathbb{Z}$-módulo tal que $3 \cdot 2 = 0$ pero $3 \neq 0$ (en $\mathbb{Z}$) y $2 \neq 0$ (en $\mathbb{Z}/6$).

Definición 24.13. Sea M un R-módulo. Un subconjunto S de M será un **submódulo** de M si $(S,+)$ es un subgrupo de $(M,+)$ y además $x \cdot s \in S$ para todo $x \in R$ y $s \in S$.

Ejemplos 24.14. Sea M un R-módulo.

1) $\{0\}$ y M son submódulos de M.
2) Si R es un cuerpo, S es un submódulo de M si y sólo si S es un subespacio de M.

3) Si $R = \mathbb{Z}$, entonces S es un submódulo si y sólo si S es un subgrupo de M.

Ejemplo 24.15. Si $M = {}_RR$, entonces $S \subseteq M$ es un submódulo si y sólo si S es un ideal a izquierda de R

Ejemplo 24.16. Si V es un espacio vectorial y $T\colon V \to V$ es una transformación lineal, entonces V es un $K[X]$-módulo con

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Un submódulo W será entonces un subespacio T-invariante de V, es decir un subspacio vectorial de V tal que $T(W) \subseteq W$.

Ejercicio 24.17. Demuestre que un subconjunto S de M es un submódulo si y sólo si $r_1 s_1 + r_2 s_2 \in S$ para todo $r_1, r_2 \in R$ y ${}_1, s_2 \in S$.

Ejercicio 24.18. Si S y T son submódulos de M, entonces

$$S + T = \{s + t : s \in S, t \in T\}$$

es un submódulo de M.

Definición 24.19. Sean M y N módulos sobre R. Un **morfismo** de módulos es una función $f\colon M \to N$ tal que $f(x+y) = f(x) + f(y)$ y $f(r \cdot x) = r \cdot f(x)$ para todo $x, y \in M$ y $r \in R$.

Sea $\mathrm{Hom}_R(M,N)$ el conjunto de morfismos de módulos $M \to N$.

Ejercicio 24.20. Sea $f\colon M \to N$ un morfismo de módulos.

1) Si S es un submódulo de M, entonces $f(S)$ es un submódulo de N.
2) Si T es un submódulo de N, entonces $f^{-1}(T)$ es un submódulo de M.

Si $f \in \mathrm{Hom}_R(M,N)$, se define el **núcleo** de f como el submódulo

$$\ker f = f^{-1}(\{0\}) = \{m \in M : f(m) = 0\}$$

de M. Diremos que f es un **monomorfismo** si f es inyectiva, que es un **epimorfismo** si f es sobreyectiva y que es un **isomorfismo** si f es biyectiva.

Ejercicio 24.21. Sea $f \in \mathrm{Hom}_R(M,N)$. Son equivalentes:

1) f es monomorfismo.
2) $\ker f = \{0\}$.
3) Para todo módulo T y todo $g, h \in \mathrm{Hom}_R(T,M)$, $f \circ g = f \circ h \implies g = h$.
4) Para todo módulo T y todo $g \in \mathrm{Hom}(T,M)$, $f \circ g = 0 \implies g = 0$.

Ejemplo 24.22. Sea $R = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}$. Veamos que $\begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix} \not\cong \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix}$ como R-módulos, donde la estructura de módulos está dada por la multiplicación usual de matrices. Sea $f\colon \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix} \to \begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix}$ un isomorfismo de módulos y sea $x_0 \in \mathbb{R} \setminus \{0\}$ tal que $f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_0 \\ 0 \end{pmatrix}$. Entonces

$$f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = f\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

una contradicción pues f es inyectiva.

Si S y T son submódulos de M, diremos que M es **suma directa** de S y T si $M = S + T$ y además $S \cap T = \{0\}$. La notación que utilizaremos en este caso será $M = S \oplus T$. Observemos que si $M = S \oplus T$, entonces todo $m \in M$ puede escribirse unívocamente como $m = s + t$ para ciertos $s \in S$ y $t \in T$. En efecto, la descomposición existe gracias a que $M = S + T$. Si $m \in M$ se descompone como $m = s + t = s_1 + t_1$, donde $s, s_1 \in S$ y $t, t_1 \in T$, entonces $-s_1 + s = t_1 - t \in S \cap T = \{0\}$ y luego $s = s_1$ y $t = t_1$. Si $M = S \oplus T$, el submódulo S es un **sumando directo** de M y el submódulo T es un **complemento** para S en M.

Ejemplos 24.23.

1) Para todo módulo M, los submódulos $\{0\}$ y M son sumandos directos de M.
2) Si $M = \mathbb{R}^2$ con la estructura usual de espacio vectorial, entonces todo subespacio de M es un sumando directo.

Ejemplo 24.24. Si $M = \mathbb{Z}$ como $\mathbb{Z}$-módulo, $m\mathbb{Z}$ es sumando directo de M si y sólo si $m \in \{0, 1\}$, pues $n\mathbb{Z} \cap m\mathbb{Z} = \{0\}$ si y sólo si $nm = 0$.

Proposición 24.25. *Un módulo N es isomorfo a un sumando directo del módulo M si y sólo si existen morfismos $i\colon N \to M$ y $p\colon M \to N$ tales que $p \circ i = \mathrm{id}_N$. En este caso, $M = \ker p \oplus i(N)$.*

Demostración. Supongamos que N es isomorfo a un sumando directo de M, es decir $M = S \oplus T$ y sea $s\colon N \to S$ un isomorfismo. Para cada $m \in M$ existen únicos $s \in S$ y $t \in T$ tales que $m = s + t$. Definimos entonces el epimorfismo $q\colon M \to S$, $m \mapsto s$. Observemos que $q(m) = m$ si y sólo si $m \in S$, es decir que q es un **proyector** de M sobre S con respecto a T. Definimos además el morfismo $i\colon N \to M$, $n \mapsto s(n)$, y el morfismo $p\colon M \to N$, $m \mapsto s^{-1}(q(m))$. Como $s(n) \in S$,

$$p(i(n)) = p(s(n)) = s^{-1}(q(s(n))) = s^{-1}(s(n)) = n$$

para todo $n \in N$.

Demostremos ahora la recíproca. Afirmamos que i es monomorfismo: si $i(n) = 0$, entonces $n = p(i(n)) = p(0) = 0$. Luego $i\colon N \to i(N)$ es un isomorfismo. Veamos ahora que $M = \ker p \oplus i(N)$. Si $m \in M$, entonces

$$m = m - i(p(m)) + i(p(m)) \in \ker p + i(N),$$

pues $p(m - i(p(m))) = p(m) - p(m) = 0$. Si $m \in \ker p \cap i(N)$, entonces $0 = p(m)$ y además $m = i(n)$ para algún $n \in N$. Entonces $0 = p(m) = p(i(n)) = n$ y luego $m = 0$. □

La **suma directa** de submódulos puede extenderse a un número finito de sumandos. Si $S_1, \ldots, S_n$ son submódulos de M, diremos que $M = S_1 \oplus \cdots \oplus S_n$ si todo $m \in M$ puede escribirse unívocamente como $m = s_1 + \cdots + s_n$ para ciertos $s_1 \in S_1, \ldots, s_n \in S_n$.

Ejercicio 24.26. Demuestre que $M = S_1 \oplus \cdots \oplus S_n$ si y sólo si $M = S_1 + \cdots + S_n$ y además

$$S_i \cap \left(\sum_{j \neq i} S_j \right) = \{0\}$$

para todo $i \in \{1, \ldots, n\}$.

Ejercicio 24.27. Si $\{S_i : i \in I\}$ es una familia de submódulos de M, entonces $\cap_{i \in I} S_i$ es un submódulo de M.

Ejemplo 24.28. Sea $T : \mathbb{R}^2 \to \mathbb{R}^2$, $T(x,y) = (0,y)$ y sea $M = \mathbb{R}^2$ con la estructura de $\mathbb{R}[X]$-módulo dada por

$$\left(\sum_{i=0}^{n} a_i X^i \right) \cdot (x,y) = \sum_{i=0}^{n} a_i T^i(x,y).$$

Vamos a demostrar que $\{0\}$, M, $\mathbb{R} \times \{0\}$ y $\{0\} \times \mathbb{R}$ son los únicos submódulos de M. Si N es un submódulo no nulo de M, sea $(x_0, y_0) \in N \setminus \{(0,0)\}$. Si $(x,y) \in M$ es tal que $xy \neq 0$, entonces

$$\left(\frac{x}{x_0} + \left(\frac{y}{y_0} - \frac{x}{x_0} \right) X \right) \cdot (x_0, y_0) = (x,y)$$

y luego $N = M$. Si $y_0 = 0$, entonces $N = \mathbb{R} \times \{0\}$, pues $\frac{x}{x_0} \cdot (x_0, 0) = (x,0)$. Si $x_0 = 0$, entonces $N = \{0\} \times \mathbb{R}$, pues $\frac{y}{y_0} \cdot (0, y_0) = (0,y)$

Ejemplo 24.29. Sea $M = \mathbb{R}^2$ como $\mathbb{R}[X]$-módulo con la acción

$$\left(\sum_{i=0}^{n} a_i X^i \right) \cdot (x,y) = \sum_{i=0}^{n} a_i T^i(x,y),$$

donde $T : M \to M$, $T(x,y) = (y,x)$. Vamos a calcular todos los submódulos de M. Si $N \subseteq M$ es un submódulo entonces N es un espacio vectorial real. Supongamos que $N \neq \{(0,0)\}$ y que $N \neq \mathbb{R}^2$. Como entonces $\dim N = 1$, sea $\{(a_0, b_0)\}$ una base de N. Como N es un submódulo, $(b_0, a_0) = X \cdot (a_0, b_0) \in N$. En particular, existe $\lambda \in \mathbb{R}$ tal que $(b_0, a_0) = \lambda (a_0, b_0)$. Como $(a_0, b_0) \neq (0,0)$, sin perder generalidad podemos

suponer que $a_0 \neq 0$. Esto implica que $\lambda^2 a_0 = \lambda(\lambda a_0) = \lambda b_0 = a_0$ y entonces $\lambda^2 = 1$. Si $\lambda = 1$, entonces $a_0 = b_0$. Si $\lambda = -1$, entonces $a_0 = -b_0$. En conclusión, N está generado por $(1,1)$ o por $(1,-1)$.

Ejemplo 24.30. Si V es un espacio vectorial y $T\colon V \to V$ es una transformación lineal, entonces V es un $K[X]$-módulo con

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Si $g\colon V \to V$ es un morfismo de $K[X]$-módulos, entonces g conmuta con T, pues

$$(g \circ T)(v) = g(T(v)) = g(X \cdot v) = X \cdot g(v) = T(g(v)) = (T \circ g)(v)$$

para todo $v \in V$.

Ejemplo 24.31. Veamos que $\mathrm{Hom}_R(M,N)$ es un $Z(R)$-módulo. Si $f \in \mathrm{Hom}_R(M,N)$ y $r \in R$, definimos la función $r \cdot f\colon M \to N$, $m \mapsto f(r \cdot m)$, que es un morfismo de grupos abelianos. Si $r,s \in Z(R)$, entonces f es un morfismo pues

$$\begin{aligned}(r \cdot (s \cdot f))(m) &= (s \cdot f)(r \cdot m) \\ &= f(s \cdot (r \cdot m)) = f((sr) \cdot m) = f((rs) \cdot m) = ((rs) \cdot f)(m).\end{aligned}$$

Si M es un módulo y N es un submódulo, entonces M/N es un grupo abeliano y el morfismo canónico $\pi\colon M \to M/N$, $x \mapsto x+N$, es un morfismo sobreyectivo de grupos. Veamos que el **cociente** M/N es un módulo con

$$r \cdot (x+N) = (r \cdot x) + N,$$

donde $r \in R$ y $x \in M$. Para esto, tenemos que ver la buena definición de la acción en M/N. Si $x+N = y+N$, entonces, como $x-y \in N$, se tiene que

$$r \cdot x - r \cdot y = r \cdot (x-y) \in N,$$

es decir $r \cdot (x+N) = r \cdot (y+N)$. Dejamos como ejercicio demostrar que la función $\pi\colon M \to M/N$, $x \mapsto x+N$, es un morfismo sobreyectivo de módulos.

Ejemplo 24.32. Si $R = M = \mathbb{Z}$ y $N = 2\mathbb{Z}$, entonces $M/N \simeq \mathbb{Z}/2$.

Ejemplo 24.33. Sea R un anillo conmutativo. Veamos que $M \simeq \mathrm{Hom}_R({}_R R, M)$. Como R es un anillo conmutativo, $\mathrm{Hom}_R({}_R R, M)$ es un módulo, ver ejemplo 24.31. Sea $\varphi\colon M \to \mathrm{Hom}_R({}_R R, M)$, $m \mapsto f_m$, donde $f_m\colon R \to M$, $r \mapsto r \cdot m$. Para ver que φ está bien definida hay que observar que $\varphi(m) \in \mathrm{Hom}_R({}_R R, M)$, es decir

$$f_m(r+s) = (r+s) \cdot m = r \cdot m + s \cdot m, \quad f_m(rs) = (rs) \cdot m = r \cdot (s \cdot m) = r \cdot f_m(s).$$

Para ver que φ es morfismo primero vemos que $\varphi(m+n) = \varphi(m) + \varphi(n)$ para todo $m,n \in M$, pues

$$\begin{aligned}\varphi(m+n)(r) &= f_{m+n}(r) = r\cdot(m+n)\\ &= r\cdot m + r\cdot n = f_m(r)+f_n(r) = \varphi(m)(r)+\varphi(n)(r).\end{aligned}$$

Además $\varphi(r\cdot m) = r\cdot\varphi(m)$ para todo $r\in R$ y $m\in M$, pues

$$\begin{aligned}\varphi(r\cdot m)(s) &= f_{r\cdot m}(s) = s\cdot(r\cdot m) = (sr)\cdot m\\ &= (rs)\cdot m = f_m(rs) = \varphi(m)(rs) = (r\cdot\varphi(m))(s).\end{aligned}$$

Falta ver que φ es un isomorfismo. Veamos primero que φ es monomorfismo. Si $\varphi(m)=0$, entonces $r\cdot m = \varphi(m)(r) = 0$ para todo $r\in R$. En particular, $m = 1\cdot m = 0$. Veamos ahora que φ es epimorfismo. Si $f\in \mathrm{Hom}_R({}_RR, M)$, sea $m = f(1)$. Entonces $\varphi(m) = f$ pues $\varphi(m)(r) = r\cdot m = r\cdot f(1) = f(r)$.

Tal como hicimos con grupos, puede demostrarse que si M es un módulo y N es un submódulo de M, el par $(M/N, \pi\colon M\to M/N)$ tiene las siguientes propiedades:

1) $N\subseteq \ker\pi$.
2) Si $f\colon M\to T$ es un morfismo tal que $N\subseteq\ker f$, entonces existe un único morfismo $\varphi\colon M/N\to T$ tal que $\varphi\circ\pi = f$.

Recordemos que si S y T son submódulos de un módulo M, entonces $S\cap T$ y $S+T = \{s+t : s\in S, t\in T\}$ son ambos submódulos de M. Se tienen entonces los teoremas de isomorfismos.

1) Si $f\in\mathrm{Hom}_R(M,N)$, entonces $M/\ker f\simeq f(M)$.
2) Si $T\subseteq N\subseteq M$ son submódulos, entonces

$$\frac{M/T}{N/T}\simeq M/N$$

3) Si S y T son submódulos de M, entonces $(S+T)/S\simeq T/(S\cap T)$.

Ejemplo 24.34. Si R es un cuerpo y V es un R-módulo, entonces V es un espacio vectorial. Si S y T son subespacios de V, entonces son submódulos de V. El segundo teorema de isomorfismos nos dice que $(S+T)/T\simeq S/(S\cap T)$, un isomorfismo de espacios vectoriales. Al aplicar dimensión,

$$\dim(S+T)-\dim T = \dim(S)-\dim(S\cap T).$$

Ejemplo 24.35. Si S es un sumando directo de M y T es un complemento para S, entonces $T\simeq M/S$, pues

$$M/S = (S\oplus T)/S\simeq T/(S\cap T) = T/\{0\}\simeq T$$

por el segundo teorema de isomorfismos. Luego todos los complementos de S en M serán isomorfos.

Puede demostrarse además el teorema de la correspondencia, que afirma que existe una correspondencia biyectiva entre los submódulos de M/N y los submó-

dulos de M que contienen a N. La correspondencia está dada por $S \mapsto \pi^{-1}(S)$ y $\pi(T) \hookleftarrow T$.

Ejercicio 24.36. Sea $f \in \mathrm{Hom}_R(M,N)$. Son equivalentes:

1) f es epimorfismo.
2) $N/f(M) \simeq \{0\}$.
3) Para todo módulo T y todo $g,h \in \mathrm{Hom}_R(N,T)$, $g \circ f = h \circ f \implies g = h$.
4) Para todo módulo T y todo $g \in \mathrm{Hom}_R(N,T)$, $g \circ f = 0 \implies g = 0$.

Ejercicio 24.37. Sea R un anillo conmutativo y sean M_1 y M_2 ideales maximales de R. Pruebe que $R/M_1 \simeq R/M_2$ como R-módulos si y sólo si existe $r \in R \setminus M_2$ tal que $rM_1 \subseteq M_2$.

Capítulo 25
El teorema de Maschke

Si G es un grupo finito, un morfismo de grupos $G \to \mathbf{GL}(V)$, donde V es un espacio vectorial complejo de dimensión finita, se dice una **representación** de G. Si el espacio vectorial V tiene dimensión n, al fijar una base para V podemos considerar $G \to \mathbf{GL}(V) \simeq \mathbf{GL}_n(\mathbb{C})$.

Ejemplo 25.1. Como $\mathbb{S}_3 = \langle (12), (123) \rangle$, la función $\rho : \mathbb{S}_3 \to \mathbf{GL}_3(\mathbb{C})$,

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

es una representación de $\mathbb{S}_3$.

Ejemplo 25.2. Como el grupo de cuaterniones $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ está generado por $\{i, j\}$, la función $\rho : G \to \mathbf{GL}_2(\mathbb{C})$,

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

es una representación de Q_8.

Ejemplo 25.3. Sea $G = \langle g \rangle$ cíclico de orden seis. La función $\rho : G \to \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

es una representación del grupo G cíclico de orden seis.

Ejemplo 25.4. Sea $G = \langle g \rangle$ cíclico de orden cuatro. La función $\rho : G \to \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

es una representación del grupo G cíclico de orden cuatro.

Observemos que existe una correspondencia biyectiva

$$\{\text{representaciones de } G\} \leftrightarrow \{\mathbb{C}[G]\text{-módulos de dimensión finita}\}.$$

Si $\rho\colon G \to \mathbf{GL}(V)$ es una representación, entonces V es un $\mathbb{C}[G]$-módulo con

$$\left(\sum_{g\in G} \lambda_g g\right)\cdot v = \sum_{g\in G} \lambda_g \rho(g)(v).$$

Recíprocamente, si V es un $\mathbb{C}[G]$-módulo, entonces $\rho\colon G \to \mathbf{GL}(V)$, $\rho(g)(v) = g\cdot v$, es una representación de G en V. Puede verificarse que estas construcciones son una la inversa de la otra.

Definición 25.5. Un módulo M se dice **simple** (o irreducible) si $M \neq \{0\}$ y M no tiene submódulos propios no triviales.

Ejemplo 25.6. Si A es un álgebra, vimos que todo A-módulo es un espacio vectorial. Los módulos de dimensión uno serán entonces módulos simples.

Ejemplo 25.7. Sea $G = \langle g\rangle$ cíclico de orden tres y sea $M = \mathbb{R}^3$ con la estructura de $\mathbb{R}[G]$-módulo dada por $g\cdot(x,y,z) = (y,z,x)$. El conjunto

$$N = \{(x,y,z) \in \mathbb{R}^3 : x+y+z = 0\}$$

es un submódulo de M. Veamos que N es simple. Si N contiene un submódulo no trivial S, sea $(x_0,y_0,z_0) \in S \setminus \{(0,0,0)\}$. Como S es un submódulo,

$$(y_0,z_0,x_0) = g\cdot(x_0,y_0,z_0) \in S.$$

Afirmamos que $\{(x_0,y_0,z_0),(y_0,z_0,x_0)\}$ es un conjunto linealmente independiente. Si existe $\lambda \in \mathbb{R}$ tal que $\lambda(x_0,y_0,z_0) = (y_0,z_0,x_0)$, entonces $x_0 = \lambda^3 x_0$. Como $x_0 = 0$ implica que $y_0 = z_0 = 0$, entonces $\lambda = 1$. En particular, $x_0 = y_0 = z_0$, una contradicción, pues $x_0+y_0+z_0 = 0$. Luego $\dim S = 2$ y entonces $S = N$.

