Leandro Vendramin

Álgebra II

– Notas –

12 de septiembre de 2020

Índice general

Parte I
Grupos

Capítulo 1
Grupos y subgrupos

grupos

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 en virtud de esta propiedad, 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.

Notación 1.7. 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 1.8. 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 $k \in \mathbb{Z}$.

Ejercicio 1.9. 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 1.10. 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.

Ejemplo 1.11. 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 1.12. 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 1.13. 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 1.14 (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 $\mathbb{S}_4$.

Ejemplo 1.15. 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 $3 \mapsto 3$.

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

Ejemplo 1.16. 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: $\mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\}$. La tabla de multiplicación de este grupo 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

Ejemplo 1.17. 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 1.18. 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 1.19. Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G.

Ejemplo 1.20. $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Ejemplo 1.21. $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Ejemplo 1.22. 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 1.23. 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 1.24. 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 1.25. Demuestre que $Z(\mathbb{S}_3) = \{\mathrm{id}\}$ y calcule $C_{\mathbb{S}_3}((12))$.

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

Ejercicio 1.26. 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 1.27. $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$. 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 $\det(ab^{-1}) = \det(a)\det(b)^{-1} = 1$.

Ejercicio 1.28. 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 1.29. *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 $m = \min\{s \in S : s > 0\}$. 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 interesantes:

Ejemplo 1.30. 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 $d = \text{mcd}(a,b)$.

Ejercicio 1.31. 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 $d = ar + bs$.

Observemos que dos enteros a y b serán **coprimos** si y sólo si $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Ejemplo 1.32. Si S y T son subgrupos de $\mathbb{Z}$, entonces $S \cap T$ es también un subgrupo de $\mathbb{Z}$. Sabemos que $S = a\mathbb{Z}$ para algún $a \in \mathbb{N}$ y $T = b\mathbb{Z}$ para algún $b \in \mathbb{N}$. Además $S \cap T = m\mathbb{Z}$ para algún $m \in \mathbb{N}$ porque $S \cap T$ es también un subgrupo de $\mathbb{Z}$. Ese entero positivo m es el **mínimo común múltiplo** de a y b, es decir $m = \text{mcm}(a,b)$.

Ejercicio 1.33. Sean $a,b \in \mathbb{Z} \setminus \{0\}$ y sea $m = \text{mcm}(a,b)$. 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.

Ejercicio 1.34. Sean $a,b \in \mathbb{N}$, $d = \text{mcd}(a,b)$ y $m = \text{mcm}(a,b)$. Entonces $ab = dm$.

Ejercicio 1.35. 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 1.36. 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 $X = \{g_1,\ldots,g_k\}$, entonces $\langle X \rangle = \langle \{g_1,\ldots,g_k\} \rangle = \langle g_1,\ldots,g_k \rangle$.

Ejercicio 1.37. Demuestre que $\langle X \rangle$ será 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 1.38. Demuestre que

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

Un ejemplo importante de un grupo generado por dos elementos es el grupo diedral.

Ejemplo 1.39. El conjunto

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

es un subgrupo no abeliano de $\mathbb{S}_4$.

Ejemplo 1.40. 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 1.41. 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 conmutador de un grupo G a veces se conoce como el **subgrupo derivado** de G. Más adelante se justificará esta terminología.

Ejemplo 1.42. $[\mathbb{Z},\mathbb{Z}] = \{0\}$ pues $\mathbb{Z}$ es un grupo abeliano. Obviamente, en este ejemplo utilizamos la notación aditiva.

Ejercicio 1.43. 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. El primer ejemplo aparece en el libro de Carmichael [1].

Ejemplo 1.44. Sea G el subgrupo de $\mathbb{S}_{16}$ generado por las permutaciones

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

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

Mencionamos otro ejemplo, encontrado por Guralnick [2] antes de que el uso de computadoras en teoría de grupos fuera masivo.

Ejemplo 1.45. 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 $\{1, g, \ldots, g^{d-1}\} \subseteq \langle g \rangle$

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.

xca:orden2 **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.

