Capítulo 7
Homomorfismos de grupos

Hasta el momento hemos visto algunas nociones básicas de grupos y varios ejemplos. Para relacionar diferentes grupos, necesitamos la noción de homomorfismo, una aplicación entre grupos que preserva su estructura. Después de estudiar homomorfismos, vamos a definir los subgrupos normales y grupos cociente. Todo esto es análogo al material del capítulo 4.

7.1 Definición y primeros ejemplos

7.1.1. Definición. Un **homomorfismo** entre grupos G y H es una aplicación $\phi\colon G \to H$ tal que para cualesquiera $g_1, g_2 \in G$ se cumple

$$\phi(g_1 g_2) = \phi(g_1)\,\phi(g_2).$$

7.1.2. Ejemplo. Para todo grupo G la aplicación identidad $\mathrm{id}\colon G \to G$ es un homomorfismo. ▲

7.1.3. Ejemplo. Todo homomorfismo de anillos $\phi\colon A \to B$ es un homomorfismo de grupos aditivos (esto hace parte de la definición). Además, todo homomorfismo de anillos $\phi\colon A \to B$ se restringe a un homomorfismo de grupos multiplicativos $\phi^\times\colon A^\times \to B^\times$. ▲

7.1.4. Ejemplo. La reducción módulo n es un homomorfismo de grupos aditivos

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

Además, tenemos un homomorfismo de grupos multiplicativos (poco interesante)

$$\{\pm 1\} \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad +1 \mapsto [1],\ -1 \mapsto [n-1].$$

Si $n \mid m$, entonces tenemos un homomorfismo de grupos aditivos

$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [a]_m \mapsto [a]_n$$

y un homomorfismo de grupos multiplicativos

$$(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad [a]_m \mapsto [a]_n.$$ ▲

7.1.5. Ejemplo. Para ver más homomorfismos familiares, podemos revisar algunas propiedades conocidas del análisis real y complejo.

1) El signo de un número racional (resp. real) no nulo es un homomorfismo de grupos multiplicativos

$$\mathbb{Q}^\times \to \{\pm 1\}\ (\text{resp. } \mathbb{R}^\times \to \{\pm 1\}), \quad x \mapsto \operatorname{sgn} x := \begin{cases} +1, & \text{si } x > 0, \\ -1, & \text{si } x < 0. \end{cases}$$

2) El valor absoluto de un número racional (resp. real, complejo) no nulo es un homomorfismo

$$\mathbb{Q}^\times \to \mathbb{Q}_{>0}, \text{ (resp. } \mathbb{R}^\times \to \mathbb{R}_{>0}, \mathbb{C}^\times \to \mathbb{R}_{>0}), \quad x \mapsto |x|.$$

De hecho, para cualesquiera x e y se tiene $|xy| = |x| \cdot |y|$.

3) Consideremos el grupo aditivo $\mathbb{R}$ y el grupo multiplicativo de los números reales positivos $\mathbb{R}_{>0}$. La función exponencial es un homomorfismo

$$\exp\colon \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x.$$

De hecho, para cualesquiera $x, y \in \mathbb{R}$ tenemos $e^{x+y} = e^x e^y$.

4) De manera similar, la exponencial compleja es un homomorfismo

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z.$$

Para cualesquiera $z, w \in \mathbb{C}$ tenemos $e^{z+w} = e^z e^w$.

5) El logaritmo es un homomorfismo

$$\log\colon \mathbb{R}_{>0} \to \mathbb{R}, \quad x \mapsto \log x.$$

Para cualesquiera $x, y > 0$ se cumple $\log(xy) = \log(x) + \log(y)$.

6) Para cualquier número real positivo $\alpha > 0$ la aplicación

$$\mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto x^\alpha$$

es un homomorfismo: se tiene $(xy)^\alpha = x^\alpha y^\alpha$. ▲

7.1.6. Ejemplo. El determinante de matrices invertibles de $n \times n$ es un homomorfismo de grupos

$$\det\colon \mathrm{GL}_n(A) \to A^\times$$

—de hecho, $\det(ab) = \det a \cdot \det b$. ▲

7.1.7. Ejemplo. Sean A un dominio de factorización única y $K = \operatorname{Frac} A$. Para un primo $p \in A$ la valuación p-ádica es un homomorfismo de grupos

$$\begin{aligned} v_p\colon K^\times &\to \mathbb{Z}, \\ \frac{a}{b} &\mapsto v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b). \end{aligned}$$

Si en lugar de $\mathbb{Z}$ queremos trabajar con un grupo multiplicativo, podemos definir el **valor absoluto p-ádico** de $x \in \mathbb{Q}^\times$ como sigue:

$$|x|_p := \rho^{v_p(x)}$$

para algún $0 < \rho < 1$. Entonces, para cualesquiera $x, y \in \mathbb{Q}^\times$ se cumple

$$|xy|_p = |x|_p \cdot |y|_p.$$

De esta manera se obtiene un homomorfismo de grupos multiplicativos

$$\begin{aligned} |\cdot|_p\colon K^\times &\to \mathbb{R}_{>0}, \\ x &\mapsto |x|_p. \end{aligned}$$

(Para $x = 0$ se define $|0|_p := 0$, lo que concuerda con la definición $v_p(0) := \infty$.) ▲

7.1.8. Ejemplo. El símbolo de Legendre es un homomorfismo de grupos multiplicativos

$$\left(\frac{\cdot}{p}\right): \mathbb{F}_p^\times \to \{\pm 1\},$$
$$a \mapsto \left(\frac{a}{p}\right).$$

De hecho, para cualesquiera $a, b \in \mathbb{F}_p^\times$ se cumple $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ▲

Las siguientes aplicaciones son homomorfismos por la definición de las estructuras algebraicas correspondientes.