Ejemplo 25.8. Sea $M = \mathbb{R}^2$ con la estructura de $\mathbb{R}[X]$-módulo dada por

$$\left(\sum_{i=0}^{n} a_i X^i\right)\cdot m = \sum_{i=0}^{n} a_i T^i(m).$$

donde $T\colon \mathbb{R}^2 \to \mathbb{R}^2$, $T(x,y) = (y,-x)$. Veamos que M es simple. Si N es un submódulo no nulo, sea $(x_0,y_0) \in N \setminus \{(0,0)\}$. Si $(x,y) \in M$, veamos que existen $\alpha,\beta \in \mathbb{R}$ tales que

$$(\alpha+\beta X)\cdot(x_0,y_0) = (x,y).$$

En efecto, basta tomar

$$\alpha = \frac{x_0x+y_0y}{x_0^2+y_0^2}, \quad \beta = \frac{y_0x-x_0y}{x_0^2+y_0^2},$$

pues

$$\begin{aligned}(\alpha+\beta X)\cdot(x_0,y_0) &= \alpha(x_0,y_0)+\beta\cdot(X\cdot(x_0,y_0))\\ &= (\alpha x_0,\alpha y_0)+(\beta y_0,-\beta x_0)\\ &= (\alpha x_0+\beta y_0,\alpha y_0-\beta x_0)\\ &= (x,y).\end{aligned}$$

Definición 25.9. Un módulo M se dice **semisimple** (o completamente reducible) si es suma directa de módulos simples.

Vimos en el capítulo anterior que si M es un módulo, se dice que un submódulo S de M se complementa en M si existe un submódulo T de M tal que $M = S \oplus T$.

Lema 25.10. *Si $p\colon M \to M$ es un morfismo tal que $p^2 = p$, entonces*

$$M = \ker p \oplus p(M).$$

Demostración. Como p es un morfismo, $\ker p$ y $p(M)$ son submódulos de M. Para ver que $M = \ker p + p(M)$ alcanza con observar que todo $m \in M$ puede escribirse como $m = (m - p(m)) + p(m)$ y que $m - p(m) \in \ker p$ pues

$$p(m-p(m)) = p(m) - p^2(m) = p(m) - p(m) = 0.$$

Veamos ahora que $\ker p \cap p(M) = \{0\}$. Si $m \in \ker p \cap p(M)$, escribimos $m = p(m_1)$ para algún $m_1 \in M$. Como entonces $0 = p(m) = p^2(m_1) = m_1$, se concluye que $m = 0$. □

Recordemos que una **proyección** (o proyector) de un módulo M es un morfismo $p\colon M \to M$ tal que $p^2 = p$.

Lema 25.11. *Si A es un álgebra y M es un A-módulo de dimensión finita tal que todo submódulo de M se complementa, entonces M es semisimple.*

Demostración. Procederemos por inducción en $\dim M$. Si $M = \{0\}$ el resultado es trivial. Si $M \neq \{0\}$, sea S un submódulo no nulo de M de dimensión minimal. En particular, S es simple. Por hipótesis sabemos que existe un submódulo T de M tal que $M = S \oplus T$. Como $\dim T < \dim M$, la hipótesis inductiva implica que T es suma directa de módulos simples. Luego M también lo es. □

El lema anterior vale también para módulos arbitrarios sobre anillos. Sin embargo, la demostración requiere el uso del lema de Zorn.

Ejemplo 25.12. Sea $R = M_2(\mathbb{C})$ y sea $M = {}_RR$. Los subconjuntos

$$I = \begin{pmatrix}\mathbb{C} & 0\\ \mathbb{C} & 0\end{pmatrix}, \quad J = \begin{pmatrix}0 & \mathbb{C}\\ 0 & \mathbb{C}\end{pmatrix}$$

son submódulos de M tales que $M \simeq I \oplus J$. Veamos que M es semisimple, es decir que I y J son simples.

Si S es un submódulo no nulo de I, sea $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \in S$ no nulo. Supongamos que $a \neq 0$, el caso $c \neq 0$ es similar. Entonces

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Análogamente se demuestra que $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in S$. Luego $S = I$ y entonces I es simple. La misma técnica nos permite demostrar que J es simple.

Es importante observar que si A es un álgebra y M es un módulo semisimple de dimensión finita, entones M es suma directa de finitos simples.

Teorema 25.13 (Maschke). *Sea G un grupo finito y sea M un $\mathbb{C}[G]$-módulo de dimensión finita. Entonces M es semisimple.*

Demostración. Gracias al lema anterior, alcanza con demostrar que todo submódulo S de M se complementa. Como, en particular, S es un subespacio de M, existe un subespacio T_0 de M tal que $M = S \oplus T_0$ (como espacios vectoriales). Vamos a usar el espacio vectorial T_0 para construir un submódulo T de M que complementa a S. Como $M = S \oplus T_0$, cada $m \in M$ puede escribirse unívocamente como $m = s + t_0$ para ciertos $s \in S$ y $t_0 \in T$. Podemos definir entonces la transformación lineal

$$p_0 \colon M \to S, \quad p_0(m) = s,$$

donde $m = s + t_0$ con $s \in S$ y $t_0 \in T$. Observemos que si $s \in S$, entonces $p_0(s) = s$. En particular, $p_0^2 = p_0$ pues $p_0(m) \in S$.

El problema es que p_0 no es, en general, un morfismo de $\mathbb{C}[G]$-módulos. Promediamos sobre el grupo G para conseguir un morfismo de grupos: Sea

$$p \colon M \to S, \quad p(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_0(g \cdot m).$$

Primero demostramos que p es un morfismo de $\mathbb{C}[G]$-módulos. Alcanza con ver que $p(g \cdot m) = g \cdot p(m)$ para todo $g \in G$ y $m \in M$. En efecto,

$$p(g \cdot m) = \frac{1}{|G|} \sum_{h \in G} h^{-1} \cdot p_0(h \cdot (g \cdot m)) = \frac{1}{|G|} \sum_{h \in G} (gh^{-1}) \cdot p_0(h \cdot m) = g \cdot p(m).$$

Veamos ahora que $p(M) = S$. La inclusión $\subseteq$ es trivial, pues S es un submódulo de M y además $p_0(M) \subseteq S$. Recíprocamente, si $s \in S$, entonces $g \cdot s \in S$, pues S es un submódulo. Luego $s = g^{-1} \cdot (g \cdot s) = g^{-1} \cdot p_0(g \cdot s)$ y en consecuencia

$$s = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (g \cdot s) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (p_0(g \cdot s)) = p(s).$$

Como $p(m) \in S$ para todo $m \in M$, entonces $p^2(m) = p(m)$, es decir que p es un proyector en S. Luego S se complementa en M, es decir $M = S \oplus \ker(p)$. □

La misma demostración del teorema de Maschke vale para el álgebra de grupo real o racional. La descomposición de un módulo sobre el álgebra de grupo dependerá fuertemente del cuerpo sobre el que se trabaje.

Ejemplo 25.14. Sea $G = \langle g \rangle$ el grupo cíclico de orden cuatro y sea $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Sea $M = \mathbb{C}^{2\times 1}$ con la estructura de $\mathbb{C}[G]$-módulo dada por

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix},$$

es decir, si $a, b, c, d \in \mathbb{C}$, entonces

$$(a1 + bg + cg^2 + dg^3) \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} (a-d)u + (c-b)v \\ (1-b)u + (a-d)v \end{pmatrix}.$$

Sabemos por el teorema de Maschke que M es semisimple. Veamos cómo descomponer el módulo M como suma directa de simples. Como $\dim M = 2$, tendremos que M es suma directa de dos submódulos de dimensión uno. Observemos que si S es un submódulo tal que $\{0\} \subsetneq S \subsetneq M$, entonces $\dim S = 1$. Además

$$S = \left\{ \lambda \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} : \lambda \in \mathbb{C} \right\} \text{ es un submódulo de } M \iff \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} \text{ es autovector de } \rho_g.$$

Como la matriz ρ_g tiene polinomio característico $X^2 + 1$, se sigue que $\begin{pmatrix} i \\ 1 \end{pmatrix}$ es autovector de ρ_g de autovalor $-i$ y que $\begin{pmatrix} -i \\ 1 \end{pmatrix}$ es autovector de autovalor i. Luego M se descompone en suma directa de simples como

$$M = \mathbb{C} \begin{pmatrix} i \\ 1 \end{pmatrix} \oplus \mathbb{C} \begin{pmatrix} -i \\ 1 \end{pmatrix}$$

Observar que en ejemplo anterior pudimos descomponer a la matriz ρ_g gracias a la existencia de autovectores, algo que no pasaría si consideramos módulos sobre el álgebra de grupo real.

Ejemplo 25.15. Sea $G = \langle g \rangle$ el grupo cíclico de orden cuatro y sea $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Sea $M = \mathbb{R}^{2\times 1}$ con la estructura de $\mathbb{R}[G]$-módulo dada por

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix}.$$

Tal como hicimos en el ejemplo anterior, como $\dim M = 2$, si S es un submódulo de M tal que $\{0\} \subsetneq S \subsetneq M$, entonces $\dim S = 1$. Pero como ρ_g no tiene autovectores reales, M no tendrá submódulos de dimensión uno. En consecuencia, M es simple como $\mathbb{R}[G]$-módulo.

Capítulo 26
Sucesiones exactas

Definición 26.1. Sea $M_1, M_2, \ldots$ una sucesión de R-módulos y para cada $n \in \mathbb{N}$ sea $f_n \colon M_n \to M_{n-1}$ un morfismo. Diremos que la sucesión

$$\cdots \xrightarrow{f_{n+2}} M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \cdots$$

de módulos y morfismos es **exacta** si $\ker f_n = f_{n+1}(M_{n+1})$ para todo $n \in \mathbb{N}$.

En general nos encontraremos con **sucesiones exactas cortas**, es decir decir, sucesiones de la forma

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0, \tag{26.1}$$

donde la exactitud significa que f es monomorfismo, g es epimorfismo y que $f(M) = \ker g$.

Ejemplos 26.2. La sucesión

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

es exacta si y sólo si f es un monomorfismo. Similarmente, la sucesión

$$M \xrightarrow{g} N \longrightarrow 0$$

es exacta si y sólo si g es un epimorfismo.

Ejemplo 26.3. La sucesión

$$0 \longrightarrow M \xrightarrow{f} M \oplus N \xrightarrow{g} N \longrightarrow 0, \tag{26.2}$$

donde $f(m) = (m, 0)$ y $g(m, n) = n$, es exacta.

Nos interesa saber cuándo una sucesión exacta 26.1 es de la forma (26.2). Para eso necesitamos algunas definiciones.

Definición 26.4. Sea $f \in \mathrm{Hom}_R(M,N)$. Diremos que el morfismo f es una **sección** si existe $g \in \mathrm{Hom}_R(N,M)$ tal que $g \circ f = \mathrm{id}_M$.

Definición 26.5. Sea $f \in \mathrm{Hom}_R(M,N)$. Diremos que el morfismo f es una **retracción** si existe $g \in \mathrm{Hom}_R(N,M)$ tal que $f \circ g = \mathrm{id}_N$.

Dejamos como ejercicio demostrar que una sección es siempre inyectiva. La afirmación recíproca no es cierta, ya que la inclusión $2\mathbb{Z} \hookrightarrow \mathbb{Z}$ de Z-módulos es un monomorfismo que no es una sección. Similarmente, una retracción es siempre sobreyectiva y la recíproca no es cierta ya que por ejemplo $\mathbb{Z} \to \mathbb{Z}/2$ es un epimorfismo de $\mathbb{Z}$-módulos que no es una retracción.

Definición 26.6. La sucesión exacta

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

y la sucesión exacta

$$0 \longrightarrow A_1 \longrightarrow B_1 \longrightarrow C_1 \longrightarrow 0$$

se dirán **equivalentes** (o isomorfas) si existen isomorfismos α, β y γ tales que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \end{array} \tag{26.3}$$

es conmutativo.

El siguiente lema es de gran utilidad, aunque bastante técnico.

Lema 26.7 (de los cinco). *Si el diagrama*

$$\begin{array}{ccccccccc} A & \xrightarrow{r} & B & \xrightarrow{s} & C & \xrightarrow{t} & D & \xrightarrow{u} & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ A_1 & \xrightarrow{r_1} & B_1 & \xrightarrow{s_1} & C_1 & \xrightarrow{t_1} & D_1 & \xrightarrow{u_1} & E_1 \end{array} \tag{26.4}$$

es conmutativo y con filas exactas, valen las siguientes afirmaciones:

1) Si α es epimorfismo y β y δ son monomorfismos, entonces γ es monomorfismo.
2) Si ε es monomorfismo y β y δ son epimorfismos, entonces γ es epimorfismo.
3) Si α, β, δ y ε son isomorfismos, entonces γ es isomorfismo.

Demostración. Demostremos la primera afirmación. Sea $c \in C$ tal que $\gamma(c) = 0$. Queremos ver que $c = 0$. Como $\gamma(c) = 0$, entonces $\delta(t(c)) = t_1(\gamma(c)) = 0$. Como δ es inyectiva, $t(c) = 0$, es decir $c \in \ker t = s(B)$. En particular, $c = s(b)$ para algún $b \in B$. Si $b_1 = \beta(b)$, entonces

$$s_1(b_1) = s_1(\beta(b)) = \gamma(s(b)) = \gamma(c) = 0$$

y entonces $b_1 \in \ker s_1 = r_1(A_1)$. En particular, $b_1 = r_1(a_1)$ para algún $a_1 \in A_1$. Como α es epimorfismo, $a_1 = \alpha(a)$ para algún $a \in A$. Entonces

$$\beta(b) = b_1 = r_1(a_1) = r_1(\alpha(a)) = \beta(r(a))$$

y luego $b - r(a) \in \ker\beta = \{0\}$, es decir $b = r(a)$. En conclusión,

$$c = s(b) = s(r(a)) = 0.$$

Demostremos la segunda afirmación. Sea $c_1 \in C_1$. Queremos ver que $c_1 = \gamma(c)$ para algún $c \in C$. Sea $d_1 = t_1(c_1)$. Como δ es epimorfismo, $d_1 = \delta(d)$ para algún $d \in D$. Entonces

$$u_1(\delta(d)) = u_1(t_1(c_1)) = 0$$

y luego $\delta(d) \in \ker u_1$. Como $0 = u_1(\delta(d)) = \varepsilon(u(d))$ y ε es un monomorfismo, entonces $u(d) = 0$, es decir $d \in \ker u = t(C)$. En consecuencia, $d = t(c)$ para algún $c \in C$. Como

$$t_1(c_1) = d_1 = \delta(d) = \delta(t(c)) = t_1(\gamma(c)),$$

entonces $c_1 - \gamma(c) \in \ker t_1 = s_1(B_1)$, lo que significa que $c_1 - \gamma(c) = s_1(b_1)$ para algún $b_1 \in B_1$. Como β es un epimorfismo, $b_1 = \beta(b)$ para algún $b \in B$. Luego $c_1 - \gamma(c) = s_1(\beta(b)) = \gamma(s(b))$ y entonces $c_1 = \gamma(c) + \gamma(s(b)) = \gamma(c + s(b))$. □

Ejercicio 26.8. Consideremos el diagrama conmutativo

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ X_1 & \xrightarrow{f_1} & Y_1 & \xrightarrow{g_1} & Z_1 \end{array}$$

y supongamos que tiene filas exactas. Demuestre las siguientes afirmaciones:

1) Si α, γ y f_1 son monomorfismos entonces β es monomorfismo.
2) Si α, γ y g son epimorfismos entonces β es epimorfismo.
3) Si β es monomorfismo y α y g son epimorfismos entonces γ es monomorfismo.
4) Si β es epimorfismo y f_1 y γ son monomorfismos entonces α es epimorfismo.

Proposición 26.9. *Si*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es exacta, las siguientes afirmaciones son equivalentes:

1) f es una sección.
2) g es una retracción.

3) Existen un isomorfismo φ de forma que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & T & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & M \oplus T & \longrightarrow & T & \longrightarrow & 0 \end{array} \tag{26.5}$$

es conmutativo.

Demostración. Veamos que (2) $\Longrightarrow$ (3). Como g es una retracción, existe un morfismo $h\colon T \to N$ tal que $g \circ h = \mathrm{id}_T$. Sea $\varphi\colon M \oplus T \to N$, $\varphi(m,t) = f(m) + h(t)$. Entonces φ es morfismo y el diagrama (26.5) es conmutativo pues

$$(g \circ \varphi)(m,t) = g(f(m)) + h(t)) = t, \quad \varphi(m,0) = f(m).$$

Para ver que φ es un isomorfismo, se utiliza el lema de los cinco.

La demostración de la implicación (1) $\Longrightarrow$ (3) es similar. Como f es una sección, existe un morfismo $h\colon N \to M$ tal que $h \circ f = \mathrm{id}_M$. Hay que usar entonces la función $\psi\colon N \to M \oplus T$, $n \mapsto (h(n), g(n))$, pues

$$\begin{aligned} &\psi(f(m)) = (h(f(m)), g(f(m))) = (m,0) = i_1(m), \\ &p_2(\psi(n)) = p_2(h(n), g(n)) = g(n). \end{aligned}$$

Como ψ es un isomorfismo gracias al lema de los cinco, $\varphi = \psi^{-1}$.

Para ver que (3) $\Longrightarrow$ (2), consideramos el diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & T & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & M & \underset{p_1}{\overset{i_1}{\rightleftarrows}} & M \oplus T & \underset{i_2}{\overset{p_2}{\rightleftarrows}} & T & \longrightarrow & 0 \end{array}$$

donde $i_1(m) = (m,0)$, $p_1(m,t) = m$, $i_2(t) = (0,t)$ y $p_2(m,t) = t$. Definimos entonces el morfismo $h\colon T \to N$, $t \mapsto \varphi(i_2(t))$. Tenemos

$$g(h(t)) = g(\varphi(0,t)) = p_2(0,t) = t.$$

Para ver que (3) $\Longrightarrow$ (1) consideramos el mismo diagrama que en la implicación anterior y definimos el morfismo $h\colon N \to M$, $n \mapsto p_1(\varphi(n))$. Entonces

$$h(f(m)) = p_1(\varphi(f(m))) = p_1(i_1(m)) = p_1(m,0) = m. \qquad \square$$

Diremos que la sucesión exacta

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es **escindida** (o que se parte) si cumple alguna de las condiciones de la proposición anterior.

Ejercicio 26.10. Sean

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0$$

una sucesión exacta de módulos y $r \in R$. Pruebe que son equivalentes:

1) Para todo $x \in X$ tal que existe $m \in M$ con $f(x) = r \cdot m$, existe $x_1 \in X$ con $x_1 = r \cdot x$.
2) Para todo $y \in Y$ tal que $r \cdot y = 0$ existe $m \in M$ tal que $r \cdot m = 0$ e $y = g(m)$.

Ejercicio 26.11. Sea

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0$$

Demuestre que g es una retracción si y sólo si existen morfismos $s\colon Y \to M$ y $r\colon M \to X$ tales que $f \circ r + s \circ g = \mathrm{id}_M$.

Describiremos ahora el funtor $\mathrm{Hom}_R(M,-)$.

Informalmente, un funtor $\mathrm{Hom}_R(M,-)$ es una regla que para cada módulo N nos devolverá el grupo abeliano $\mathrm{Hom}_R(M,N)$ y para cada morfismo $f \in \mathrm{Hom}_R(A,B)$ nos devoverá el morfismo $f_*\colon \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B)$, $f_*(\alpha) = f \circ \alpha$, de grupos abelianos.

Proposición 26.12. *Si la sucesión*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

es exacta, entonces

$$0 \longrightarrow \mathrm{Hom}_R(M,A) \xrightarrow{f_*} \mathrm{Hom}_R(M,B) \xrightarrow{g_*} \mathrm{Hom}_R(M,C)$$

es exacta.

Demostración. Primero veamos que f_* es monomorfismo. Si $f \circ \alpha = 0$, entonces $\alpha = 0$ pues f es monomorfismo.