Ejercicio 2.18. Calcule el orden de la matrix $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

Ejercicio 2.19. 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 $2n$.

Capítulo 3
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 3.1. 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 3.2. 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 3.3. Las permutaciones disjuntas conmutan.

Observación 3.4. 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 3.5. *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 3.6. *Toda $\sigma \in \mathbb{S}_n \setminus \{id\}$ 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 $\sigma(i_1) \neq i_1$. 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 $\sigma = \sigma_1\sigma_2\cdots\sigma_r$, 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 $\sigma_1 = \tau_1$ 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 3.7.

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

$$E_{i,j}E_{k,l} = \begin{cases} E_{i,l} & \text{si } j = k, \\ 0 & \text{si } j \neq k. \end{cases} \tag{3.1}$$

eq:E

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

Demostración. Es un cálculo directa que utiliza la fórmula (3.1). 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 3.9. 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 3.10. 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 3.11. *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 3.12. 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 3.13. $|\mathbb{A}_n| = n!/2$.

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, $\tau \in \mathbb{A}_n\sigma$. 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 3.14. 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.

pro:A_n3ciclos

Proposición 3.15. $\mathbb{A}_n = \langle \{3\text{-}ciclos\} \rangle$.

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 3.16. 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 3.17. 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 4
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:

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

Ejercicio 4.1. Demuestre que hemos definido 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.

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 4.2. *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 4.3. 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 4.4. Los subgrupos de $\mathbb{S}_3$ son $\{id\}$, $\mathbb{S}_3$, los subgrupos $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$ de orden dos y el subgrupo $\langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$ de orden tres. Si $H = \langle(12)\rangle = \{id, (12)\}$, entonces

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

Ejemplo 4.5. 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 4.6. 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.

Tener una relación de equivalencia módulo H nos permite escribir a G como unión disjunta de coclases a izquierda (o a derecha) de H en G. Además dos coclases cualesquiera son iguales o disjuntas.

Teorema 4.7 (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 4.8. *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 4.9. *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, $G = H = \langle g \rangle$. $\square$

cor:ordenes_coprimos

Corolario 4.10. *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 4.11 (pequeño teorema de Fermat). Sea p un número primo. Demuestre que $a^{p-1} \equiv 1 \mod p$ 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 coprimos con n. El grupo de unidades de $\mathbb{Z}/n$ tiene $\varphi(n)$ elementos (pues $x \in \mathbb{Z}/p$ es inversible si y sólo si x es coprimo con n).

Ejercicio 4.12 (teorema de Euler). Sean a y n enteros coprimos. Demuestre que $a^{\phi(n)} \equiv 1 \mod n$.

No vale la recíproca del teorema de Lagrange.

Ejemplo 4.13. 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 $(\mathbb{A}_4 : H) = 6$, 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 4.14. 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 5
Cocientes

cocientes

Si G es un grupo y N es un subgrupo de G, nos interesa saber cuándo la operación $G/N \times G/N \to G/N$, $(xN, yN) \mapsto xyN$, está bien definida. 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 $y^{-1}ny \in N$.

Definición 5.1. 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 $N \trianglelefteq G$.

pro:normalidad

Proposición 5.2. *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 $(1) \implies (3)$, 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 5.3. *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 5.4. Si G es un grupo, entonces $\{1\}$ y G son subgrupos normales de G.

Ejemplo 5.5. 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 5.6. Si G es un grupo, entonces $[G,G]$ es un subgrupo normal de G pues

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

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

Ejemplo 5.7. 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

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

Ejemplo 5.8. 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 5.9. 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 5.10. $\mathbf{SL}_n(\mathbb{R})$ 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 5.11. El grupo de Klein $K = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en $\mathbb{S}_4$.

Ejercicio 5.12. Sea $G = \mathbb{Z}/p \times (\mathbb{Z}/p)^\times$ el grupo dado por la operación

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

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

El siguiente ejercicio es útil:

Ejercicio 5.13. 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 $S \trianglelefteq G$, entonces $T \leq N_G(S)$.
3. Si $T \leq N_G(S)$, entonces TS es un grupo y además $S \leq TS$.

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 $G = \mathbb{D}_8$ 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, $N = \mathbb{S}_4$.

Grupo!cociente

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 ïguales.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 $Q \simeq \mathbb{S}_3$.

Para terminar el capítulo mencionamos dos ejercicios de mucha utilidad.

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

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

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

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 $y^iH = y^jH$ para i, j tales que $i < j$, entonces $y^{j-i} \in H$ con $j - i \leq p-2$). Como $y = xhx^{-1}$, entonces

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

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 $(yx)H = y^iH$ para algún $i \in \{1, \ldots, p-1\}$ y entonces

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

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.

cor:p_menor

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 $g^n \in H$. □

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 $HK = KH = \{\mathrm{id}, (12)(34)\}$ 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.

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

thm:|HK|

Teorema 6.5. *Sean H y K subgrupos finitos de un grupo G. Entonces*

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

Demostración. Sea $Q = H \cap K$ y sea

$$\theta : H \times K \to HK, \quad \theta(h,k) = hk,$$

La función θ es claramente sobreyectiva.

Vamos a demostrar que si $x \in HK$, entonces $|\theta^{-1}(x)| = |H \cap K|$. Si $x \in HK$, entonces $x = hk$ para algún $h \in H$ y $k \in K$. Alcanza con ver que

$$\theta^{-1}(x) = \{(h\gamma, \gamma^{-1}k) : \gamma \in H \cap K\}.$$

Veamos la inclusión no trivial. Si $(h_1,k_1) \in \theta^{-1}(x)$, entonces

$$\theta(h_1,k_1) = h_1k_1 = x = hk.$$

En consecuencia, $\gamma = h^{-1}h_1 = kk_1^{-1} \in H \cap K$. Luego $(h_1,k_1) = (h\gamma, \gamma^{-1}k)$ para algún $\gamma \in H \cap K$. Como la otra inclusión es trivial, el teorema queda demostrado al observar que

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

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 29.

> 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.

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 $g = h(g^{-1}h_1g)$ para ciertos $h, h_1 \in H$. Luego

$$1 = hg^{-1}h_1 \implies h_1h = g \in H \implies H = K,$$

una contradicción.

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 gurpos, 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** $f|_S\colon S \to G$ 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 $f(1) = 1$ y que $f(g^{-1}) = f(g)^{-1}$ $f(g^n) = f(g)^n$ 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 $\ker f = \{1, 8, 13, 20\}$.

exa:afin **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 $\ker\pi = H$. 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. $\mathbb{S}_2 \simeq \mathbb{Z}/2 \simeq \mathbb{G}_2$.

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

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

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

$$f(x) = f(p(x/p)) = pf(x/p),$$

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 G_1, G_2 y G_3 grupos. Si $f \in \mathrm{Hom}(G_1,G_2)$ y $g \in \mathrm{Hom}(G_2,G_3)$, entonces $g \circ f \in \mathrm{Hom}(G_1,G_3)$.

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

Ejemplo 7.35. 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 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 $y \in G$ 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 $|y^2| = 3$, lo que nos dice que siempre existe $z \in G$ tal que $|z| = 3$. Tenemos

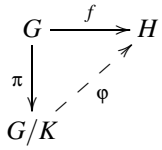
$$\langle x,z\rangle = \{1,x,z,z^2,xz,xz^2\} = G.$$

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 $|xz| = 6$ y luego $G = \langle xz\rangle \simeq \mathbb{Z}/6$. Si $xz = xz^2$, entonces $G = \langle x,z : x^2 = z^2 = 1, xzx^{-1} = z^2\rangle \simeq \mathbb{D}_3$.