Veamos ahora que $\mathrm{im}(f_*) \subseteq \ker g_*$. Si $\beta = f_*\alpha = f \circ \alpha$, entonces

$$g \circ \beta = (g \circ f) \circ \alpha = 0,$$

pues $\mathrm{im}\, f \subseteq \ker g$, es decir $\beta \ker g_*$.

Veamos que vale también la inclusión $\mathrm{im}(f_*) \supseteq \ker g_*$. Si $g_*\beta = g \circ \beta = 0$, entonces $\beta(m) \in \ker g = \mathrm{im}\, f$ para todo $m \in M$. Si $m \in M$, existe un único $a \in A$ tal que $\beta(m) = f(a)$. Si $\alpha\colon M \to A$, $m \mapsto a$, entonces $\alpha \in \mathrm{Hom}_R(M,A)$ es tal que $\beta = f \circ \alpha$. □

Ejemplo 26.13. Obervemos que g_* podría no ser un epimorfismo. Si $g\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es el morfismo canónico de $\mathbb{Z}$-módulos, entonces $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = \{0\}$ aunque $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z}) \neq \{0\}$.

Diremos que el funtor $\mathrm{Hom}_R(M,-)$ es **exacto** si para toda sucesión

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

exacta se tiene que la sucesión

$$0 \longrightarrow \hom_R(M,A) \xrightarrow{f_*} \hom_R(M,B) \xrightarrow{g_*} \hom_R(M,C) \longrightarrow 0$$

de grupos abelianos y morfismos es también exacta.

Proposición 26.14. *Si la sucesión exacta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

se parte, entonces

$$0 \longrightarrow \mathrm{Hom}_R(M,A) \xrightarrow{f_*} \mathrm{Hom}_R(M,B) \xrightarrow{g_*} \mathrm{Hom}_R(M,C) \longrightarrow 0$$

también se parte.

Demostración. Debemos demostrar que g_* es sobreyectiva. Por hipótesis sabemos que existe $h \in \mathrm{Hom}_R(C,B)$ tal que $g \circ h = \mathrm{id}_C$. Si $f \in \mathrm{Hom}_R(M,C)$, entonces

$$(g_* \circ h_*)(f) = g_*(h_*(f)) = g_*(h \circ f) = g \circ (h \circ f) = (g \circ h) \circ f = \mathrm{id}_B \circ f = f.$$

Como $g_* \circ h_* = \mathrm{id}$, se concluye que g_* es sobreyectiva y que la sucesión exacta además se parte. □

De la misma forma se define el funtor $\mathrm{Hom}_R(-,M)$. Para cada módulo N el funtor nos devolverá el módulo $\mathrm{Hom}_R(N,M)$ y para cada morfismo $f \in \mathrm{Hom}_R(A,B)$ nos devoverá un morfismo $f^*\colon \mathrm{Hom}_R(B,M) \to \mathrm{Hom}_R(A,M)$, $f^*(\alpha) = \alpha \circ f$. Tal como demostramos la proposición anterior puede verse que si la sucesión exacta

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

se parte, entonces

$$0 \longrightarrow \hom_R(C,M) \xrightarrow{g^*} \hom_R(B,M) \xrightarrow{f^*} \hom_R(A,M) \longrightarrow 0$$

también se parte.

Ejemplo 26.15. Si usamos el resultado anterior con la sucesión exacta

$$0 \longrightarrow B \xrightarrow{i_B} A \oplus B \xrightarrow{p_A} A \longrightarrow 0$$

donde $i_B(b) = (0,b)$ y $p_A(a,b) = a$, podemos demostrar que

$$\mathrm{Hom}_R(A\oplus B,M)\simeq \mathrm{Hom}_R(A,M)\times \mathrm{Hom}_R(B,M). \tag{26.6}$$

Puede verificarse que el isomorfismo está dado por $f\mapsto (f\circ i_A, f\circ i_B)$, donde $i_A\colon A\to A\oplus B$, $i_A(a)=(a,0)$ y $i_B\colon B\to A\oplus B$, $i_B(b)=(0,b)$.

Ejemplo 26.16. Tal como se hizo en el ejemplo anterior, puede demostrarse que

$$\mathrm{Hom}_R(M,A\times B)\simeq \mathrm{Hom}_R(M,A)\times \mathrm{Hom}_R(M,B). \tag{26.7}$$

En este caso el isomorfismo es $f\mapsto (p_A\circ f, p_B\circ f)$, donde $p_A\colon A\oplus B\to A$, $p_A(a,b)=a$ y $p_B\colon A\oplus B\to B$, $p_B(a,b)=b$.

Para entender mejor por qué usamos sumas y productos en las fórmulas (26.6) y (26.7) mencionamos que pueden demostrarse las fórmulas

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, M\right)\simeq \prod_{i\in I}\mathrm{Hom}_R(M_i,M),$$
$$\mathrm{Hom}_R\left(M, \prod_{i\in I} M_i\right)\simeq \prod_{i\in I}\mathrm{Hom}_R(M,M_i).$$

Capítulo 27
Módulos finitamente generados

Definición 27.1. Sea M un módulo y X un subconjunto de M. El submódulo (X) de M generado por X se define como la intersección de todos los submódulos de M que contienen al conjunto X.

El submódulo de M generado por el conjunto X es el menor submódulo de M que contiene a X. Puede demostrarse además que

$$(X) = \left\{ \sum_{i=1}^{n} r_i \cdot x_i : n \in \mathbb{N}_0,\, r_i \in R,\, x_i \in X \right\}$$

Definición 27.2. Diremos que un submódulo S de M es **finitamente generado** si $S = (X)$ para algún conjunto finito X.

Ejemplos 27.3.

1) $\{1\}$ y $\{2,3\}$ son conjuntos de generadores de $\mathbb{Z}$.
2) $\{2\}$ no es un conjunto de generadores de $\mathbb{Z}$.

Ejemplo 27.4. Sea $R = \{f\colon [0,1] \to \mathbb{R}\}$ el anillo de funciones $[0,1] \to \mathbb{R}$ con las operaciones

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x), \quad x \in [0,1].$$

Sea $M = {}_R R$, es decir el anillo R con la estructura de módulo dada por la representación regular a izquierda. Como el conjunto

$$S = \{f \in R : f(x) \neq 0 \text{ para finitos } x\}$$

es un ideal a izquierda de R, es un submódulo de M. Como módulo, M está generado por la función constantemente igual a uno. Sin embargo, S no es finitamente generado. En efecto, si $S = (f_1, \ldots, f_k)$, sea

$$X = \{x \in [0,1] : f_i(x) \neq 0 \text{ para algún } i\}.$$

Como X es finito, podemos suponer que $X = \{x_1, \ldots, x_l\}$. Sea $x_0 \in [0,1] \setminus X$ y sea $\varphi\colon [0,1] \to \mathbb{R}$ tal que $\varphi(x_0) = 1$ y $\varphi(x) = 0$ para todo $x \neq x_0$. Entonces $\varphi \in S$ pero $\varphi \notin (f_1, \ldots, f_k)$, pues

$$\left(\sum_{i=1}^{k} r_i \cdot f_i\right)(x_0) = \sum_{i=1}^{k} r_i(x_0) f_i(x_0) = 0 \neq 1 = \varphi(x_0).$$

Ejemplo 27.5. Sea K un cuerpo y sea V un espacio vectorial. Si $T\colon V \to V$ es una transformación lineal, entonces V es un $K[X]$-módulo con

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Veamos que V es de dimensión finita, entonces V es finitamente generado como $K[X]$-módulo. En efecto, si $\{v_1, \ldots, v_n\}$ es una base del espacio vectorial V, entonces $V = (v_1, \ldots, v_n)$ como $K[X]$-módulo, pues para cada $v \in V$ existen constantes $\lambda_1, \ldots, \lambda_k \in K \subseteq K[X]$ tales que $v = \sum_{i=1}^{n} \lambda_i v_i$.

Ejemplo 27.6. Sea $G = \{g_1, \ldots, g_k\}$ un grupo finito de orden k y supongamos que $g_1 = 1$. Si M es un $\mathbb{C}[G]$-módulo finitamente generado, entonces, en particular, M es un espacio vectorial de dimensión finita. En efecto, M es un espacio vectorial con la acción

$$\lambda m = (\lambda g_1) \cdot m = (\lambda 1) \cdot m$$

para todo $\lambda \in \mathbb{C}$ y $m \in M$. Supongamos ahora que $M = (m_1, \ldots, m_l)$. Para cada $m \in M$ existen $\alpha_1, \ldots, \alpha_l \in \mathbb{C}[G]$ tales que

$$m = \alpha_1 \cdot m_1 + \cdots + \alpha_l \cdot m_l.$$

Además para cada $j \in \{1, \ldots, l\}$ existen $\lambda_{ij} \in \mathbb{C}$ tales que $\alpha_j = \sum_{i=1}^{k} \lambda_{ij} g_i$. En consecuencia, cada $m \in M$ puede escribirse como

$$m = \sum_{i=1}^{k} \sum_{j=1}^{l} \lambda_{ij} (g_j \cdot m_i)$$

para ciertos $\lambda_{ij} \in \mathbb{C}$, donde $i \in \{1, \ldots, k\}$ y $j \in \{1, \ldots, l\}$. En particular, M es de dimensión finita, pues $\dim M \leq kl$.

Proposición 27.7. *Si*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es exacta, valen las siguientes afirmaciones.

1) Si N es finitamente generado, entonces T es finitamente generado.
2) Si M y T son finitamente generados, entonces N es finitamente generado.

Demostración. Comenzaremos con la demostración de la primera afirmación. Veremos que si $N = (n_1, \dots, n_k)$, entonces $T = (g(n_1), \dots, g(n_k))$. En efecto, si $t \in T$, existe $n \in N$ tal que $g(n) = t$. Si escribimos $n = \sum_{i=1}^{k} r_i \cdot n_i$, entonces

$$t = g(n) = \sum_{i=1}^{k} r_i \cdot g(n_i).$$

Demostremos ahora la segunda afirmación. Supongamos que $M = (m_1, \dots, m_k)$ y que $T = (t_1, \dots, t_l)$. Como g es sobreyectiva, para cada $i \in \{1, \dots, l\}$ existe $n_i \in N$ tal que $g(n_i) = t_i$. Vamos a demostrar que $N = (f(m_1), \dots, f(m_k), n_1, \dots, n_l)$. Sea $n \in N$. Como $g(n) \in T$, existen $r_1, \dots, r_l \in R$ tales que

$$g(n) = \sum_{i=1}^{l} r_i \cdot t_i = g\left(\sum_{i=1}^{l} r_i \cdot n_i \right),$$

lo que implica que $n - \sum_{i=1}^{l} r_i \cdot n_i \in \ker g = f(M)$. En particular, existen $s_1, \dots, s_k \in R$ tales que

$$n - \sum_{i=1}^{l} r_i \cdot n_i = \sum_{j=1}^{k} s_j \cdot f(m_j),$$

pues $f(M) = (f(m_1), \dots, f(m_k))$. □

Proposición 27.8. *Sea M un módulo. Entonces M es finitamente generado si y sólo M es isomorfo a un cociente de R^k para algún $k \in \mathbb{N}$.*

Demostración. Si $M = (m_1, \dots, m_k)$, entonces $\varphi \colon R^k \to M$, $(r_1, \dots, r_k) \mapsto \sum r_i m_i$, es un epimorfismo y luego $R^k / \ker \varphi \simeq M$. Recíprocamente, si $\varphi \colon R^k \to M$ es un epimorfismo, como R^k está generado por $\{e_i : 1 \leq i \leq k\}$, donde

$$(e_i)_j = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

el conjunto $\{\varphi(e_i) : 1 \leq i \leq k\}$ genera $\varphi(R^k) = M$. □

Tal como vimos en la teoría de anillos, tener objetos finitamente generados está relacionado con el concepto de noetherianidad.

Definición 27.9. Un módulo se dice **noetheriano** si toda sucesión $M_1 \subseteq M_2 \subseteq \cdots$ de submódulos de M se estabiliza, es decir que existe n tal que $M_k = M_{n+k}$ para todo $k \in \mathbb{N}$.

Proposición 27.10. *Sea M un módulo. Las siguientes afirmaciones son e quivalentes:*

1) M es noetheriano.
2) Todo submódulo de M es finitamente generado.

3) Toda familia no vacía de submódulos de M tiene un elemento maximal (con respecto a la inclusión).

Demostración. Demostremos que $(2) \implies (1)$. Si $S_1 \subseteq S_2 \subseteq \cdots$ es una sucesión de submódulos de M, puede demostrarse que $S = \cup_{i\geq 1} S_i$ es un submódulo de M. Como S es finitamente generado, digamos $S = (x_1, \ldots, x_n)$ para finitos elementos $x_1, \ldots, x_n \in M$, entonces $x_1, \ldots, x_n \in S_N$ para algún $N \in \mathbb{N}$. Luego $S \subseteq S_N$ y entonces $S_N = S_{N+k}$ para todo $k \in \mathbb{N}$.

Demostremos ahora que $(1) \implies (3)$. Si F es una familia no vacía de submódulos de M que no tiene elementos maximales, sea $S_1 \in F$. Como S_1 no es maximal, existe entonces $S_2 \in F$ tal que $S_1 \subsetneq S_2$. Si tenemos $S_1 \subsetneq \cdots \subsetneq S_k$, entonces la no maximalidad de S_k nos dice que existe $S_{k+1} \in F$ tal que $S_k \subsetneq S_{k+1}$, de forma que la sucesión de los S_j no se estabiliza.

Por último, demostramos que $(3) \implies (2)$. Sea S un submódulo de M y sea

$$F = \{T \subseteq S : T \subseteq M \text{ submódulo finitamente generado}\}.$$

Por hipótesis, F tiene un elemento maximal, digamos N. Entonces N es un submódulo de M tal que $N \subseteq S$ y N es finitamente generado, digamos $N = (n_1, \ldots, n_k)$. Si $N = S$, en particular S es finitamente genreado. Si $N \neq S$, sea $x \in S \setminus N$. Entonces $N \subseteq (n_1, \ldots, n_k, x) \subseteq S$, lo que implica, por la maximalidad de N, que $N = (n_1, \ldots, n_k, x)$, una contradicción pues $x \notin N$. □

Ejercicio 27.11. Si

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es exacta, valen las siguientes afirmaciones:

1) Si N es noetheriano, entonces M y T son noetherianos.
2) Si M y T son noetherianos, entonces N es noetheriano.

Ejercicio 27.12. Un anillo R es noetheriano si y sólo si el módulo ${}_RR$ es noetheriano.

Ejercicio 27.13. Si $M_1, \ldots, M_n$ son noetherianos, entonces $M_1 \oplus \cdots \oplus M_n$ es noetheriano.

Es interesante mencionar que el resultado del ejercicio anterior no vale para sumas infinitas de módulos. Puede demostrarse por ejemplo que $\mathbb{Z}^{\mathbb{N}}$ no es noetheriano, pues no es finitamente generado.

Proposición 27.14. *Si R es noetheriano y M es un módulo finitamente generado, entonces M es noetheriano.*

Demostración. Como M es finitamente generado, digamos $M = (m_1, \ldots, m_k)$, existe un epimorfismo $R^k \to N$, $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^k r_i \cdot m_i$, donde $R^k = \oplus_{i=1}^k R$. Como R es noetheriano, R^k es noetheriano y luego M es también noetheriano. □

Capítulo 28
Módulos libres

Definición 28.1. Sea X un subconjunto de un módulo M. Diremos que X es **linealmente independiente** si para cada $k \in \mathbb{N}$, $r_1, \ldots, r_k \in R$ y $m_1, \ldots, m_k \in X$ tales que $r_1 \cdot m_1 + \cdots + r_k \cdot m_k = 0$ se tiene que $r_1 = \cdots = r_k = 0$. Un conjunto que no es linealmente independiente se dirá **linealmente dependiente**.

La independencia lineal en módulos es levemente distinta a la que conocemos para espacios vectoriales. En módulos la dependencia lineal no garantiza que uno de los elementos del conjunto pueda escribirse como combinación lineal de los otros, ya que en el anillo R no siempre podremos dividir.

Ejemplo 28.2. Consideramos $\mathbb{Z}$ como $\mathbb{Z}$-módulo. El conjunto $\{2,3\} \subseteq \mathbb{Z}$ es linealmente dependiente pues $(-3) \cdot 2 + 2 \cdot 3 = 0$. Observemos que 2 no es un múltiplo entero de 3, tampoco 3 es un múltiplo entero de 2.

Ejemplo 28.3. El conjunto $\{1\}$ del módulo ${}_R R$ es linealmente independiente. Si r es un divisor de cero de R, entonces $\{r\}$ es linealmente dependiente.

En módulos, un conjunto minimal de generadores puede ser linealmente dependiente.

Ejemplo 28.4. Sea $R = M_2(\mathbb{R})$ y sea $M = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$. Dejamos como ejercicio demostrar que M es un módulo sobre el anillo R con la multiplicación usual de matrices. El conjunto $\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$ es un conjunto minimal de generadores y es linealmente dependiente.

Ejemplo 28.5. Sea $M = \mathbb{Q}$ como $\mathbb{Z}$-módulo. Si $x \in \mathbb{Q} \setminus \{0\}$, entonces $\{x\}$ es linealmente independiente. Si $x, y \in \mathbb{Q}$ son tales que $x \neq y$, entonces $\{x, y\}$ es linealmente dependiente.

Si V es un espacio vectorial y $v \in V \setminus \{0\}$, entonces $\{v\}$ es linealmente independiente, pues si $\lambda \neq 0$ y $v \neq 0$, entonces $\lambda v \neq 0$. En la teoría de módulos, las cosas pueden ser distintas.

Ejemplo 28.6. Todo subconjunto del $\mathbb{Z}$-módulo $\mathbb{Z}/n$ es linealmente dependiente.

Ejercicio 28.7. Sea $f \in \mathrm{Hom}_R(M,N)$ y sea X un subconjunto de M.

1) Si X es linealmente dependiente, entonces $f(X)$ también.
2) Si X es linealmente independiente y f es monomorfismo, entonces $f(X)$ es linealmente independiente.
3) Si $M = (X)$ y f es epimorfismo, entonces $N = (f(X))$.

Definición 28.8. Sea M un módulo. Un subconjunto B de M es una **base** de M si es linealmente independiente y además $(B) = M$. Un módulo M se dice **libre** si admite una base.

Ejemplos 28.9.

1) Todo espacio vectorial es un módulo libre.
2) ${}_RR$ es libre con base $\{1\}$.
3) El $\mathbb{Z}$-módulo $\mathbb{Q}$ no es libre.
4) R^n es libre como R-módulo.

Ejemplo 28.10. Las únicas bases de $\mathbb{Z}$ como $\mathbb{Z}$-módulo son $\{1\}$ y $\{-1\}$.

El ejemplo siguiente es bien conocido en el caso de espacios vectoriales. Los módulos sobre anillos de división son muy similares a los espacios vectoriales y por esa razón se los llama **espacios vectoriales sobre anillos de división**.

Ejemplo 28.11. Sea R un anillo de división y sea M un R-módulo no nulo finitamente generado. Vamos a demostrar las siguientes propiedades:

1) Todo conjunto finito de generadores contiene una base. En particular, M es libre.
2) Todo conjunto linealmente independiente puede extenderse a una base.
3) Dos bases cualesquiera tienen la misma cantidad de elementos.

Para demostrar la primera afirmación procederemos por inducción en la cantidad de generadores de M. Si $M = (m)$, entonces $\{m\}$ es base pues $\{m\}$ es linealmente independiente: si $r \cdot m = 0$ y $r \neq 0$, entonces

$$m = 1 \cdot m = (r^{-1}r) \cdot m = r^{-1} \cdot (r \cdot m) = 0.$$

Si vale para $k-1$ generadores, sea $M = (m_1, \ldots, m_k)$. Si $\{m_1, \ldots, m_k\}$ no es linealmente independiente, entonces existen $r_1, \ldots, r_k \in R$ no todos cero tales que

$$r_1 \cdot m_1 + \cdots + r_k \cdot m_k = 0.$$

Sin perder generalidad podemos suponer que $r_k \neq 0$. Entonces

$$v_k = \sum_{i=1}^{k-1} (r_k^{-1} r_i) \cdot m_i \in (m_1, \ldots, m_{k-1}).$$

Como entonces $M = (m_1, \ldots, m_k) = (m_1, \ldots, m_{k-1})$, la hipótesis inductiva implica que M es libre.

Vamos a demostrar ahora que todo conjunto X linealmente independiente puede extenderse a una base. Sea $X = \{x_1, \ldots, x_k\}$ tal que $M = (X)$. Como $M \neq \{0\}$, sin perder generalidad podemos suponer que $x_1 \neq 0$. Como R es de división, el conjunto $\{x_1\}$ es linealmente independiente, pues si $r \neq 0$ y $r \cdot x_1 = 0$, entonces

$$x_1 = 1 \cdot r = (r^{-1}r) \cdot x_1 = r^{-1} \cdot (r \cdot x) = r^{-1} \cdot 0 = 0.$$

Sea $Y = \{y_1, \ldots, y_l\}$ un subconjunto de X maximal tal que Y es linealmente independiente. Veamos que $X \subseteq (Y)$. Sea $x \in X$. Si $x \notin Y$, entonces, como $Y \subseteq Y \cup \{x\}$, la maximalidad de Y implica que $\{x\} \cup Y$ es linealmente dependiente, es decir que existen $r, r_1, \ldots, r_k \in R$ no todos cero tales que

$$r \cdot x + \sum_{i=1}^{l} r_i \cdot y_i = 0.$$

Si $r = 0$, entonces $r_1 = \cdots = r_l = 0$ porque los y_j son linealmente independientes, una contradicción. Luego $r \neq 0$ y entonces

$$x = -\sum_{i=1}^{l} (-r^{-1}r_i) \cdot y_i \in (Y).$$

Luego $X \subseteq (Y)$. En conclusión Y es una base de M pues $M = (Y)$ y además Y es linealmente independiente.

Demostremos que dos bases finitas cualesquiera tienen la misma cantidad de elementos. Para eso es suficiente demostrar que si X e Y son conjuntos finitos linealmente independientes tales que $(X) \subseteq (Y)$, entonces $|X| \leq |Y|$. Supongamos que $|X| = k$ e $|Y| = l$. Procederemos por inducción en l. Si $l = 1$ y $k > 1$, entonces exiten $r_1, r_2 \in R$ tales que $x_1 = r_1 \cdot y_1$ y $x_2 = r_2 \cdot y_1$. Luego

$$x_2 = r_2 \cdot y_1 = r_2 \cdot (r_1^{-1} \cdot x_1) = (r_2 r_1^{-1}) \cdot x_1,$$

una contradicción pues $\{x_1, x_2\}$ es linealmente independiente. Supongamos ahora que el resultado es verdadero para $l - 1$ y sea $l = |Y|$. Para cada j escribimos

$$x_j = \sum_{i=1}^{l} r_{ji} \cdot y_i,$$

donde $r_{ji} \in R$. Si $r_{j1} \neq 0$ para todo j, entonces $x_j = \sum_{i=2}^{l} r_{ji} \cdot y_i$ para todo j y luego $(X) \subseteq (y_2, \ldots, y_l)$, que implica que $|X| \leq l - 1 < l = |Y|$. Si existe j tal que $r_{j1} \neq 0$, sin perder generalidad podemos suponer que $r_{11} \neq 0$. Para cada $j \in \{2, \ldots, k\}$ sea

$$z_j = x_j - (r_{j1} r_{11}^{-1}) \cdot x_1.$$

Como $z_j \in (y_2, \dots, y_l)$ para todo j y los z_j son linealmente independientes, la hipótesis inductiva impica que $k-1 \leq l-1$, es decir $|X| \leq |Y|$.

El ejemplo anterior nos permite hablar de la **dimensión** de un módulo sobre un anillo de división.

Ejemplo 28.12. El anillo $\mathbb{R}[X]$ es un $\mathbb{R}$-módulo libre con base $\{1, X, X^2, \dots\}$. También es un $\mathbb{R}[X]$-módulo libre con base $\{1\}$.

Ejercicio 28.13. Demuestre que el conjunto $\{(a,b),(c,d)\}$ es base del $\mathbb{Z}$-módulo $\mathbb{Z} \times \mathbb{Z}$ si y sólo si $ad - bc \in \{-1, 1\}$.

En particular, $\{(1,0),(0,1)\}$ es una base de $\mathbb{Z} \times \mathbb{Z}$ como $\mathbb{Z}$-módulo.

Ejemplo 28.14. Si $u \in \mathscr{U}(R)$, entonces $\{u\}$ es una base de ${}_R R$. Recíprocamente, si R es un dominio íntegro y $\{z\}$ es una base de ${}_R R$, entonces $z \in \mathscr{U}(R)$, pues, como $1 = yz$ para algún $y \in R$, también se tiene que $zy = 1$ pues

$$(zy-1)z = z(yz) - z = z1 - z = z - z = 0.$$

Ejemplo 28.15. Sea I un conjunto no vacío. El R-módulo $R^{(I)}$ es libre con base $\{e_i : i \in I\}$, donde

$$(e_i)_j = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Ejemplo 28.16. Si $R = M_2(\mathbb{Z})$, entonces $M = {}_R R$ es libre con base $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. El submódulo $N = \begin{pmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & 0 \end{pmatrix}$ no admite una base como R-módulo.

A diferencia de lo que pasa con espacios vectoriales, el tamaño de una base no es un invariante.

Ejemplo 28.17. Sea V el espacio vectorial (complejo) con base infinita $e_0, e_1, e_2, \dots$ y sea $R = \operatorname{End}(V)$ con la estructura de anillo dada por

$$(f+g)(v) = f(v) + g(v), \quad (fg)(v) = f(g(v))$$

para $f, g \in R$ y $v \in V$.

Sea $M = {}_R R$. Sabemos que $\{\mathrm{id}\}$ es una base para R. Mostraremos que M admite también una base que tiene dos elementos. Si $r, s \in R$ son tales que

$$\begin{aligned} r(e_{2n}) &= e_n, & r(e_{2n+1}) &= 0, \\ s(e_{2n}) &= 0, & s(e_{2n+1}) &= e_{2n}, \end{aligned}$$

entonces $\{r, s\}$ es base de M.

Si $f \in R$, entonces $f = \alpha r + \beta s$, donde $\alpha \colon V \to V$, $e_n \mapsto f(e_{2n})$ para todo $n \in \mathbb{N}$, y $\beta \in V \to V$, $e_n \mapsto f(e_{2n+1})$ para todo $n \in \mathbb{N}$. En efecto,

$$(\alpha r+\beta s)(e_{2n}) = \alpha(r(e_{2n}))+\beta(s(e_{2n})) = f(e_{2n}),$$
$$(\alpha r+\beta s)(e_{2n+1}) = \alpha(r(e_{2n+1}))+\beta(s(e_{2n+1})) = f(e_{2n+1}).$$

Además $\{r,s\}$ es linealmente independiente, pues si $\alpha r+\beta s = 0$ para $\alpha,\beta \in R$, entonces al evaluar en los e_{2n} se obtiene que $\alpha = 0$ y al evaluar en los e_{2n+1} se obtiene que $\beta = 0$.

Ejemplo 28.18. Si M es un módulo libre con base X y N es un módulo libre con base Y, entonces $M \oplus N$ es un módulo libre con base

$$\{(x,0) : x \in X\} \cup \{(0,y) : y \in Y\}.$$

Ejercicio 28.19. Sea R es un anillo conmutativo. Si M y N son libres y finitamente generados, entonces $\mathrm{Hom}_R(M,N)$ es libre y finitamente generado.

Veamos algunos resultados básicos que nos permiten entender qué significa tener un módulo libre.

Proposición 28.20. *Si M es libre, entonces existe un subconjunto $\{m_i : i \in I\}$ de M tal que para cada $m \in M$ existen únicos $r_i \in R$, $i \in I$, donde $r_i = 0$ salvo finitos $i \in I$ tales que $m = \sum r_i \cdot m_i$.*

Demostración. Como M es libre, existe una base $\{m_i : i \in I\}$ de M. Si $m \in M$, entonces podemos escribir $m = \sum r_i \cdot m_i$ (suma finita) para ciertos $r_i \in I$. Veamos que los r_i son únicos. Si $m = \sum s_i \cdot m_i$, entonces $\sum (r_i - s_i) \cdot m_i = 0$. La independencia lineal del conjunto $\{m_i : i \in I\}$ implica entonces que $r_i = s_i$ para todo $i \in I$. □

Proposición 28.21. *Sea M libre con base $\{m_i : i \in I\}$ y sea N un submódulo de M. Si $\{n_i : i \in I\} \subseteq N$ es un subcobjunto, existe un único $f \in \mathrm{Hom}_R(M,N)$ tal que $f(m_i) = n_i$ para todo $i \in I$.*

Bosquejo de la demostración. Basta con observar que el único morfismo $f : M \to N$ debe definirse como $f(\sum r_i \cdot m_i) = \sum r_i \cdot n_i$. □

Una aplicación sencilla de la proposición anterior:

Ejemplo 28.22. Veamos que no existe un epimorfismo $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ (de $\mathbb{Z}$-módulos). En efecto, si $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ es un epimorfismo, sea $\{u,v\}$ una base de $\mathbb{Z} \times \mathbb{Z}$. Entonces $f(k) = u$ y $f(l) = v$ para ciertos $k,l \in \mathbb{Z}$. La proposición 28.21 implica que existe un morfismo $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $g(u) = k$ y $g(v) = l$. En particular, $f \circ g = \mathrm{id}_{\mathbb{Z}\times\mathbb{Z}}$ y luego g es un monomorfismo. Como

$$g(lu - kv) = lg(u) - kg(v) = lk - kl = 0,$$

se tiene entonces que $lu - kv = 0$ y luego $k = l = 0$, pues $\{u,v\}$ es linealmente independiente, una contradicción.

Otra propiedad importante de los módulos libres:

Proposición 28.23. *Si M es libre, entonces $M \simeq R^{(I)}$ para algún conjunto I.*

Demostración. Supongamos que M es libre con base $\{m_i : i \in I\}$. Vimos una proposición que nos dice que existe un único morfismo $f \in \mathrm{Hom}_R(M, R^{(I)})$ tal que $f(m_i) = e_i$ para todo $i \in I$, donde

$$(e_i)_j = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Veamos que f es un isomorfismo. Primero veamos que f es epimorfismo: dado $(r_i)_{i\in I} \in R^{(I)}$, entonces $f(\sum r_i \cdot m_i) = (r_i)_{i\in I}$. Para ver que es monomorfismo:

$$0 = f(\sum r_i \cdot m_i) = \sum r_i \cdot f(m_i) = \sum r_i \cdot e_i \implies r_i = 0 \text{ para todo } i \in I. \qquad \square$$

Corolario 28.24. *Todo módulo es (isomorfo a un) cociente de un módulo libre.*

Demostración. Si M es un módulo, vamos a demostrar que existe un módulo libre L y un epimorfismo $f \in \mathrm{Hom}_R(L, M)$, ya que entonces $L/\ker f \simeq M$ por el primer teorema de isomorfismos. Sea $\{m_i : i \in I\}$ un conjunto de generadores de M, que siempre existe, ya que podríamos tomar por ejemplo el conjunto $\{m : m \in M\}$ y sea $L = R^{(I)}$. Entonces L es libre y $f\colon R^{(I)} \to M$, $e_i \mapsto m_i$, es un epimorfismo. $\square$

Otra propiedad importante de los módulos libres:

Proposición 28.25. *Si M es un módulo libre, $f \in \mathrm{Hom}_R(N, T)$ es un epimorfismo y $h \in \mathrm{Hom}_R(M, T)$, entonces existe $\varphi \in \mathrm{Hom}_R(M, N)$ tal que $f \circ \varphi = h$.*

Demostración. Si $\{m_i : i \in I\}$ es base de M, como f es un epimorfismo, para cada $i \in I$ existe $n_i \in N$ tal que $f(n_i) = h(m_i)$. Como M es libre, existe un único morfismo $\varphi\colon M \to N$ tal que $\varphi(m_i) = n_i$ para todo $i \in I$. Este morfismo cumple $f \circ \varphi = h$. $\square$

Sea R un dominio íntegro y sea $S = R \setminus \{0\}$.

En el conjunto $R \times S$ definimos la siguiente relación:

$$(r, s) \sim (r_1, s_1) \iff r s_1 - r_1 s = 0.$$

Dejamos como ejercicio verificar que $\sim$ es una relación de equivalencia.

La clase de equivalencia del par (r, s) será denotada por r/s o bien $\frac{r}{s}$.

Puede demostrarse que el conjunto $K(R) = (R \times S)/\sim$ de clases de equivalencia es un cuerpo con las operaciones

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{r s_1 + r_1 s}{s s_1}, \quad \frac{r}{s}\frac{r_1}{s_1} = \frac{r r_1}{s s_1}. \tag{28.1}$$

$K(R)$ se llama el **cuerpo de fracciones** de R. Por ejemplo, $K(\mathbb{Z}) = \mathbb{Q}$.

Para demostrar que $K(R)$ es un cuerpo primero debemos ver que las operaciones 28.1 están bien definidas. Por ejemplo, si $r/s \sim r'/s'$ y $r_1/s_1 \sim r_1'/s_1'$, entonces $r/s + r_1/s_1 \sim r'/s' + r_1'/s_1'$. En efecto, como $r/s \sim r'/s'$, entonces $rs' - r's = 0$. Similarmente, $r_1 s_1' - r_1' s_1 = 0$, pues $r_1/s_1 \sim r_1'/s_1'$. Luego

$$\frac{rs_1 + r_1 s}{ss_1} = \frac{r's'_1 + r'_1 s'}{s's'_1}$$

pues

$$(rs_1 + r_1 s)s's'_1 = rs_1 s's'_1 + r_1 ss's'_1 = r'ss_1 s'_1 + r'_1 s_1 ss' = (r's'_1 + r'_1 s)ss_1.$$

De la misma forma se demuestra que el producto también está bien definido. Dejamos como ejercicio verificar que con estas operaciones $K(R)$ es un cuerpo.

Teorema 28.26. *Sea R un dominio íntegro. Si M es un módulo libre con base finita, entonces dos bases cualesquiera de M tienen la misma cantidad de elementos.*

Demostración. Sea $K = K(R)$ el cuerpo de fracciones de R. Es sencillo verificar que el grupo abeliano $V = \mathrm{Hom}_R(M, K)$ es un K-espacio vectorial con la acción

$$(\lambda f)(m) = \lambda f(m),$$

donde $\lambda \in K$, $f \in V$ y $m \in M$.

El espacio vectorial V tiene bien definida su dimensión. Calculemos entonces $\dim V$. Para eso, sea $\{e_1, \ldots, e_n\}$ una base de M. Para cada $i \in \{1, \ldots, n\}$ sea

$$f_i \colon M \to K, \quad e_j \mapsto \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Veamos que $\{f_1, \ldots, f_n\}$ es base de V. Es un conjunto de generadores de V pues si $f \in V$, entonces

$$f = \sum_{i=1}^{n} f(e_i) f_i,$$

pues estos morfismos coinciden en los elementos de una base de M, es decir $f(e_j) = (\sum_{i=1}^{n} f(e_i) f_i)(e_j)$ para todo $j \in \{1, \ldots, n\}$. Además $\{f_1, \ldots, f_n\}$ es linealmente independiente, pues si $0 = \sum_{i=1}^{n} \lambda_i f_i$, entonces, al evaluar en cada e_j, se tiene que

$$0 = \left(\sum_{i=1}^{n} \lambda_i f_i \right)(e_j) = \lambda_j$$

para todo $j \in \{1, \ldots, n\}$. Luego $n = \dim V$. □

Definición 28.27. Sea R un dominio íntegro. Si M es un módulo finitamente generado, se define el **rango** de M como el cardinal de una base de M. Si M no es finitamente generado diremos que el rango de M es infinito. El rango del módulo M será denotado por $\mathrm{rank}(M)$.

El teorema anterior puede extenderse para módulos sobre anillos conmutativos. En consecuencia, la noción de rango de un módulo queda bien definida para módulos sobre anillos conmutativos. En efecto, sea F un módulo libre con base en un conjunto X. Como R es conmutativo, sabemos que R admite un ideal maximal I.

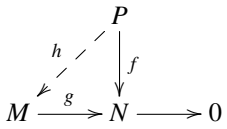
Como I es maximal, el cociente $K = R/I$ es entonces un cuerpo. Puede verificarse que el subconjunto

$$I \cdot F = \left\{ \sum_{i=1}^{n} r_i \cdot x_i : n \in \mathbb{N}, r_1, \ldots, r_n \in I \right\}$$

es un submódulo de F. El módulo cociente $V = F/(I \cdot F)$ es un K-espacio vectorial con base $\{x + I \cdot F : x \in X\}$. Luego $|X| = \dim V$.

Capítulo 29
Módulos proyectivos

Definición 29.1. Un módulo P se dice **proyectivo** si dados $f \in \mathrm{Hom}_R(P,N)$ y un epimorfismo $g \in \mathrm{Hom}_R(M,N)$ existe $h \in \mathrm{Hom}_R(P,M)$ tal que $g \circ h = f$, es decir que existe un morfismo h que hace conmutativo al diagrama



Ejemplo 29.2. Todo módulo libre es proyectivo. En efecto, si S es base de módulo libre P, dado $s \in S$ existe $m \in M$ tal que $g(m) = f(s)$. Definimos entonces $h\colon P \to M$, $h(s) = m$ y extendemos por linealidad.

En particular, $\mathbb{Z}$ es libre como $\mathbb{Z}$-módulo.

Teorema 29.3. *Sea P un módulo. Las siguientes afirmaciones son equivalentes:*

1) P es proyectivo.
2) $\mathrm{Hom}_R(P,-)$ es exacto.
3) Toda sucesión exacta

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

se parte, es decir que existe $h \in \mathrm{Hom}_R(P,M)$ tal que $g \circ h = \mathrm{id}_P$. En particular, $M \simeq N \oplus P$.
4) P es sumando directo de un libre.

Demostración. Probemos primero que $(1) \Leftrightarrow (2)$. Sea

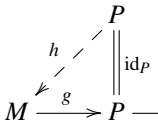
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

una sucesión exacta. Tenemos que probar que si P es proyectivo, entonces la sucesión

$$0 \longrightarrow \hom_A(P,A) \xrightarrow{f_*} \hom_A(P,B) \xrightarrow{g_*} \hom_A(P,C) \longrightarrow 0$$

es exacta. Dado un morfismo $\beta\colon P \to C$, como P es proyectivo y g es epimorfismo, existe $\alpha \in \mathrm{Hom}_R(P,B)$ tal que $g_*(\alpha) = g \circ \alpha = \beta$. Luego g_* es epimorfismo. Recíprocamente, es claro que si g_* es un epimorfismo entonces P es proyectivo.

Veamos ahora que $(1) \implies (3)$. Si $0 \to N \to M \to P \to 0$ es una sucesión exacta, entonces se parte, pues como P es proyectivo existe $h \in \mathrm{Hom}_P(P,N)$ tal que el diagrama



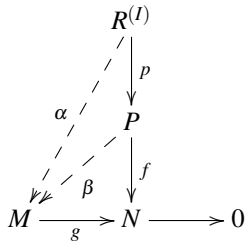
es conmutativo, lo que significa que $g \circ h = \mathrm{id}_P$. Para ver que $M \simeq N \oplus P$ basta usar la proposición 26.9.

Veamos ahora que $(3) \implies (4)$. Sabemos que P es cociente de un módulo libre, es decir que existe un conjunto I y un epimorfismo $\varphi\colon R^{(I)} \to P$. Como la sucesión

$$0 \longrightarrow \ker\varphi \longrightarrow R^{(I)} \xrightarrow{\varphi} P \longrightarrow 0$$

de módulos y morfismos es exacta, se parte es decir que existe $h \in \mathrm{Hom}_R(P,R^{(I)})$ tal que $\varphi \circ h = \mathrm{id}_P$. Luego P es sumando directo de un libre, pues $R^{(I)} \simeq \ker\varphi \oplus P$.

Finalmente probemos $(4) \Rightarrow (1)$. Si $f\colon M \to N$ es un epimorfismo y $g\colon P \to N$, como P es sumando directo del libre $R^{(I)}$, definimos $\beta\colon P \to M$, $\beta = \alpha \circ i$, donde $i\colon P \to R^{(I)}$ es la inclusión. El diagrama



donde $p\colon R^{(I)} \to P$ es tal que $p \circ i = \mathrm{id}_P$, es entonces conmutativo, pues

$$g \circ \beta = (g \circ \alpha) \circ i = f \circ (p \circ i) = f \circ \mathrm{id}_P = f. \qquad \square$$

No todo proyectivo es libre.