Estamos en condiciones de enunciar y demostrar los teoremas de isomorfismos. Primero comenzaremos con un teorema técnico pero fundamental.

thm:cocientes

Teorema 7.36. *Sea $f\colon G \to H$ un morfismo de grupos y K un subgrupo normal de G tal que $K \subseteq \ker f$. Existe entonces 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, $\ker\varphi = \ker f/K$ *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.*

Demostración. Sea $\varphi\colon G/K \to H$, $xK \mapsto f(x)$. 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

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

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:

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

En consecuencia, $\ker\varphi = \{xK : x \in \ker f\} = \ker f/K$. La igualdad $\varphi(G/K) = f(G)$ es trivial.

De la definición de φ se obtiene inmediatamente que $\pi \circ \varphi = f$. Esta igualdad además garantiza la unicidad del morfismo φ pues si ψ es tal que $\psi \circ \pi = f$,

$$\varphi(xK) = \varphi(\pi(x)) = (\varphi \circ \pi)(x) = f(x) = (\psi \circ \pi)(x) = \psi(\pi(x)) = \psi(xK). \quad \square$$

Como corolario obtenemos:

Corolario 7.37 (primer teorema de isomorfismos). *Si $f\colon G \to H$ es un morfismo de grupos, entonces $G/\ker f \simeq f(G)$.*

Demostración. Es el teorema anterior con $H = f(G)$ y $K = \ker f$. $\square$

Ejemplos 7.38. Si G es un grupo, entonces $G/\{1\} \simeq G$ y $G/G \simeq \{1\}$.

Ejemplo 7.39. 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 7.40. 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 7.41. 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 sobreyectiva y que $\ker f = n\mathbb{Z}$. El resultado que queremos demostrar se obtiene entonces inmediatamente del primer teorema de isomorfismos.

Ejemplo 7.42. 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 7.43. 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 7.44. 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 7.45. 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 $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$.

El segundo teorema de isomorfismos resultará de gran utilidad al estudiar series de composición y resolubilidad.

Teorema 7.46 (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*

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

Demostración. Sea $\pi\colon G \to G/N$ el morfismo canónico. Ya vimos que la restricción $\pi|_T\colon T \to G/N$ es también 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 teormea de isomorfismos,

$$T/T \cap N \simeq \pi(T).$$

Observemos que $\pi(T) = NT/N$ pues es el subgrupo de G/N formado por las coclases de N en G con representantes en T. □

Ejemplo 7.47. 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 $HN = \langle 2\rangle$ y que $H \cap N = \{0, 12\}$. Calculemos las coclases de N en HN:

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

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 $HN/N \simeq H/H\cap N$. El isomorfismo está dado por $f\colon H/(H\cap N) \to HN/N$, $h+(H\cap N) \mapsto h+N$. En nuestro caso, $f(0+(H\cap N)) = 0+N$, $f(4+(H\cap N)) = 4+N$ y $f(8+(H\cap N)) = 8+N = 2+N$.

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 7.48. Si V es un espacio vectorial, entonces, en particular, V es un grupo abeliano. Si S y T son subespacios de V, entonces V y T son subgrupos normales de V. El segundo teorema de isomorfismos, en notación aditiva, nos dice que

$(S+T)/T \simeq S/(S\cap T)$. Puede verificarse que este isomorfismo es, en realidad, un isomorfismo de espacios vectoriales. Luego

$$\dim(S+T) - \dim T = \dim(S) - \dim(S\cap T).$$

Ejemplo 7.49. 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 7.50. *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. □

Antes de demostrar otro de los teoremas de isomorfismos, necesitamos el siguiente lema técnico.

lem:2do **Lema 7.51.** *Sea $f\colon G\to H$ un morfismo de grupos y sean $U\trianglelefteq G$ y $V\trianglelefteq H$. 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

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

Demostración. Observemos que la conmutatividad del diagrama es $\pi_V \circ f = g \circ \pi_U$. Por el teorema 7.36 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. □

Un caso particular del lema nos permite demostrar elegantemente el tercer teorema de isomorfismos.