Ejemplo 29.4. Sea $R = \mathbb{Z} \times \mathbb{Z}$. Como R es libre como R-módulo, $\mathbb{Z} \times \{0\}$ es proyectivo, pues es sumando directo de un módulo libre. Sin embargo, $\mathbb{Z} \times \{0\}$ no es libre como R-módulo. En efecto, si lo fuera, sea $\{(x_i,0) : i \in I\}$ una base de $\mathbb{Z} \times \{0\}$. Entonces $(1,1) \cdot (x_1,0) = (x_1,0) = (1,0) \cdot (x_1,0)$, una contradicción.

Cocientes de proyectivos pueden no ser proyectivos.

Ejemplo 29.5. Veamos que el $\mathbb{Z}$-módulo $\mathbb{Z}/n\mathbb{Z}$ no es proyectivo. Si $\mathbb{Z}/n\mathbb{Z}$ es proyectivo, entonces, gracias al teorema anterior, la sucesión exacta

$$0 \longrightarrow n\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

donde i es la inclusión y π es el epimorfismo canónico, se parte, es decir existe $h \in \mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z})$ tal que $\pi \circ h = \mathrm{id}_{\mathbb{Z}/n}$, una contradicción pues sabemos que $\mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) = \{0\}$.

Submódulos de proyectivos pueden no ser proyectivos.

Ejemplo 29.6. Sea $M = \mathbb{Z}/4$ como $\mathbb{Z}/4$-módulo. Como M es libre, es proyectivo. Veamos que el submódulo $N = \{0, 2\}$ no es proyectivo. Si N fuera proyectivo, entonces la sucesión exacta

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{i} \mathbb{Z}/4 \xrightarrow{\pi} \mathbb{Z}/2 \longrightarrow 0,$$

debería partirse, lo que implicaría que tendríamos en particular un isomorfismo $\mathbb{Z}/4 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$ de grupos abelianos, una contradicción.

Ejercicio 29.7. Si N es un submódulo de M tal que M/N es libre, entonces N es sumando directo de M.

Si R es un anillo, $e \in R$ es **idempotente** si $e^2 = e$. Ejemplos triviales de idempotentes son 0 y 1. Observemos que si e es un idempotente no trivial, entonces $I_1 = Re$ y $I_2 = R(1-e)$ son ideales a izquierda tales que $I_1 \cap I_2 = \{0\}$ y además $R = I_1 + I_2$. En efecto, para ver que $R = I_1 + I_2$ basta observar que, como $1 = e + (1-e)$, entonces $r = r1 = r(e + (1-e)) = re + r(1-e)$ para todo $r \in R$. Para ver que $I_1 \cap I_2 = \{0\}$ sea $x \in I_1 \cap I_2$. Entonces $x = re = s(1-e)$ para ciertos $r, s \in R$ y luego

$$0 = s(1-e)e = xe = (re)e = re^2 = re = x.$$

En particular, por el primer teorema de isomorfismos,

$$R \simeq R/(I_1 \cap I_2) \simeq R/I_1 \times R/I_2.$$

Ejemplo 29.8. Si $e \in \mathbb{Z}/24$ es idempotente, entonces $e \in \{0, 1, 9, 16\}$.

Ejemplo 29.9. Los idempotentes no triviales de $M_2(\mathbb{R})$ son las matrices de la forma $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $a + d = 1$ y $ad = bc$.

Los idempotentes del anillo están en correspondencia biyectiva con los proyectores de la representación regular $M = {}_R R$. En efecto, si p es un proyector, entonces $e = p(1)$ es un idempotente. Recíprocamente, si e es un idempotente del anillo, entonces el morfismo $p\colon M \to M$, $m \mapsto e \cdot m$, es un proyector, pues

$$p(p(m)) = e \cdot (e \cdot m) = e^2 \cdot m = e \cdot m = p(m)$$

para todo $m \in M$.

Ejemplo 29.10. Como 0 y 1 son los únicos idempotentes del anillo $\mathbb{Z}$, la correspondencia biyectiva entre idempotentes del anillo y proyectores del módulo nos da otra demostración de que los únicos sumandos directos de $\mathbb{Z}$ son $\{0\}$ y $\mathbb{Z}$.

Ejemplo 29.11. Si $e \in R$ es idempotente, el ideal a izquierda Re es proyectivo como R-módulo. En efecto, la función $\varphi\colon R \to Re$, $r \mapsto re$, es un epimorfismo de módulos. La sucesión exacta

$$0 \longrightarrow \ker\varphi \longrightarrow R \xrightarrow{\varphi} Re \longrightarrow 0,$$

se parte, pues la inclusión $i\colon Re \to R$ es una sección: $\varphi(i(re)) = \varphi(re) = re^2 = re$. Luego $R \simeq \ker\varphi \oplus Re$ y entonces Re es proyectivo por ser sumando directo de un módulo libre.

Ejercicio 29.12. Sea R un anillo conmutativo y sea I un ideal de R. Demuestre que I es un sumando directo de R si y sólo si existe $u \in R$ tal que $I = (u) = (u^2)$.

Ejercicio 29.13. Demuestre que ${}_RR$ es semisimple si y sólo si todo ideal a izquierda de R está generado por un idempotente.

Proposición 29.14. *Sea M un módulo finitamente generado. Entonces M es proyectivo si y sólo si existe $n \in \mathbb{N}$ y $p \in \mathrm{Hom}_R(R^n, R^n)$ tal que $M \simeq p(R^n)$ y $p^2 = p$.*

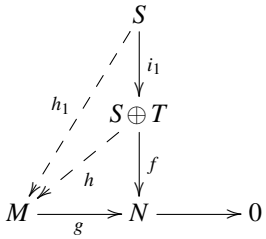
Demostración. Supongamos primero que M es proyectivo. Entonces M es sumando directo de R^n, digamos $R^n = M \oplus N$ para algún modulo N. La función $p\colon R^n \to R^n$, $p(m,n) = m$, es un morfismo de módulos tal que $p^2 = p$ y $p(R^n) = M$.

Recíprocamente, si existe $p \in \mathrm{Hom}_R(R^n, R^n)$ tal que $p^2 = p$ y $p(R^n) \simeq M$, entonces $p \circ (\mathrm{id} - p) = 0$. Esto nos permite descomponer al anillo R^n en idempotentes ortogonales, es decir $R^n \simeq p(R^n) \oplus (\mathrm{id} - p)(R^n)$. Luego $M \simeq p(R^n)$ es proyectivo por ser sumando directo de un libre. □

Ejemplo 29.15. Sea $R = \mathbb{Z}/6 = \{0, 1, \ldots, 5\}$ y sea $M = {}_RR$. Sabemos que M es libre con base $\{1\}$. Si $I = \{0, 2, 4\}$ y $J = \{0, 3\}$, entonces I y J son ideales de R, es decir que son submódulos de M. Si $m \in M$, entonces $m = -2m + 3m \in I + J$. Como además $m \in I \cap J = \{0\}$, se concluye que $M \simeq I \oplus J$. En particular, I y J son proyectivos como R-módulos por ser sumandos directos del módulo libre M. Observemos que I está generado por el idempotente $e = 4$ y que J está generado por el idempotente $1 - e = 3$.

Proposición 29.16. *El módulo $S \oplus T$ es proyectivo si y sólo si S y T son proyectivos.*

Demostración. Consideremos el diagrama



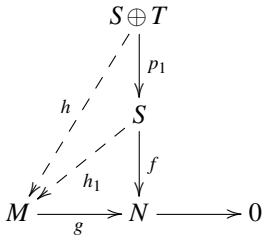
Veamos primero que si S y T son proyectivos, entonces $S \oplus T$ es proyectivo. Como S y T son proyectivos, existen $h_1 : S \to M$ y $h_2 : T \to M$ tales que $g \circ h_1 = f \circ i_1$ y $g \circ h_2 = f \circ i_2$, donde $i_1 : S \to S \oplus T$, $i_1(s) = (s,0)$, $i_2 : T \to S \oplus T$, $i_2(t) = (0,t)$. Si definimos el morfismo $h : S \oplus T \to M$,

$$h(s,t) = h_1(s) + h_2(t),$$

entonces tenemos que

$$\begin{aligned} g(h(s,t)) &= g(h_1(s) + h_2(t)) = g(h_1(s)) + g(h_2(t)) \\ &= f(i_1(s)) + f(i_2(t)) = f(s,0) + f(0,t) = f(s,t). \end{aligned}$$

Demostremos ahora que si $S \oplus T$ es proyectivo, entonces S es proyectivo. Consideramos el diagrama



Sea $i_1 : S \to S \oplus T$, $i_1(s) = (s,0)$. Como por hipótesis $S \oplus T$ es proyectivo, existe un morfismo $h : S \oplus T \to M$ tal que $g \circ h = f \circ p_1$. Definimos entonces $h_1 : S \to M$, $h_1(s) = h(s,0)$ y vemos que

$$g(h_1(s)) = g(h(s,0)) = f(s).$$

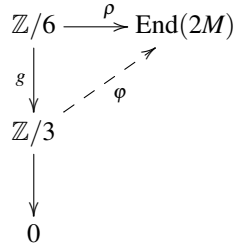
Similarmente se demuestra que T es también proyectivo. □

Dejamos como ejercicio demostrar que $\oplus_{i \in I} M_i$ es proyectivo si y sólo si M_i es proyectivo para todo $i \in$ I.

Ejemplo 29.17. Sea $R = \mathbb{Z}/6$. Veamos que todo R-módulo es proyectivo. Si M es un R-módulo, afirmamos que $M = 2M \oplus 3M$, donde $2M = \{2m : m \in M\} \subseteq M$ y $3M = \{3m : m \in M\} \subseteq M$, ambos submódulos de M. En efecto, $M = 2M + 3M$, pues $m = -2m + 3m \in 2M + 3M$. Además $2M \cap 3M = \{0\}$ pues si $m \in 2M \cap 3M$, entonces, como $m = 2x = 3y$ para ciertos $x, y \in M$, se tiene que

$$0 = 6x = 3(2x) = 3m = 3(3y) = 9y = 3y = m.$$

Veamos que $2M$ es proyectivo como R-módulo. Como $2M$ es un R-módulo, tenemos un morfismo de anillos $\rho\colon R \to \mathrm{End}(2M)$ con núcleo $\ker\rho = \{0,3\}$. Como $(\mathbb{Z}/6)/\ker\rho \simeq \mathbb{Z}/3$, la propiedad universal del cociente implica que existe un único morfismo φ tal que el diagrama



donde g es un epimorfismo, conmuta, es decir

$$\rho(k)(2m) = \varphi(g(k))(2m).$$

Luego $2M$ es un R-módulo si y sólo si $2M$ es un $\mathbb{Z}/3$-módulo. Como $\mathbb{Z}/3$ es un cuerpo, $2M$ es libre como $\mathbb{Z}/3$-módulo, por ser un espacio vectorial sobre el cuerpo $\mathbb{Z}/3$. En particular, $2M$ es proyectivo como $\mathbb{Z}/3$-módulo. En conclusión, $2M$ es proyectivo como R-módulo. Análogamente se demuestra que $3M$ es proyectivo. Luego M es proyectivo por ser suma directa de proyectivos.

Ejemplo 29.18. Sea $R = \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$. Como R es libre como R-módulo y además

$$R = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$$

los submódulos $\begin{pmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$ son proyectivos.

Veamos otro ejemplo de un módulo proyectivo que no es libre. Recordemos que si R es un anillo conmutativo e I y J son ideales de R, entonces

$$I + J = \{x + y \mid x \in I,\ y \in J\}$$

es el menor ideal que contiene a $I \cup J$. Además IJ es el ideal formado por las sumas finitas $\sum_i x_i y_i$, donde $x_i \in I$, $y_i \in J$.

Lema 29.19. *Sea R un dominio íntegro y sean I y J ideales tales que $I + J = R$. Consideremos el morfismo de R-módulos $g\colon I \times J \to R$, $(x,y) \mapsto x + y$. Entonces:*

1) g es sobreyectiva.
2) $\ker(g) = \{(x,-x) \mid x \in I \cap J\}$.

3) $I \times J \simeq (I \cap J) \oplus R$ como R-módulos.
4) Si $I \cap J$ es principal entonces I y J son R-módulos proyectivos.

Demostración. Las primeras dos afirmaciones son evidentes.

Para demostrar (3) consideremos la sucesión exacta

$$0 \longrightarrow I \cap J \xrightarrow{f} I \times J \xrightarrow{g} R \longrightarrow 0$$

donde $f(x) = (x, -x)$. Como R es libre como R-módulo, R es proyectivo y entonces la sucesión se parte, es decir $I \oplus J \simeq I \times J \simeq (I \cap J) \oplus R$ como R-módulos.

Para demostrar (4), supongamos que $I \cap J = (x)$. Si $x = 0$, como $I \cap J = \{0\}$, el ítem nos dice que $I \oplus J \simeq I \times J \simeq R$ y luego I y J son proyectivos por ser sumandos directos de un libre. Si $x \neq 0$, entonces, como R es un dominio íntegro, $R \to I \cap J$, $r \mapsto rx$, es un isomorfismo de R-módulos. Luego $I \oplus J \simeq I \times J \simeq (I \cap J) \oplus R \simeq R \oplus R$ y entonces I y J son proyectivos por ser sumandos directos de un libre. □

Veamos una aplicación concreta del lema anterior.

Ejemplo 29.20. Sea $R = \mathbb{Z}[\sqrt{-5}]$ y consideremos los ideales

$$I = (3, 1 + \sqrt{-5}), \quad J = (3, 1 - \sqrt{-5}).$$

Vamos a demostrar lo siguiente:

1) I no es principal.
2) I no es libre como R-módulo.
3) I es proyectivo.
4) $R/I \simeq \mathbb{Z}_3$ y luego I es maximal.

Valen además las afirmaciones análogas para J.

Demostremos la primera afirmación. Si I es principal, digamos $I = (a + b\sqrt{-5})$ entonces, como $3 \in I$, existen $c, d \in \mathbb{Z}$ tales que $3 = (a + b\sqrt{-5})(c + \sqrt{-5}d)$. Si aplicamos la función multiplicativa $N(a + b\sqrt{-5}) = a^2 + 5b^2$,

$$9 = (a^2 + 5b^2)(c^2 + 5d^2)$$

y entonces $a^2 + 5b^2 \in \{1, 3, 9\}$. Como $I \neq R$, $a^2 + 5b^2 \geq 5$ y luego $a^2 + 5b^2 = 9$. En particular,

$$(a, b) \in \{(-3, 0), (3, 0), (2, 1), (2, -1), (-2, -1), (-2, 1)\}$$

Vimos que los casos $(a, b) \in \{(-3, 0), (3, 0)\}$ no son posibles. Para el resto de los posibles valores de (a, b) se tiene que $9 = 9(c^2 + 5d^2)$ y luego $c^2 + 5d^2 = 1$, lo que implica que $c \in \{-1, 1\}$ y entonces $3 = a + b\sqrt{-5}$ o bien $3 = -a - b\sqrt{-5}$, una contradicción.

Demostremos la segunda afirmación. Supongamos que I es libre como R-módulo. Como R es numberable, sea $\{x_i \mid i \in \mathbb{N}\}$ es una base de I. Tenemos entonces que $|I| = 1$, pues de lo contrario, si $|I| \geq 2$, como $x_1(-x_2) + x_2 x_1 = 0$, se tendría que el

conjunto $\{x_i \mid i \in I\}$ es linealmente dependiente. Tenemos entonces que $|I| = 1$, es decir I es principal, una contradicción.

Demostremos ahora la tercera afirmación. Primero observemos que $I+J = R$ pues $I+J$ es un ideal y además $1 = (3-(1+\sqrt{-5}))-(1-\sqrt{-5}) \in I+J$. Probemos ahora $I \cap J$ es principal, más precisamente $I \cap J = (3)$. Para esto primero observemos que, en general, vale la fórmula

$$(I+J)(I \cap J) \subseteq IJ$$

y entonces, como $I+J = R$, se tiene que $I \cap J = IJ$. Todo elemento del ideal IJ es una suma finita $\sum_i x_i y_i$, donde $x_i \in I$, $y_i \in J$. Como

$$\begin{aligned}\sum &(3u+(1+\sqrt{-5})v(3u'+(1-\sqrt{-5})v' \\ &= 3\sum(3uu'+uv'(1-\sqrt{-5})+u'v(1+\sqrt{-5})+2vv'),\end{aligned}$$

es claro que $IJ \subseteq (3)$. La otra inclusión es evidente. El lema anterior implica que entonces I y J son ambos proyectivos.

Probemos ahora la última afirmación. Consideremos la inclusión $i\colon \mathbb{Z} \to \mathbb{Z}[\sqrt{-5}]$ y el epimorfismo canónico $p\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}]/I$. Entonces $f = p \circ i$ es un morfismo sobreyectivo tal que $\ker(p \circ i) = (3)$ pues si $m \in \ker(p \circ i)$ entonces

$$\begin{aligned}m &= 3(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}) \\ &= (3a+c-5d)+(3b+d+c)\sqrt{-5}.\end{aligned}$$

Luego $m = 3a-3b-6d \in 3\mathbb{Z}$. La inclusión $3\mathbb{Z} \subseteq \ker(p \circ i)$ es trivial. Para ver que f es sobreyectivo basta observar que $f(a-b) = a+b\sqrt{-5}$, pues

$$f(a-b) = p(a-b) = (a-b)+I = (a+b\sqrt{-5})+I$$

ya que $(a-b)-(a+b\sqrt{-5}) = -b(1+\sqrt{-5}) \in I$. Por el teorema de isomorfismos, $\mathbb{Z}/3\mathbb{Z} \simeq p(i(\mathbb{Z}))$ y luego I es un ideal maximal.

Ejercicio 29.21. Sean P y P_1 dos módulos proyectivos. Consideremos el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{f} & P & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & & & & & \| & & \\ 0 & \longrightarrow & K_1 & \xrightarrow{f_1} & P_1 & \xrightarrow{g_1} & M & \longrightarrow & 0 \end{array}$$

con filas exactas. Demuestre que $P \oplus K_1 \simeq P_1 \oplus K$.

Capítulo 30
El teorema de estructura

En este capítulo R será un dominio de ideales principales. Esta hipótesis hace que los módulos tengan buenas propiedades, casi como pasa en el caso de espacios vectoriales.

Teorema 30.1. *Sea R un dominio de ideales principales. Si F es un módulo libre finitamente generado y N es un submódulo de F, entonces N es también libre y además* $\operatorname{rank}(N) \leq \operatorname{rank}(F)$.

Demostración. Procederemos por inducción en $n = \operatorname{rank}(F)$. Si $n = 1$, entonces $F \simeq {}_RR$ y los submódulos de F son exactamente los ideales a izquierda de R. En particular, $N = (r)$ para algún $r \in R$. Si $r = 0$, entonces $N = \{0\}$ y el resultado es verdadero. Si $r \neq 0$, entonces $\{r\}$ es base de N y también el resultado es cierto.

Supongamos ahora que el resultado es válido para todo módulo libre de rango $< n$. Sea $\{f_1, \ldots, f_n\}$ una base de F y sea $F_n = (f_1, \ldots, f_{n-1})$. Por hipótesis inductiva, el submódulo $U = N \cap F_n$ es libre de rango $\leq n-1$. Sea $\{n_1, \ldots, n_k\}$ una base de U (por convención, si $U = \{0\}$, entonces $k = 0$). Si $f \in F$, existen únicos $r_1, \ldots, r_n \in R$ tales que

$$f = \sum_{i=1}^{n} r_i \cdot f_i.$$

Queda definido entonces un morfismo

$$\varphi \colon F \to R, \quad \sum_{i=1}^{n} r_i \cdot f_i \mapsto r_n.$$

Si $\varphi(N) = \{0\}$, entonces $N \subseteq (f_1, \ldots, f_{n-1})$ y luego $N = U$. Si $\varphi(N) \neq \{0\}$, entonces $\varphi(N)$ es un ideal de R, digamos $\varphi(N) = (x)$ para algún $x \in R \setminus \{0\}$. Sea $n_{k+1} \in N$ tal que $\varphi(n_{k+1}) = x$. Veamos que $\{n_1, \ldots, n_k, n_{k+1}\}$ es base de N. Si $n \in N$, entonces $\varphi(n) = rx$ para algún $r \in R$. Entonces $n - r \cdot n_{k+1} \in N \cap \ker \varphi = N \cap F_n = U$ pues $\varphi(n - r \cdot n_{k+1}) = 0$. En particular,

$$n - r \cdot n_{k+1} \in (n_1, \ldots, n_k) \implies n \in (n_1, \ldots, n_k, n_{k+1}).$$

Veamos ahora que $\{n_1,\dots,n_k,n_{k+1}\}$ es linealmente independiente. Si

$$0=\sum_{i=1}^{k+1} r_i\cdot n_i,$$

para $r_1,\dots,r_{k+1}\in R$, entonces, como $\varphi(n_i)=0$ para todo $i\in\{1,\dots,k\}$, se tiene que

$$0=\varphi(r_{k+1}\cdot n_{k+1})=r_{k+1}x,$$

que implica $r_{k+1}=0$. Queda entonces que $\sum_{i=1}^{k} r_i\cdot n_i=0$. Como $\{n_1,\dots,n_k\}$ es base de U, se concluye que $r_1=\cdots=r_k=0$. □

El teorema anterior también vale en el caso de bases infinitas. La demostración, sin embargo, depende del lema de Zorn.

Corolario 30.2. *Sea R un dominio de ideales principales. Si M es proyectivo y finitamente generado, entonces M es libre.*

Demostración. Supongamos que $M=(m_1,\dots,m_k)$. Sabemos que M es sumando directo de un libre F. Fijemos una base de F y sea $X=\{f_1,f_2,\dots\}$ un subconjunto finito de esa base de F tal que

$$m_j=\sum_{i=1}^{n_j} r_{ij}\cdot f_i$$

para ciertos $r_{ij}\in R$ y ciertos $n_1\dots,n_k\in\mathbb{N}$. Por construcción, X es linealmente indepdendiente y $M=(X)$. □

El corolario anterior vale también para módulos arbitrarios. La demostración puede consultarse por ejemplo en [4, I, Theorem 5.1].

Corolario 30.3. *Sea R un dominio de ideales principales. Si M es finitamente generado y N es un submódulo de M, entonces N es también finitamente generado.*

Demostración. Sabemos que existe un módulo libre F de rango finito y un epimorfismo $\varphi\colon F\to M$. Como $N_1=\varphi^{-1}(N)$ es un submódulo de F, el teorema anterior implica que $\operatorname{rank}(N_1)\le\operatorname{rank}F$. Si $\{x_1,\dots,x_k\}$ es base de N_1, entonces, como φ es un epimorfismo, $\{\varphi(x_1),\dots,\varphi(x_k)\}$ es un conjunto de generadores de $\varphi(N_1)=\varphi(\varphi^{-1}(N))=N$. En particular, $\operatorname{rank}(N)\le k=\operatorname{rank}(N_1)\le\operatorname{rank}(F)$. □

Algunos ejercicios útiles:

Ejercicio 30.4. Sea R un dominio de ideales principales y sea M un módulo libre. Si S es un submódulo de M tal que M/S es libre, entonces $M\simeq S\oplus(M/S)$. Si además S es libre, entonces

$$\operatorname{rank}(M)=\operatorname{rank}(S)+\operatorname{rank}(M/S).$$

Ejercicio 30.5. Sea R un dominio de ideales principales. Si M es un módulo libre de rango n, entonces todo conjunto linealmente independiente de M tiene a lo sumo n elementos.

Ejercicio 30.6. Sea R un dominio de ideales principales y sean M y N dos módulos libres. Demuestre que $M \simeq N$ si y sólo si $\text{rank}(M) = \text{rank}(N)$.

Ejercicio 30.7. Sea R un dominio de ideales principales. Si M es un módulo libre tal que $n = \text{rank}(M)$ y $\{s_1, \ldots, s_n\}$ es un conjunto de generadores, entonces $\{s_1, \ldots, s_n\}$ es una base de M.

Si M es un módulo, el **anulador** de M se define como

$$\text{Ann}(M) = \{r \in R : r \cdot m = 0 \text{ para todo } m \in M\}.$$

Si $m \in M$ se define

$$\text{Ann}(m) = \{r \in R : r \cdot m = 0\}.$$

Observar que $\text{Ann}(M) = \cap_{m \in M} \text{Ann}(m)$. Dejamos como ejercicio demostrar que $\text{Ann}(M)$ y $\text{Ann}(m)$ son ideales de R. Si $r \in R$, el anulador de r en M se define como

$$\text{Ann}_M(r) = \{m \in M : r \cdot m = 0\}.$$

Dejamos como ejercicio demostrar que $\text{Ann}_M(r)$ es un submódulo de M.

Ejercicio 30.8. Sean M un módulo, $m \in M$ y $r \in R$ tal que $\text{Ann}(m) = (r)$. Sea $p \in R$ irreducible.

1) Si p divide a r, entonces $(m)/p \cdot (m) \simeq R/(p)$.
2) Si p no divide a r, entonces $p \cdot (m) = (m)$.

La **torsión** de un módulo M se define como el subconjunto

$$T(M) = \{m \in M : r \cdot m = 0 \text{ para algún } r \in R\}.$$

Queda como ejercicio demostrar que $T(M)$ es un submódulo de M. Se dice que un módulo M **no tiene torsión** si $T(M) = \{0\}$ y que es **de torsión** si $T(M) = M$.

Ejercicio 30.9. Si $M \simeq N$, entonces $T(M) \simeq T(N)$.

Ejercicio 30.10. Demuestre que $T(\oplus_{i \in I} M_i) \simeq \oplus_{i \in I} T(M_i)$.

Ejercicio 30.11. Sean R un dominio principal y M un R-módulo. Pruebe que si M es finitamente generado y $S \subseteq M$ es un submódulo libre tal que M/S no tiene torsión, entonces M es libre

Ejemplos 30.12.

1) $T({}_R R) = \{r \in R : rs = 0 \text{ para algún } s \in R\}$.
2) $T(\mathbb{Z}/n) = \mathbb{Z}/n$.
3) $T(\mathbb{Q}) = \{0\}$.

4) $T(\mathbb{Z}^{\mathbb{N}}) = \{0\}$.

Ejemplo 30.13. Si V es un espacio vectorial de dimensión finita y $T\colon V \to V$ es una transformación lineal, sabemos que V es un $K[X]$-módulo con la acción

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Veamos que V es de torsión, es decir $V = T(V)$. Sea $n = \dim V$. Si $v \in V$, entonces $\{v, T(v), \ldots, T^n(v)\}$ es linealmente dependiente, pues tiene $n+1$ elementos. En particular, existen $a_0, \ldots, a_n \in K$ no todos cero tales que

$$0 = \sum_{i=0}^{n} a_i T^i(v) = \left(\sum_{i=0}^{n} a_i X^i\right) \cdot v.$$

Luego $v \in T(V)$.

Teorema 30.14. *Sea R un dominio de ideales principales y sea M finitamente generado. Si $T(M) = \{0\}$, entonces M es libre.*

Demostración. Sin perder generalidad podemos suponer que M es no nulo. Supongamos además que $M = (X)$, donde X es un conjunto finito de generadores. Si $x \in X$, entonces $r \cdot x = 0 \iff r = 0$, pues $T(M) = \{0\}$. Sea $S = \{x_1, \ldots, x_k\} \subseteq X$ maximal con respecto a la siguiente propiedad:

$$r_1 \cdot x_1 + \cdots + r_k \cdot x_k = 0 \text{ para } r_1, \ldots, r_k \in R \implies r_1 = \cdots = r_k = 0.$$

Sea $F = (S)$ el módulo libre con base en el conjunto S. Si $X = S$, no hay nada para demostrar. Si $y \in X \setminus S$, entonces existen $r_y, r_1, \ldots, r_k \in R$ no todos cero tales que

$$r_y \cdot y + \sum_{i=1}^{k} r_i \cdot x_i = 0.$$

Como entonces $r_y \cdot y = -\sum_{i=1}^{k} r_i \cdot x_i \in F$, se concluye que $r_y \neq 0$, pues si $r_y = 0$ entonces $r_1 = \cdots = r_k = 0$. Como X es finito,

$$r = \prod_{y \in X \setminus S} r_y$$

está bien definido pues R es conmutativo y es tal que $r \cdot X \subseteq F$. Si $f\colon M \to M$, $x \mapsto r \cdot x$, entonces f es un morfismo tal que $f(M) = r \cdot M$. Como $T(M) = \{0\}$, entonces $\ker f = \{0\}$. Luego

$$r \cdot M = f(M) \simeq M$$

y en consecuencia M es libre. □

Teorema 30.15. *Sea R un dominio de ideales principales. Si M es un módulo finitamente generado, entonces $M = T(M) \oplus F$ con $F \simeq M/T(M)$ libre y finitamente generado. La parte de torsión es única y la parte libre es única salvo isomorfismos.*

Demostración. Veamos que $T(M/T(M)) \simeq \{0\}$. Si $x + T(M) \in T(M/T(M))$, sea $r \in R \setminus \{0\}$ tal que $r \cdot (x + T(M)) = T(M)$. Entonces $r \cdot x \in T(M)$, es decir que existe $s \in R \setminus \{0\}$ tal que $s \cdot (r \cdot x) = (sr) \cdot x = 0$. Como $sr \neq 0$, se concluye que $x \in T(M)$.

Como M es finitamente generado, el cociente $M/T(M)$ es también finitamente generado. Como además $M/T(M)$ no tiene torsión, se concluye que $M/T(M)$ es libre. Como entonces $M/T(M)$ es proyectivo, la sucesión exacta

$$0 \longrightarrow T(M) \xrightarrow{i} M \xrightarrow{\pi} M/T(M) \longrightarrow 0$$

donde i es la inclusión y π es el morfismo canónico, el teorema 29.3 implica que $M \simeq T(M) \oplus M/T(M)$.

Para demostrar la unicidad, supongamos que $M = T \oplus L$, donde T es de torsión y L es libre. Primero demostraremos que $T = T(M)$. Claramente $T \subseteq T(M)$. Por otro lado, si $m \in T(M)$, entonces $m = t + l$ para ciertos $t \in T$ y $l \in L$. En particular, $r \cdot m = 0$ y $s \cdot t = 0$ para ciertos $r, s \in R$. Como R es conmutativo,

$$0 = (rs) \cdot m = (rs) \cdot (t + l) = (rs) \cdot t + (rs) \cdot l = (rs) \cdot l.$$

y entonces $l \in T(L)$. Pero como L es libre, $T(L) = \{0\}$ (pues $T(L)$ es también libre y entonces cualquier elemento x de una base de $T(L)$ sería tal que $\{x\}$ es linealmente independiente, una contradicción). Luego $l = 0$ y en consecuencia $m = t \in T$. La unicidad salvo isomorfismo de la parte libre se obtiene inmediatamente al observar que ese submódulo es isomorfo a $M/T(M)$. □

Si $p \in R$ es un elemento irreducible, se define la componente p-primaria de M como el subconjunto

$$M_p = \{x \in M : p^l \cdot x = 0 \text{ para algún } l \in \mathbb{N}\}.$$

Dejamos como ejercicio demostrar que M_p es un submódulo de M.

Lema 30.16. *Sean $p, t \in R$ tales que p y t son coprimos. Si $p \in R$ es irreducible y además $\mathrm{Ann}(M) = (p^k t)$, entonces $\mathrm{Ann}_M(p^k) = M_p$.*

Demostración. Demostremos que $\mathrm{Ann}_M(p^k) \supseteq M_p$, ya que la otra inclusión es trivial. Si $x \in M_p$, entonces $p^k \cdot x = 0$ para algún $l \in \mathbb{N}$. Observemos que $(p^k t) \cdot x = 0$, pues $x \in M$. Como p^l y t son coprimos, existen $r, s \in R$ tales que $1 = rp^l + st$ y luego

$$p^k \cdot x = 1 \cdot (p^k \cdot x) = (rp^l + st) \cdot (p^k \cdot x) = rp^{l+k} \cdot x + (st) \cdot (p^k \cdot x) = 0. \qquad \square$$

Lema 30.17. *Si $\mathrm{Ann}(M) = (ab)$ y a y b son coprimos, entonces*

$$M = \mathrm{Ann}_M(a) \oplus \mathrm{Ann}_M(b).$$

Demostración. Como a y b son coprimos, existen $r,s \in R$ tales que $1 = ra+sb$. Si $m \in M$, entonces

$$m = 1 \cdot m = (ra+sb) \cdot m = (ra) \cdot m + (sb) \cdot m \in \mathrm{Ann}_M(b) + \mathrm{Ann}_M(a),$$

pues $(ab) \cdot M = 0$. Además, si $m \in \mathrm{Ann}_M(a) \cap \mathrm{Ann}_M(b)$, entonces

$$m = 1 \cdot m = (ra+sb) \cdot m = 0. \qquad \square$$

Los dos lemas que vimos nos permiten demostrar el siguiente resultado:

Teorema 30.18 (de la descomposición primaria). *Sea R un dominio de ideales principales y sean $p_1, \ldots, p_k \in R$ irreducibles distintos y no asociados tales que $\mathrm{Ann}(M) = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})$. Si M es finitamente generado y $T(M) = M$, entonces*

$$M = \bigoplus_{i=1}^{k} M_{p_i}.$$

Demostración. Como $T(M) = M$, $\mathrm{Ann}(M) \neq \{0\}$. En efecto, si $M = (m_1, \ldots, m_l)$, entonces cada $m_i \in T(M)$ y entonces existe $r_i \in R \setminus \{0\}$ tal que $r_i \cdot m_i = 0$ para todo i. Como R es un dominio, $r_1 \cdots r_l \neq 0$ y cumple $(r_1 \cdots r_l) \cdot m_i = 0$ para todo $i \in \{1, \ldots, l\}$, es decir $r_1 \cdots r_l \in \mathrm{Ann}\, M$. Los dos lemas que vimos anteriormente nos permiten escribir entonces

$$M = \bigoplus_{i=1}^{k} \mathrm{Ann}_M(p_i^{\alpha_i}) = \bigoplus_{i=1}^{k} M_{p_i}. \qquad \square$$

Puede demostrarse que la descomposición mencionada en el teorema anterior es única salvo en el orden de los sumandos. Más precisamente, si

$$M = N_{q_1} \oplus \cdots \oplus N_{q_l},$$

donde los N_{q_i} son primarios tales que $\mathrm{Ann}(N_{q_i}) = (q_i^{\beta_i})$ y los $q_1, \ldots, q_l$ son irreducibles distintos no asociados, entonces $k = l$ y existe $\sigma \in \mathbb{S}_k$ tal que $M_{p_i} = N_{q_{\sigma(i)}}$ para todo i, los $q_{\sigma(i)}$ y los p_i son asociados para todo i y además

$$q_1^{\beta_1} \cdots q_k^{\beta_k} = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Para la demostración ver por ejemplo [5, Theorem 6.9].

Teorema 30.19 (de la descomposición cíclica). *Sea R un dominio de ideales principales. Sea M un módulo finitamente generado tal que $T(M) = M$. Si $\mathrm{Ann}(M) = (p^{\alpha})$ para algún $p \in R$ irreducible, entonces*

$$M = (m_1) \oplus \cdots \oplus (m_k),$$

donde cada $m_j \in M$ es tal que $\mathrm{Ann}(m_j) = (p^{\alpha_j})$ y $\alpha = \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k$.

Demostración. Sea $m \in M$ tal que $p^\alpha \cdot m = 0$ y $p^{\alpha-1} \cdot m \neq 0$. Si $M = (m)$, no hay nada para demostrar. En caso contrario, vamos a demostrar que existe un submódulo S de M tal que $M = (m) \oplus S$. En este caso, como S también cumple las hipótesis del teorema, podemos repetir el procedimiento y obtener

$$M = (m) \oplus (m_1) \oplus \cdots \oplus (m_k) \oplus S_k,$$

donde $\mathrm{Ann}(m_i) = (p^{\alpha_i})$. Como M es noetheriano, la sucesión

$$(m) \subseteq (m, m_1) \subseteq (m, m_1, m_2) \subseteq \cdots$$

debe estabilizarse, lo que se traduce en la existencia de algún $k \in \mathbb{N}$ tal que $S_k = \{0\}$.

Sea $M_1 = (m)$. Si $M_1 \neq M$, sea $x \in M \setminus M_1$. Necesitamos encontrar $r \in R$ tal que $S_2 = (x - r \cdot m)$ esté en suma directa con (m), es decir $(m) \cap S_2 = \{0\}$. Si $y \in (m) \cap S_2$,

$$y = a \cdot m = b \cdot (x - r \cdot m) \implies b \cdot x = (a + br) \cdot m \in (m)$$

para ciertos $a, b \in R$. Un cálculo sencillo nos muestra que el conjunto

$$I = \{\lambda \in R : \lambda \cdot x \in (m)\}.$$

es un ideal de R tal que $p^\alpha \in I$ y $b \in I$. Como R es principal y p es irreducible, entonces $I = (p^\beta)$ para algún $\beta \leq \alpha$. Si $\beta = 0$, entonces $I = R$ y luego $x = 1 \cdot x \in (m)$, una contradicción. Luego $\beta \neq 0$. Como $p^\beta \in I$, entonces $p^\beta \cdot x = c \cdot m$ para algún $c \in R$. En particular,

$$0 = p^\alpha \cdot x = p^{\alpha-\beta} \cdot (p^\beta \cdot x) = (p^{\alpha-\beta} c) \cdot m,$$

lo que implica que $p^{\alpha-\beta} c \in \mathrm{Ann}(m) = (p^\alpha)$ y entonces $c = d p^\beta$ para algún $d \in R$. En particular,

$$p^\beta \cdot x = c \cdot m = (d p^\beta) \cdot m.$$

Por definición $b \in I$ y entonces $b = e p^\beta$ para algún $e \in R$. Luego

$$b \cdot x = (e p^\beta) \cdot x = (ed p^\beta) \cdot m,$$

lo que implica que si $r = d \in R$, entonces

$$y = b \cdot (x - d \cdot m) = b \cdot x - b \cdot (d \cdot m) = 0.$$

La contrucción general es similar. Si $M_k = (m) \oplus S_k$ es tal que $M_k \neq M$, afirmamos que existe un submódulo S_{k+1} de M tal que $S_k \subsetneq S_{k+1}$ y además $(m) \cap S_{k+1} = \{0\}$. En efecto, como $M \neq M_k$, existe $x \in M \setminus M_k$. Queremos encontrar $r \in R$ tal que $(m) \cap (S_k, x - r \cdot m) = \{0\}$. Sea $S_{k+1} = (S_k, x - r \cdot m)$. Si $y \in (m) \cap S_{k+1}$, entonces existen $s \in S_k$ y $a, b \in R$ tales que $y = a \cdot m = s + b \cdot (x - r \cdot m)$, es decir

$$b \cdot x = (a + br) \cdot m - s \in (m) \oplus S_k.$$

El conjunto

$$I = \{\lambda \in R : \lambda \cdot x \in (m) \oplus S_k\}$$

es un ideal de R tal que $p^\alpha \in I$. Como I es principal, $I = (p^\beta)$ para algún $\beta \leq \alpha$. Además $\beta \neq 0$ pues $x = 1 \cdot x \notin (m) \oplus S_k$. Como $p^\beta \in I$, entonces $p^\beta \cdot x = c \cdot m + t$ para algún $c \in R$ y $t \in S_k$. En particular,

$$0 = p^\alpha \cdot x = p^{\alpha-\beta} \cdot (p^\beta \cdot x) = (p^{\alpha-\beta} c) \cdot m + p^{\alpha-\beta} \cdot t.$$

Luego $(p^{\alpha-\beta} c) \cdot m = 0$, pues $(m) \cap S_k = \{0\}$, y entonces podemos escribir $c = dp^\beta$ para algún $d \in R$, ya que $p^{\alpha-\beta} c \in \mathrm{Ann}(m) = (p^\alpha)$. Tenemos entonces que

$$p^\beta \cdot x = (dp^\beta) \cdot m + t.$$

Por otro lado, como $b \in I$, existe $e \in R$ tal que $b = ep^\beta$ y entonces

$$b \cdot x = e \cdot (p^\beta \cdot x) = e \cdot ((dp^\beta) \cdot m + t) = (edp^\beta) \cdot m + e \cdot t.$$

$y = b \cdot (x - r \cdot m) = (edp^\beta - ep^\beta r) \cdot m$, se concluye que $y = 0$ si elegimos $r = d$. En efecto, si $y \in (m) \cap S_{k+1}$, entonces $y = s + e \cdot t \in S_k$. Luego $y \in (m) \cap S_k = \{0\}$. □

Puede demostrarse que la descomposición del teorema anterior es única. Más precisamente, si $M = (n_1) \oplus \cdots \oplus (n_l)$, donde $\mathrm{Ann}(n_i) = (q^{\beta_i})$ para todo i y algún irreducible q de R y $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_l$, entonces $\mathrm{Ann}(n_i) = \mathrm{Ann}(m_i)$ para todo i. En particular, $k = l$, p y q son asociados y $\alpha_i = \beta_i$ para todo $i \in \{1, \ldots, k\}$. Para la demostración ver por ejemplo [5, Theorem 6.11].