Teorema 7.52 (tercer teorema de isomorfismos). *Sean S y T subgrupos normales de un grupo G tales que $S \subseteq T$. Entonces S es normal en T y T/S es normal en G/S. Además*

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

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

Demostración. Sean $H = G/U$, $U = T$, $V = T/S$ y $f = \pi_S \colon G \to G/S$ el morfismo canónico. El lema anterior 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 $\pi_S^{-1}(T/S) = T$. □

Ejemplo 7.53. Si n divide a m, 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.

Teorema 7.54 (de la correspondencia). *Sea $f \colon G \to H$ un morfismo de grupos y sea $K = \ker f$. Existe una correspondencia biyectiva entre*

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

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 $x\, nG$, 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 5.2. □

Veamos una aplicación del teorema anterior.

Proposición 7.55. *Si* $f\colon G \to f(G)$ *es un morfismo de grupos y* $H \leq G$ *es tal que* $\ker f \subseteq H$, *entonces* $(G : H) = (f(G) : f(H))$.

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

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

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 $\alpha(gH) = f(g)f(H)$. Basta ver 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 $g_1H = gH$. □

Observación 7.56. 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.

Ejemplo 7.57. 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 G/N tiene cuatro elementos, G/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 G/N y allí todo subgrupo es normal pues G/N es abeliano.

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

Ejemplo 7.58. 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

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

de $\mathbb{Z}/6$.

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 7.59. 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 7.60 (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 $n\mathbb{N}$. 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 7.61. *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 $g \in G$. Entonces $g \notin K$ pues, como $h \notin \mathbb{A}_n$,

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

Si $K = \ker(f \circ g)$, entonces $K = \{1\}$ pues G es simple. Además, la composición signo$\circ f$ es una función biyectiva pues signo$(f(1)) = 1$ y signo$(f(g)) = -1$. En consecuencia, por el primer teorema de isomorfismos, $G \simeq G/K \simeq \mathbb{Z}/2$. 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 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 8.1. $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}/2$ pues $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id}\}$.

Ejemplo 8.2. 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 $\mathrm{Aut}(G)/Inn(G)$ se conoce como el grupo de **automorfismos exteriores** de G.

Ejemplo 8.3. 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 $|\mathrm{Aut}(\mathbb{S}_3)| \leq 6$. Luego $\mathrm{Aut}(\mathbb{S}_3) = \mathrm{Inn}(\mathbb{S}_3) \simeq \mathbb{S}_3$.

Ejemplo 8.4. 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 sobre el cuerpo $\mathbb{Z}/p$ de dimensión dos y todo automorfismo del grupo es también una transformación lineal inversible.

Ejemplo 8.5. 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 **??** 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 8.6. $\mathrm{Aut}(\mathbb{Z}/8) \simeq \mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\} = \langle 3,5 \rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

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 8.7. *Sean G un grupo finito y abeliano y $n = \mathrm{máx}\{|g| : g \in G\}$. 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.

lem:X^n-1

Lema 8.8. *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 8.9. *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

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

Vamos a demostrar que 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 8.10. *Sea G un grupo abeliano. Si G tiene elementos de órdenes k y l, entonces G tiene un elemento de orden* $\operatorname{mcm}(k,l)$.

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 4.10 en la página 23 como aplicación del teorema de Lagrange. Supongamos entonces que $d = \operatorname{mcd}(k,l) > 1$. Escribimos

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

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

$$x = g^{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}, \quad y = h^{p_{r+1}^{\beta_{r+1}} \cdots p_r^{\beta_r}}.$$

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 8.11. 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 $5/\operatorname{mcd}(8,10) = 10/2 = 5$ y que $8 \in \mathbb{Z}/80$ tiene orden $80/\operatorname{mcd}(8,80) = 80/8 = 10$. 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 $\operatorname{mcm}(5,10) = 10$.

Ahora sí, el teorema.

Teorema 8.12. *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 8.8. 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 $\operatorname{mcm}(k,n) > n$, 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 8.8. □

Capítulo 9
Producto semidirecto

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

Teorema 9.1. *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 $g = h_1 h_1$ para $h_1 \in H$ y $k_1 \in K$, entonces, como $hk = h_1 k_1$, se tiene que $h_1^{-1} h = k_1 k^{-1} \in H \cap K = \{1\}$ y luego $h = h_1$ y $k = k_1$.