Corolario 30.20. *Sea R un dominio de ideales principales. Si M es un módulo finitamente generado, entonces $M = F \oplus T$, donde F es libre y T es un submódulo de torsión. Si $\mathrm{Ann}(T) = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})$, donde los p_i son irreducibles distintos y no asociados, entonces M puede descomponerse como*

$$M = F \oplus \underbrace{\big((m_{1,1}) \oplus \cdots \oplus (m_{1,l_1})\big)}_{M_{p_1}} \oplus \cdots \oplus \underbrace{\big((m_{k,1}) \oplus \cdots \oplus (m_{k,l_k})\big)}_{M_{p_k}}$$

*donde $\mathrm{Ann}(m_{i,j}) = (p_i^{\alpha_{i,j}})$ y $\alpha_i = \alpha_{i,1} \geq \alpha_{i,2} \geq \cdots \geq \alpha_{i,l_i}$. Los $p_i^{\alpha_{i,j}}$ son los **divisores elementales** de M.*

Demostración. Sabemos que M puede descomponerse como $M = F \oplus T(M)$, donde F es un submódulo libre y $T(M)$ es el submódulo de torsión de M. Por el teorema de la descomposición primaria, podemos descomponer al submódulo $T(M)$ como $T(M) = M_{p_1} \oplus \cdots \oplus M_{p_k}$ para ciertos irreducibles distintos y no asociados $p_1, \ldots, p_k \in R$. A su vez, por el teorema de la descomposición cíclica, cada M_{p_j} puede descomponerse como suma directa de cíclicos, digamos

$$M_{p_j} = (m_{j,1}) \oplus \cdots \oplus (m_{j,l_j}),$$

donde $\mathrm{Ann}(m_{i,j}) = (p_i^{\alpha_{i,j}})$ y $\alpha_i = \alpha_{i,1} \geq \alpha_{i,2} \geq \cdots \geq \alpha_{i,l_i}$. □

También puede demostrarse la unicidad de la descomposición del corolario anterior. Más precisamente, el rango de la parte libre, los submódulos primarios y los anuladores quedarán unívocamente determinados por M. Una demostración puede consultarse en [5, Theorem 6.12].

Corolario 30.21 (descomposicion en factores invariantes). *Sea R un dominio de ideales principales. Si M es un módulo finitamente generado, entonces*

$$M = F \oplus D_1 \oplus \cdots \oplus D_k,$$

*donde F es un submódulo libre de M y los D_i son submódulos cíclicos de M tales que $\operatorname{Ann}(D_i) = (d_i)$, donde $d_i \mid d_{i-1}$ para todo $i \in \{2, \ldots, k\}$. Los d_i son los **factores invariantes** de la descomposicion.*

Demostración. El corolario anterior nos permite descomponer a M como

$$M = F \oplus \underbrace{\big((m_{1,1}) \oplus \cdots \oplus (m_{1,l_1})\big)}_{M_{p_1}} \oplus \cdots \oplus \underbrace{\big((m_{k,1}) \oplus \cdots \oplus (m_{k,l_k})\big)}_{M_{p_k}},$$

donde $\alpha_i = \alpha_{i,1} \geq \alpha_{i,2} \geq \cdots \geq \alpha_{i,l_i}$. Si agrupamos ordenadamente los sumandos cíclicos de orden coprimo, digamos

$$\begin{aligned} D_1 &= (m_{1,1}) \oplus (m_{2,1}) \oplus \cdots \\ D_2 &= (m_{1,2}) \oplus (m_{2,2}) \oplus \cdots \\ D_3 &= (m_{1,3}) \oplus (m_{2,3}) \oplus \cdots \\ &\vdots \end{aligned}$$

obtenemos la descomposición que buscamos. □

Puede demostrarse que los factores invariantes quedan únivocamente determinados, salvo multiplicación por unidades, por el módulo M. Ver por ejemplo [5, Theorem 6.13].

Ejemplo 30.22. Para entender mejor la descomposición del teorema anterior hagamos un ejemplo. Si un módulo M admite una descomposición cíclica de la forma

$$M = \left((m_{1,1} \oplus (m_{1,2})) \oplus (m_{2,1}) \oplus ((m_{3,1}) \oplus (m_{3,2}) \oplus (m_{3,3})\right),$$

donde $\operatorname{Ann}(m_{1,1}) = p_1^3$, $\operatorname{Ann}(m_{1,2}) = p_1^2$, $\operatorname{Ann}(m_{2,1}) = (p_2)$, $\operatorname{Ann}(m_{3,1}) = (p_3^3)$, $\operatorname{Ann}(m_{3,2}) = (p_3^3)$ y $\operatorname{Ann}(m_{3,3}) = (p_3)$ para irreducibles distintos no asociados p_1, p_2 y p_3, entonces entonces $M = D_1 \oplus D_2 \oplus D_3$, donde

$$D_1 = (m_{1,1}) \oplus (m_{2,1}) \oplus (m_{3,1}), \quad D_2 = (m_{1,2}) \oplus (m_{3,2}), \quad D_3 = (m_{3,3}).$$

En este caso, $d_1 = p_1^3 p_2 p_3^3$, $d_2 = p_1^2 p_3^3$ y $d_3 = p_3$.

Para terminar el capítulo veremos un algoritmo que nos permite calcular efectivamente los factores invariantes de un módulo finitamente generado. Aunque lo que haremos puede hacerse sobre dominios de ideales principalers, nos concentraremos únicamente en el caso en que R sea un dominio euclidiano, ya que solamente en este contexto el algoritmo es constructivo.

Si M es un módulo finitamente generado y $\{m_1,\dots,m_k\}$ es un conjunto de generadores, existe un epimorfismo $\varphi\colon R^k \to M$, $(r_1,\dots,r_k)\mapsto \sum_{i=1}^k r_i\cdot m_i$. Por el primer teorema de isomorfismos, $M\simeq R^k/\ker\varphi$. El submódulo $\ker\varphi$ es el **submódulo de relaciones** de M. Como R es en particular un dominio de ideales principales y M es finitamente generado, $\ker\varphi$ es también finitamente generado. Sea $\{e_1,\dots,e_l\}$ un conjunto de generadores de $\ker\varphi$, digamos

$$\begin{aligned} e_1 &= (a_{11},a_{12},\dots,a_{1k}),\\ e_2 &= (a_{21},a_{22},\dots,a_{2k}),\\ &\vdots\\ e_l &= (a_{l1},a_{l2},\dots,a_{lk}). \end{aligned}$$

La matriz $A=(a_{ij})_{1\le i\le l,1\le j\le k}$ es la **matriz de relaciones** de M con respecto a los conjuntos $\{m_1,\dots,m_k\}$ y $\{e_1,\dots,e_l\}$. Veamos algunas propiedades de la matriz de relaciones.

1) Si $P\in R^{l\times l}$ es inversible, entonces las filas $\{f_1,\dots,f_l\}$ de la matriz PA generan $\ker\varphi$. Además PA es la matriz de relaciones con respecto a $\{m_1,\dots,m_k\}$ y $\{f_1,\dots,f_l\}$.
2) Si $Q\in R^{k\times k}$ es inversible con $Q^{-1}=(q_{ij})$ y para cada $j\in\{1,\dots,k\}$ se define $n_j=\sum_{i=1}^k q_{ij}\cdot m_i$, el conjunto $\{n_1,\dots,n_k\}$ genera a M y las filas de la matriz AQ generan $\ker\varphi$. Además AQ es la matriz de relaciones respecto de $\{n_1\dots,n_k\}$.

Para demostrar la primera afirmación supongamos que $P=(p_{ij})$. Las filas de la matriz PA son entonces $f_1,\dots,f_l$, donde

$$\begin{aligned} f_1 &= p_{11}e_1+\cdots+p_{1l}e_l,\\ f_2 &= p_{21}e_1+\cdots+p_{2l}e_l,\\ &\vdots\\ f_l &= p_{l1}e_1+\cdots+p_{ll}e_l. \end{aligned}$$

Además $f_j\in\ker\varphi$ para todo $j\in\{1,\dots,l\}$. Como P es inversible, $\{f_1,\dots,f_l\}$ es un conjunto de generadores de $\ker\varphi$, pues cada e_j es combinación lineal de los f_i,

$$\begin{pmatrix} e_1\\ e_2\\ \vdots\\ e_l \end{pmatrix} = P^{-1}\begin{pmatrix} f_1\\ f_2\\ \vdots\\ f_l \end{pmatrix}.$$

En particular, PA es la matriz de relaciones respecto de $\{m_1,\dots,m_k\}$ y $\{f_1,\dots,f_l\}$.

Demostremos ahora la segunda afirmación. Como

$$\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} = Q^{-1} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix},$$

entonces

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = (AQ) \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix},$$

lo que nos dice que las filas de la matriz AQ son relaciones respecto del conjunto de generadores $\{n_1,\dots,n_k\}$. Sea $\psi\colon R^k \to M$, $(r_1,\dots,r_k) \mapsto \sum_{i=1}^k r_i \cdot n_i$. Veamos que las filas de AQ generan el módulo de relaciones $\ker\psi$ respecto de $\{n_1,\dots,n_k\}$. Si $(r_1,\dots,r_k) \in \ker\psi$, entonces $\sum_{i=1}^k r_i \cdot n_i = 0$. Si escribimos esta fórmula matricialmente,

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (r_1 \cdots r_k) Q^{-1} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix},$$

donde conviene recordar que cada e_j es un elemento de R^k, entonces

$$(r_1 \cdots r_k) Q^{-1} = \left(\sum_{i=1}^k r_i \cdot q_{i1}, \sum_{i=1}^k r_i \cdot q_{2i}, \dots, \sum_{i=1}^k r_i \cdot q_{ki} \right) \in \ker\varphi.$$

Como $\ker\varphi$ está generado por el conjunto $\{e_1,\dots,e_l\}$, existen $s_1,\dots,s_l \in R$ tales que $(r_1 \cdots r_k)Q^{-1} = \sum_{i=1}^l s_i \cdot e_i$, es decir

$$(r_1 \dots r_k) Q^{-1} = (s_1 \cdots s_l) \begin{pmatrix} e_1 \\ \vdots \\ e_l \end{pmatrix} = (s_1 \cdots s_l) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lk} \end{pmatrix}.$$

Si reescribimos esta fórmula como

$$(r_1 \cdots r_k) = (s_1 \cdots s_l) AQ,$$

obtenemos entonces que $(r_1,\dots,r_k)$ es combinación lineal de las filas de AQ, pues

$$(r_1,\dots,r_k)=\left(\sum_{i=1}^{l}s_i\cdot x_{i1},\dots,\sum_{i=1}^{l}s_i\cdot x_{ik}\right)=\sum_{i=1}^{l}s_i\cdot(x_{11},\dots,x_{1k}).$$

En conclusión, $\{n_1,\dots,n_k\}$ es un conjunto de generadores de M y las filas de AQ generan el correspondiente submódulo de relaciones y AQ es la matriz de relaciones respecto de $\{n_1,\dots,n_k\}$ y $\{e_1,\dots,e_l\}$.

Proposición 30.23. *Sea A la matriz de relaciones de un módulo M. Si existen matrices inversibles $P\in R^{l\times l}$ y $Q\in R^{k\times k}$ tales que*

$$PAQ=\begin{pmatrix} a_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0\\ 0 & a_2 & \cdots & \cdot & \cdot & \cdots & 0\\ \vdots & & \ddots & & & & \vdots\\ 0 & \cdot & \cdots & a_r & \cdot & \cdots & 0\\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0\\ \vdots & & & & & \ddots & \vdots\\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{pmatrix}$$

donde $a_i\neq 0$ para todo $i\in\{1,\dots,r\}$ y $a_i \mid a_{i+1}$ para todo $i\in\{1,\dots,r-1\}$, entonces

$$M\simeq R/(a_1)\oplus\cdots\oplus R/(a_r)\oplus R^{n-r}.$$

Demostración. Sabemos que PAQ es la matriz de relaciones con respecto a un cierto conjunto de generadores $\{m_1,\dots,m_k\}$ de M y respecto al submódulo de relaciones generado por las filas de PAQ. Si $\varphi\colon R^k\to M$, $(r_1,\dots,r_k)\mapsto\sum_{i=1}^{k}r_i\cdot m_i$, entonces $R^k/\ker\varphi\simeq M$, pues φ es un epimorfismo. Para $j\in\{r+1,\dots,k\}$ sea $a_j=0$. Sea $\psi\colon R^k\to R/(a_1)\oplus\cdots\oplus R/(a_k),(s_1,\dots,s_k)\mapsto(s_1+(a_1),\dots,s_k+(a_k))$.

Un cálculo sencillo muestra que

$$\ker\psi=(a_1)\oplus\cdots\oplus(a_k)$$

y luego $R^k/\ker\psi\simeq\oplus_{i=1}^{k}R/(a_i)$.

Dejamos como ejercicio demostrar que $\ker\varphi=\ker\psi$.

En conclusión, tenemos que $M\simeq R/(a_1)\oplus\cdots\oplus R/(a_k)$. Para completar la demostración hay que observar que $R/(a_i)\simeq R$ para todo $i\in\{r+1,\dots,k\}$. □

Veamos cómo encontrar las matrices P y Q. La descomposición se conoce como la **forma normal de Smith**. Para simplificar la presentación supondremos que R es un domino euclidiano con norma φ. Transformaremos nuestra matriz mediante las siguientes operaciones:

1) Intercambiar las filas i-ésima y la j-ésima, es decir $F_i\leftrightarrow F_j$.
2) Reemplazar la fila F_i por $F_i+\lambda F_j$ para algún $\lambda\in R$ y $j\neq i$.
3) Intercambiar las columnas i-ésima y la j-ésima, es decir $C_i\leftrightarrow C_j$.
4) Reemplazar la columna C_i por $C_i+\lambda C_j$ para algún $\lambda\in R$ y $j\neq i$.

Todas estas operaciones son inversibles. Por ejemplo, la operación (1) corresponde a multiplicar a izquierda a la matriz A por una matriz de permutación. La operación (2) corresponde a multiplicar a izquierda a la matriz A por $I+\lambda E_{ij}$, donde

$$(E_{ij})_{kl} = \begin{cases} 1 & \text{si } i=k \text{ y } j=l, \\ 0 & \text{en otro caso.} \end{cases}$$

Similarmente, las operaciones de columnas se corresponden con multiplicar a derecha por matriz de permutación o matrices de la forma $I+\lambda E_{ij}$.

Teorema 30.24 (forma normal de Smith). *Sea (R,φ) un dominio euclidiano. Si $A \in R^{l\times k}$, existen matrices inversibles $P \in R^{l\times l}$ y $Q \in R^{k\times k}$ tales que*

$$PAQ = \begin{pmatrix} a_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & a_2 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & a_r & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{pmatrix}$$

con $a_1 \cdots a_k \neq 0$ y $a_i \mid a_{i+1}$ para todo $i \in \{1,\dots,r-1\}$.

Bosquejo de la demostración. Vamos a demostrar que podemos transformar a la matriz A en una matriz de la forma

$$B = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix}$$

tal que cada b_{ij} es divisible por b_{11}. Repetimos el mismo procedimiento en la submatriz

$$\begin{pmatrix} \frac{b_{22}}{b_{11}} & \cdots & \frac{b_{2m}}{b_{11}} \\ \vdots & & \vdots \\ \frac{b_{n2}}{b_{11}} & \cdots & \frac{b_{nm}}{b_{11}} \end{pmatrix}$$

e iteramos el algoritmo hasta que no podamos continuar.

Veamos cómo conseguir la matriz B. Al aplicar operaciones de fila y columna podemos suponer que el elemento de la matriz A de menor norma está en la posición $(1,1)$. Si algún a_{i1} no es divisible por a_{11}, escribimos $a_{i1} = a_{11}u + r$ para $u \in R$ y $r \in R$ tal que $\varphi(r) < \varphi(a_{11})$. Aplicamos entonces la transformación $F_i \leftarrow F_i - uF_1$ y nos queda una matriz que en el lugar $(1,i)$ tendrá al elemento r. Similarmente, si algún a_{1j} no es divisible por a_{11}, entonces $a_{1j} = va_{11} + s$ con $\varphi(s) < \varphi(a_{11})$ y aplicamos la transformación $C_j \leftarrow C_j - vC_1$ para quedarnos con una matriz que en

el lugar $(j,1)$ tiene al elemento s. Si todos los a_{i1} son divisibles por a_{11}, digamos $a_{i1} = a_{11}\lambda_i$, entonces aplicamos la transformación $F_i \leftarrow \lambda_i F_1 - F_i$. Similarmente, si todos los a_{1j} son divisibles por a_{11}, digamos $a_{1j} = a_{11}\mu_j$, entonces aplicamos la transformación $C_j \leftarrow \mu_j C_1 - C_j$. Esto nos permite quedarnos con una matriz de la forma

$$\begin{pmatrix} a_{11} & 0 \\ 0 & A_1 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}.$$

Si alguna de las entradas de la submatriz A_1 no fuera divisible por a_{11}, hacemos la operación $F_1 \leftarrow F_1 + F_i$ o bien la operación $C_1 \leftarrow C_1 + C_j$ y repetimos el procedimiento. □

Veamos algunos ejemplos.

Ejemplo 30.25. Sea

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 8 & 6 & 4 \\ 3 & 1 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

Vamos a encontrar la forma normal de Smith de la matriz A. Como el elemento de menor norma se encuentra en la posición $(3,2)$, hacemos las operaciones $F_1 \leftrightarrow F_3$ y $C_1 \leftrightarrow C_2$ y nos queda la matriz

$$\begin{pmatrix} 1 & 3 & 0 \\ 6 & 8 & 4 \\ 5 & 2 & 3 \end{pmatrix}.$$

Para obtener ceros en las posiciones $(1,2)$, $(1,3)$, $(2,1)$ y $(2,3)$ hacemos las operaciones $F_2 \leftrightarrow 6F_1 - F_2$, $F_3 \leftrightarrow 5F_1 - F_3$ y luego $C_1 \leftrightarrow 3C_1 - C_2$. Nos queda entonces la matriz

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & -10 & -4 \\ 0 & -13 & -3 \end{pmatrix}.$$

Para sacarnos de encima los números negativos multiplicamos la segunda y la tercera fila por -1, que es una unidad de $\mathbb{Z}$:

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 10 & 4 \\ 0 & 13 & 3 \end{pmatrix}.$$

Ahora hacemos lo mismo en la submatriz $\begin{pmatrix} 10 & 4 \\ 13 & 3 \end{pmatrix}$. Para que en el lugar $(2,2)$ nos quede el elemento de la submatriz que tiene menor norma, aplicamos las transformaciones $F_2 \leftrightarrow F_3$ y $C_3 \leftrightarrow C_2$. Nos queda entonces

$$\begin{pmatrix} 3 & 13 \\ 4 & 10 \end{pmatrix}.$$

Escribimos $13 = 3 \cdot 4 + 1$ y aplicamos la transformación $C_2 \leftarrow C_2 - 4C_1$ para obtener $\begin{pmatrix} 3 & 1 \\ 4 & -6 \end{pmatrix}$. Intercambiamos la primera y la segunda columna y nos queda la matriz $\begin{pmatrix} 1 & 3 \\ -6 & 4 \end{pmatrix}$. Aplicamos ahora la transformación $F_2 \leftarrow 6F_1 + F_2$ y al resultado le aplicamos la transformación $C_2 \leftarrow 3C_1 - C_2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 22 \end{pmatrix}.$$

Luego

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -22 \end{pmatrix}$$

es la forma normal de Smith de la matriz A.

Veamos ahora algunas aplicaciones.

Ejemplo 30.26. Sea M el grupo abeliano con generadores m_1, m_2, m_3 y relaciones $8m_1 + 4m_2 + 8m_3 = 0$, $4m_1 + 8m_2 + 4m_3 = 0$. La matriz de relaciones es entonces

$$A = \begin{pmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \end{pmatrix}.$$

Veamos que $M \simeq \mathbb{Z}/4 \times \mathbb{Z}/12$. Si hacemos la operación $F_1 \leftarrow 2F_2 - F_1$, nos queda la matriz

$$\begin{pmatrix} 0 & 12 & 0 \\ 4 & 8 & 4 \end{pmatrix},$$

que corresponde a los generadores $\{m_1, m_2, m_3\}$ con las relaciones $12m_2 = 0$ y $4m_1 + 8m_2 + 4m_3 = 0$. Si hacemos simultáneamente las operaciones $C_2 \leftarrow C_2 - 2C_1$ y $C_3 \leftarrow C_3 - C_1$, nos queda la matrix

$$\begin{pmatrix} 0 & 12 & 0 \\ 4 & 0 & 0 \end{pmatrix},$$

que corresponde al conjunto de generadores $\{m_1 + 2m_2 + m_3, m_2\}$ con las relaciones $12m_2 = 0$ y $4(m_1 + 2m_2 + m_3) = 0$. Por último, al intercambiar la primera y la segunda columna, nos queda la matriz

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix},$$

que corresponde al conjunto de generadores $\{m_2, m_1 + 2m_2 + m_3\}$ con las relaciones $4(m_1 + 2m_2 + m_3) = 0$ y $12m_2 = 0$. En conclusión, $M \simeq \mathbb{Z}/4 \times \mathbb{Z}/12$.

Ejemplo 30.27. Sea M el grupo abeliano generdo por $\{m_1, \ldots, m_4\}$ y sea K el subgrupo generado por $\{e_1, e_2, e_3\}$, donde

$$e_1 = 22m_3, \quad e_2 = -2m_1 + 2m_2 - 6m_3 - 4m_4, \quad e_3 = 2m_1 + 2m_2 + 6m_3 + 8m_4.$$

Queremos calcular M/K. La matriz de relaciones es

$$A = \begin{pmatrix} 0 & 0 & 22 & 0 \\ -2 & 2 & -6 & -4 \\ 2 & 2 & 6 & 8 \end{pmatrix}.$$

Si aplicamos la operación $F_1 \leftrightarrow F_3$ y después la operación $F_2 \leftarrow F_1 + F_2$ nos da la matriz

$$\begin{pmatrix} 2 & 2 & 6 & 8 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}.$$

Ahora aplicamos las operaciones $C_2 \leftarrow C_2 - C_1$, $C_3 \leftarrow C_3 - 3C_1$ y $C_4 \leftarrow C_4 - 4C_1$ y obtenemos

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}.$$

Hacemos ahora $C_4 \leftarrow C_4 - C_2$ y nos queda la matriz

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

pero ahora nos encontramos con que $4 \nmid 22$. Utilizamos las operaciones $F_2 \leftarrow F_2 + F_3$, $C_3 \leftarrow C_3 - 5C_2$, $C_3 \leftarrow C_2$, $F_3 \leftarrow F_3 - 11F_2$ y $C_3 \leftarrow C_3 - C_2$ y nos queda

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -44 & 0 \end{pmatrix}.$$

Luego el grupo abeliano M/K puede presentarse con la base $\{n_1, n_2, n_3, n_4\}$ y las relaciones $2n_1 = 0$, $2n_2 = 0$ y $44n_3 = 0$. En conclusión, $M/K \simeq \mathbb{Z} \times (\mathbb{Z}/2)^2 \times (\mathbb{Z}/44)$.

Capítulo 31
Algunas soluciones

Morfismos

7.37 Si existe $x \in G$ tal que $|x| = 9$, entonces $G \simeq \mathbb{Z}/9$. Supongamos entonces que no hay elementos de orden nueve. Por el teorema de Lagrange, todo elemento no trivial tiene orden 3. Sea $x \in G$ tal que $|x| = 3$ y sea $y \in G \setminus \langle x \rangle$. Entonces

$$G = \langle x, y \rangle = \{1, x, y, x^2, y^2, x^2y, xy^2, x^2y^2, xy\}.$$

Si $yx = xy$, entonces $G \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$. Si $yx = x^2y^2$, entonces $(xy)^2 = 1$, una contradicción. Si $yx = x^2y$, entonces, como yx^2 tiene orden tres, tenemos

$$1 = (yx^2)^3 = yx^2yx^2yx^2 = y(yx)x^2yx^2 = x^2,$$

una contradicción. De la misma forma vemos que $yx \neq xy^2$.

7.58 Observemos que la conmutatividad del diagrama es $\pi_V \circ f = g \circ \pi_U$. Por el ejercicio 7.52 sabemos que existe g si y sólo si

$$U \subseteq \ker(\pi_V \circ f) \iff f(U) \subseteq \ker(\pi_V) = V.$$

Queremos demostrar (1). Si $h \in H$ y $hV \in H/V$, queremos ver que $g(xU) = hV$ para algún $x \in G$. Como f es sobreyectiva, $f(x) = h$ para algún $x \in G$. Luego

$$g(xU) = g(\pi_U(x)) = \pi_V(f(x)) = \pi_V(h) = hV.$$

Veamos ahora (2). Sea $x \in G$ tal que $g(xU) = V$. Como

$$\pi_V(f(x)) = g(\pi_U(x)) = g(xU) = V,$$

se tiene que $f(x) \in \ker(\pi_V) = V$, es decir $x \in f^{-1}(V) = U$. Luego $\ker g$ es trivial y entonces g es inyectiva.

7.59 Sean $H = G/S$, $U = T$, $V = T/S$ y $f = \pi_S \colon G \to G/S$ el morfismo canónico. El ejercicio 7.58 nos dice que la existencia de un morfismo

$$g \colon G/T \to \frac{G/S}{T/S}$$

tal que $g \circ \pi_T = \pi_{T/S} \circ f$ es equivalente a pedir que $\pi_S(T) \subseteq T/S$, algo trivial. Como π_S es sobreyectiva, g es también sobreyectiva. Además g es inyectiva pues $\pi_S^{-1}(T/S) = T$.

Grupos de automorfismos

9.16 Como la identidad es siempre un automorfismo, es necesario encontrar otro automorfismo de G. Supongamos primero que G es no abeliano. Sea $g \in G \setminus Z(G)$ y sea γ_g la conjugación por g, es decir $x \mapsto gxg^{-1}$. Como g no es central, entonces γ_g es un automorfismo no trivial de G y luego $|\operatorname{Aut}(G)| \geq 2$.

Supongamos ahora que G es abeliano. Si existe $g \in G$ tal que $g^2 \neq 1$, entonces la función $x \mapsto x^{-1}$ es un automorfismo no trivial de G y luego $|\operatorname{Aut}(G)| \geq 2$. Supongamos entonces que $g^2 = 1$ para todo $g \in G$. En este caso, G es un espacio vectorial sobre $\mathbb{Z}/2$. Como $|G| > 2$, entonces $\dim_{\mathbb{Z}/p} G > 1$. Sea $\{x_i : i \in I\}$ una base de G. Como esta base tiene al menos dos elementos, sean $i, j \in I$ elementos distintos. Sea $f \colon G \to G$ la transformación lineal dada por

$$f(x_k) = \begin{cases} x_j & \text{si } k = i, \\ x_i & \text{si } k = j, \\ x_k & \text{en otro caso.} \end{cases}$$

Como f es una transformación lineal inversible, f es un automorfismo de G no trivial. Luego $|\operatorname{Aut}(G)| \geq 2$.

Ideales

17.6 Si $J \not\subseteq P$ y $J \not\subseteq Q$ entonces sean $x \in J \setminus P$, $y \in J \setminus Q$. Como $J \subseteq P \cup Q$ entonces $x \in Q$ y además $y \in P$. Como J es un ideal, $x + y \in J$. Como $y \in P$ y $x \notin P$ entonces $x + y \notin P$. Similarmente $x + y \notin Q$. Luego $x + y \in J \setminus P \cup Q$.

17.12 Si $f \in \operatorname{Hom}(\mathbb{Z}[\sqrt{d}], R)$, definimos $\varphi(f) = r$ donde r es tal que $r^2 = f(d)$. La función φ está bien definida pues, como

$$f(a + b\sqrt{d}) = f(a) + f(b)f(\sqrt{d}) = a1_R + b1_R f(\sqrt{d}),$$

f queda unívocamente determinado por $r = f(\sqrt{d}) \in R$ que cumple $r^2 = f(d)$. La función φ es inyectiva. Además φ es sobreyectiva, pues si $r \in R$ es tal que $r^2 = d1_R$, entonces $f(a+b\sqrt{d}) = a1_R + b1_R r$ es un morfismo de anillos $\mathbb{Z}[\sqrt{d}] \to R$. Luego $\mathrm{Hom}(\mathbb{Z}[\sqrt{d}, R)$ está en biyección con el conjunto $\{r \in R : r^2 = d1_R\}$.

17.16 Si $f\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ es un isomorfismo de anillos,

$$f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2.$$

Si $\alpha = f(\sqrt{2})$, entonces $2 = f(2) = f(\sqrt{2})^2 = \alpha^2$. Veamos que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. En efecto, si $\sqrt{2} = (a/b) + (c/d)\sqrt{2}$, entonces $\sqrt{6} \in \mathbb{Q}$, una contradicción.

17.17 Si $f\colon \mathbb{Z}/6 \to \mathbb{Z}/15$, entonces $f(1) = 1$. Por otro lado,

$$0 = f(0) = f(6) = f(1+5) = f(1) + f(5) = f(1) + 5f(1) = 6f(1).$$

Luego $f(1) \in \{0, 5, 10\}$, una contradicción.

El lema de Zorn

22.16 Sea $x \in J(R)$ y supongamos que $1 - xy$ no es una unidad de R. Entonces $1 - xy$ pertenece a algún ideal maximal M y luego $1 \in M$, una contradicción. Recíprocamente, si existe un ideal maximal M tal que $x \notin M$ entonces $R = (x, M)$ pues M es maximal. Luego $1 = xy + m$ para algún $y \in R$ y algún $m \in M$. Esto implica que $1 - xy = m \in M$ y por lo tanto $1 - xy \notin \mathscr{U}(R)$.

22.17 Sea $f\colon \mathbb{Z} \to \mathbb{Z}/n$, $k \mapsto k$ mód n. Por el teorema de la correspondencia, los ideales maximales de $\mathbb{Z}/n$ están en biyección con los ideales maximales de $\mathbb{Z}$ que contienen a $\ker f = n\mathbb{Z}$. Los ideales maximales de $\mathbb{Z}$ son de la forma $p\mathbb{Z}$ para algún primo p. Como $n\mathbb{Z} \subseteq p\mathbb{Z}$ si y sólo si p divide a n, se concluye que (p) es un ideal maximal de $\mathbb{Z}/n$ si y sólo si p es un primo que divide a n.

Módulos

24.37 Supongamos primero que $f\colon R/M_1 \to R/M_2$ es un isomorfismo de módulos. Entonces existe $r \in R \setminus M_2$ tal que $f(1 + M_1) = r + M_2$. Probemos que $rM_1 \subseteq M_2$. En efecto, si $m_1 \in M_1$ entonces

$$M_2 = f(M_1) = f(m_1 + M_1) = m_1 \cdot f(1 + M_1) = m_1 \cdot (r + M_2) = rm_1 + M_2.$$

Supongamos ahora que existe $r \in R \setminus M_2$ tal que $rM_1 \subseteq M_2$. Como M_2 es maximal, R/M_2 es un cuerpo. Sea $\pi\colon R \to R/M_2$ el morfismo canónico. Vamos a demostrar que $M_1 = M_2$. Si $x \in M_1$, entonces, como $rx \in rM_1 \subseteq M_2$, en el cuerpo R/M_2 se tiene

$$0 = \pi(rx) = \pi(r)\pi(x)$$

Hay entonces dos posibiblidades: $\pi(r) = 0$ o bien $\pi(x) = 0$. Como $r \notin M_2 = \ker \pi$, entonces $\pi(x) = 0$, es decir $x \in \ker \pi = M_1$. Luego $M_1 \subseteq M_2$, que por la maximalidad del ideal M_1 implica $M_1 = M_2$.

Sucesiones exactas

26.10 Supongamos que vale (1) y sea $m'' \in M''$ tal que $am'' = 0$. Como g es epimorfismo, existe $m \in M$ tal que $g(m) = m''$. Luego $g(am) = am'' = 0$ y $am \in \ker(g) = f(M')$. Existe entonces $m' \in M'$ tal que $am = f(m')$. Por hipótesis, existe $m'_1 \in M'$ tal que $am = f(am'_1)$ y luego $a(m - f(m'_1)) = 0$. El elemento de M que buscamos es $m - f(m'_1)$ pues $g(m - f(m'_1)) = g(m) = m''$.

Recíprocamente, supongamos que vale (2). Sea $m' \in M'$ tal que existe $m \in M$ con $f(m') = am$. Si aplicamos g obtenemos $0 = gf(m') = ag(m)$. Si usamos (2) con $g(m) \in M''$ entonces existe $m_1 \in M$ tal que $am_1 = 0$ y $g(m) = g(m_1)$. Como $\ker(g) = f(M')$, existe $m'_1 \in M'$ tal que $m - m_1 = f(m'_1)$. Esto implica que $f(m') = am = am - am_1 = af(m'_1) = f(am'_1)$. Como f es monomorfismo, $m' = am'_1$.

26.11 Si $m \in M$, $m - s(g(m)) \in \ker g = \operatorname{im} f$ pues $g(m - s(g(m))) = 0$. Como f es inyectiva, dado $m \in M$ se tiene que $m - s(g(m)) = f(x)$ para un único $x \in X$. Definimos entonces $r\colon M \to X$, $m \mapsto x$, y entonces $m - s(g(m)) = f(r(m))$ para todo $m \in M$.

Supongamos que existen r y s tales que $f \circ r + s \circ g = \mathrm{id}_M$. Si $y \in Y$, entonces $y = g(m)$ para algún $m \in M$ pues g es epimorfismo. Como $m = f(r(m)) + s(y)$, entonces

$$g(s(y)) = g(m - f(r(m))) = g(m) - g(f(r(m))) = y$$

pues $\ker g = f(X)$. 9

Módulos finitamente generados

27.11 Probemos la primera afirmación. Si $M_1 \subseteq M$ es un submódulo, entonces M_1 es finitamente generado porque $M_1 \simeq f(M_1) \subseteq M$ y M es noetheriano. Si $T_1 \subseteq T$ es un submódulo, entonces T_1 es finitamente generado por ser isomorfo a un submódulo de M que contiene a $\ker(g)$ y M es noetheriano.

Probemos la segunda afirmación. Si $K \subseteq M$ es un submódulo, consideremos la sucesión exacta

$$0 \longrightarrow f^{-1}(K) \xrightarrow{f} K \xrightarrow{g} g(K) \longrightarrow 0$$

Como S y T son noetherianos, $f^{-1}(K)$ y $g(K)$ son finitamente generados. Luego K también es finitamente generado.

Módulos libres

Módulos proyectivos

29.7 Como M/N es un módulo libre, el módulo M/S es proyectivo. Existe entonces un morfismo $s\colon M/N \to N$ tal que $\pi \circ s = \mathrm{id}_{M/N}$. En particular, $M \simeq N \oplus M/N$.

29.12 Si existe un ideal J de R tal que $R = I \oplus J$, entonces $1 = u + v$ para ciertos $u \in I$ y $v \in V$. Veamos que $I = (u)$. Si $x \in I$, entonces $x = x1 = xu + xv$. Como $xv \in I \cap J = \{0\}$, se concluye que $x = xu \in (u)$. Además

$$1 = 1 \cdot 1 = (u+v)^2 = u^2 + 2uv + v^2 = u^2 + v^2,$$

pues $uv \in I \cap J = \{0\}$. Luego $(u) = (u^2)$, pues $u = u1 = u(u^2 + v^2) = u^3 \in (u^2)$.

Supongamos ahora que existe $u \in R$ tal que $I = (u) = (u^2)$. Entonces $u = ru^2$ para algún $r \in R$. En particular, $ru = r^2u^2$. Si $e = ru$, entonces e es idempotente, pues

$$e^2 = (ru)^2 = r^2u^2 = ru = e.$$

Veamos que $I = (u) = (e)$. Basta con demostrar que $(u) \subseteq (e)$. Si $\lambda \in R$, entonces

$$\lambda u = \lambda(ru^2) = (\lambda u)(ru) = (\lambda u)e \in (e).$$

Si $J = (1-e)$, entonces $R = I \oplus J$, pues ya vimos que $I \cap J = \{0\}$ y $R = I + J$.

29.13 Si ${}_RR$ es semisimple e I es un ideal de R, sabemos que existe un submódulo J (es decir, J es ideal a izquierda de R) tal que $R = I \oplus J$. En particular, existen $e \in I$ y $f \in J$ tales que $1 = e + f$. Como $ef \in I \cap J = \{0\}$, entonces

$$e = e1 = e^2 + ef = e^2.$$

Veamos que $I = Re$. Si $x \in I$, entonces

$$x = x1 = xe + xf = xe \in Re,$$

pues $xf = x - xe \in I \cap J = \{0\}$.

Si $I = Re$ para algún idempotente $e \in R$, entonces $J = R(1-e)$ es tal que $R = I \oplus J$. En efecto, $R = I + J$, pues $r = re + r(1-e)$. Además $I \cap J = \{0\}$ pues si $r = xe = y(1-e)$, entonces

$$r = xe = xe^2 = y(1-e)e = 0.$$

29.21 Como P es proyectivo existe un morfismo $\beta\colon P \to P'$ tal que $g' \circ \beta = g$. Luego $g' \circ \beta \circ F = g \circ f = 0$ y entonces existe un morfismo $\alpha\colon K \to K'$ tal que $\beta \circ f = f' \circ \alpha$.

Sea $\phi\colon K \to K' \oplus P$ el morfismo dado por $\phi(k) = (\alpha(k), f(k))$ y $\psi\colon K' \oplus P \to P'$ el morfismo dado por $\psi(k', p) = f'(k') - \beta(p)$. La sucesión

$$0 \longrightarrow K \xrightarrow{\phi} K' \oplus P \xrightarrow{\psi} P' \longrightarrow 0$$

es exacta y se parte porque P' es proyectivo.

El teorema de estructura

30.4 Como M es libre, al usar el morfismo canónico $\varphi\colon M \to M/S$, tenemos que $M \simeq S \oplus (M/S)$.

30.5 Sea $K = K(R)$ el cuerpo de fracciones de R. Como M es libre de rango n, entonces $M \simeq R^n$. Como R^n es un subgrupo de K^n, vemos que $\{v_1, \ldots, v_n\}$ es linealmente independiente sobre K si y sólo si $\{v_1, \ldots, v_n\}$ es linealmente independiente sobre R.

30.7 Sea $\{m_1, \ldots, m_n\}$ una base de M. Como M es libre, existe un morfismo $\varphi\colon M \to M$ tal que $m_j \mapsto s_j$ para todo $j \in \{1, \ldots, n\}$. Como M es libre, M es proyectivo y entonces $M \simeq \ker\varphi \oplus M$. Como R es principal, el submódulo $\ker\varphi$ es libre de rango $\leq n$. Como además $\operatorname{rank}(M) = \operatorname{rank}(\ker\varphi) + \operatorname{rank}(M)$, se concluye que $\operatorname{rank}(\ker\varphi) = 0$ y luego $\ker\phi = \{0\}$, es decir que φ es un isomorfismo. En particular, $\{s_1, \ldots, s_n\}$ es una base de M.

30.11 Como M/S es finitamente generado y sin torsión, es libre y por tanto proyectivo. La sucesión exacta $0 \to S \to M \to M/S \to 0$ se parte y entonces $M \simeq S \oplus M/S$. Luego M es proyectivo por ser suma de proyectivos. Como R es un dominio de ideales principales, se concluye que M es libre.

Referencias

1. O. A. Cámpoli. A principal ideal domain that is not a Euclidean domain. *Amer. Math. Monthly*, 95(9):868–871, 1988.
2. R. D. Carmichael. *Introduction to the theory of groups of finite order*. Dover Publications, Inc., New York, 1956.
3. R. M. Guralnick. Commutators and commutator subgroups. *Adv. in Math.*, 45(3):319–330, 1982.
4. P. J. Hilton and U. Stammbach. *A course in homological algebra*, volume 4 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
5. S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.
6. J. C. Wilson. A principal ideal ring that is not a Euclidean ring. *Math. Mag.*, 46:34–38, 1973.
7. R. A. Wilson. 101.15 An elementary proof that not all principal ideal domains are Euclidean domains. *Math. Gaz.*, 101(551):289–293, 2017.

Índice alfabético