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

La observación anterior nos permite demostrar que f es un morfismo de grupos. Si $g = hk$ y $g_1 = h_1 k_1$ 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

$$f(g g_1) = f((hk)(h_1 k_1)) = f(h(k h_1) k_1) = f((h h_1)(k k_1)) = (h h_1, k k_1).$$

Queda como ejercicio demostrar que f es biyectiva. □

El teorema anterior puede 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 9.2. 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 9.3. *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 $\varphi : H \times K \to (H/A) \times (K/B)$, $\varphi(h,k) = (hA, kB)$. 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 9.4. 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 9.5. 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,

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

Definición 9.6. 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 $G = K \rtimes G$

Veamos algunas caracterizaciones del producto semidirecto.

Proposición 9.7. *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 $s : G/K \to G$ tal que $\pi \circ s = \mathrm{id}_{G/K}$, donde $\pi : G \to G/K$, $g \mapsto Kg$,' es el morfismo canónico.*
4. *Existe un morfismo $\rho : G \to G$ 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 $g = x_1 y_1$ con $x_1 \in K$ e $y_1 \in Q$, entonces $x_1^{-1} x = y y_1^{-1} \in K \cap Q = \{1\}$ y luego $x = x_1$ y también $y = y_1$.

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 $xyy_1x_1^{-1} = gg_1^{-1} \in K$, es decir $yy_1 \in x^{-1}Kx_1 = K$ pues $x, x_1 \in K$. Luego $yy_1 \in K \cap Q = \{1\}$ y entonces $y = y_1$ y también $x = x_1$. Veamos ahora que $\pi \circ s = \mathrm{id}_{G/K}$. Si $g = xy$ con $x \in K$ e $y \in Q$, entonces $(\pi \circ s)(Kg) = \pi(y) = Ky = Kxy = Kg$.

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

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 9.8. $\mathbb{S}_n = \mathbb{A}_n \rtimes \mathbb{Z}/2$ 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 9.9. *Sean K y Q grupos y sea $\theta : Q \to \mathrm{Aut}(K)$, $x \mapsto \theta_x$, 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 9.10. *Sean K y Q dos grupos y sea $\theta : Q \to \mathrm{Aut}(K)$ un morfismo de grupos. Entonces $K \rtimes_\theta Q$ es un producto semidirecto tal que*

$$(\theta_x(a), 1) = (1,x)(a,1)(1,x)^{-1}.$$

Bosquejo de la demostración. Sea $\pi : K \rtimes_\theta Q \to Q$, $\pi(a,x) = x$. Entonces π es un morfismo sobreyectivo. Como

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

podemos identificar estos grupos con K y Q, respectivamente. Luego, gracias a esta identificación, $G = (\ker \pi) \rtimes (\{1\} \times Q) = K \rtimes Q$. □

Proposición 9.11. *Si G es un producto semidirecto del subgrupo normal K con el subgrupo Q, existe un morfismo de grupos $\theta : Q \to \mathrm{Aut}(K)$ tal que $G \simeq K \rtimes_\theta Q$.*

Bosquejo de la demostración. Para $x \in Q$ sea $\theta_x : K \to K$, $\theta_x(a) = xax^{-1}$. 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 9.12. Sean $K = \mathbb{Z}/n$ y $Q = \mathbb{Z}/2 = \{0,1\}$. La función $\theta : Q \to \mathrm{Aut}(K)$, $1 \mapsto (x \mapsto x^{-1})$, es un morfismo de grupos. Sea $G = K \rtimes_\theta Q$. Entonces $G \simeq \mathbb{D}_n$...

Referencias

1. R. D. Carmichael. *Introduction to the theory of groups of finite order*. Dover Publications, Inc., New York, 1956.
2. R. M. Guralnick. Commutators and commutator subgroups. *Adv. in Math.*, 45(3):319–330, 1982.

Índice alfabético