7.1.9. Ejemplo.

1) Si A es un anillo (no necesariamente conmutativo) y $c \in A$ su elemento fijo, entonces la multiplicación por c por la izquierda es un homomorfismo de grupos aditivos

$$A \to A, \quad x \mapsto cx.$$

En efecto, la multiplicación es distributiva por la definición de anillos: para cualesquiera $x, y \in A$ debe cumplirse

$$c(x+y) = cx + cy.$$

De la misma manera, la multiplicación por la derecha es un homomorfismo

$$A \to A, \quad x \mapsto xc.$$

2) Si V es un espacio vectorial sobre un cuerpo k y $\lambda \in k$ es un escalar fijo, entonces la multiplicación por λ es un homomorfismo de grupos aditivos

$$V \to V, \quad v \mapsto \lambda \cdot v.$$

En efecto, según los axiomas de espacios vectoriales, se tiene

$$\lambda \cdot (u+v) = \lambda \cdot u + \lambda \cdot v.$$ ▲

7.1.10. Ejemplo. Si A es un grupo abeliano, entonces para $n \in \mathbb{Z}$ y para cualesquiera $a, b \in A$ tenemos

$$n \cdot (a+b) := \underbrace{(a+b) + \cdots + (a+b)}_{n} = \underbrace{a + \cdots + a}_{n} + \underbrace{b + \cdots + b}_{n} = n \cdot a + n \cdot b,$$

así que la multiplicación por n es un homomorfismo que se denota por

$$A \xrightarrow{\times n} A.$$

Cuando el grupo es abeliano, pero se usa la notación multiplicativa, se trata de las potencias n-ésimas $a \mapsto a^n$:

$$(ab)^n := \underbrace{ab \cdots ab}_{n} = \underbrace{a \cdots a}_{n} \cdot \underbrace{b \cdots b}_{n} =: a^n b^n.$$

Note que en un grupo no abeliano, en general $(gh)^n \neq g^n h^n$. Por ejemplo, se puede ver que G es abeliano si y solamente si $(gh)^2 = g^2 h^2$ para cualesquiera $g, h \in G$. ▲

7.2 Signo de permutaciones

> Cuando alguno me muestra un signo, si ignoro lo que significa no me puede enseñar nada; pero si lo sé, ¿qué es lo que aprendo por el signo?
>
> San Agustín, "El Maestro", Capítulo X

7.2.1. Definición. Para una permutación $\sigma \in S_n$ cuando para algunos $1 \le i < j \le n$ se tiene $\sigma(i) > \sigma(j)$, se dice que hay una **inversión**. El número

$$\operatorname{sgn}\sigma := (-1)^{\#\text{de inversiones}}$$

se llama el **signo** de σ. Se dice que σ es **par** si $\operatorname{sgn}\sigma = +1$ e **impar** si $\operatorname{sgn}\sigma = -1$.

7.2.2. Ejemplo. Para S_3 tenemos

permutación	inversiones	signo	
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	no hay	$+1$	(par)
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$3>2$	-1	(impar)
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$3>2,\ 3>1,\ 2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$2>1,\ 3>1$	$+1$	(par)
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$3>1,\ 3>2$	$+1$	(par)

▲

Recordemos algunas observaciones del capítulo anterior.

1) Toda permutación $\sigma \in S_n$ es un producto de ciclos disjuntos.

2) Todo k-ciclo es una composición de $k-1$ transposiciones:

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)\,(i_2\ i_3)\,(i_3\ i_4)\cdots(i_{k-1}\ i_k).$$

   En particular, toda permutación $\sigma \in S_n$ es un producto de transposiciones.

3) Toda transposición $(a\ b)$ puede ser escrita como una composición de $2\cdot|b-a|-1$ transposiciones de la forma $(i\ i+1)$.

   En particular, todo elemento de S_n puede ser expresado como un producto de transposiciones

$$(1\ 2),\ (2\ 3),\ (3\ 4),\ \ldots,\ (n-1\ n).$$

7.2.3. Observación. *Transposiciones cambian la paridad: si τ es una transposición y $\sigma \in S_n$ es cualquier permutación, entonces*

$$\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}\sigma.$$

Demostración. Está claro que cuando σ es de la forma $(i\ i+1)$, el signo cambia al opuesto. Luego, toda transposición $(a\ b)$ es una composición de $2\cdot|b-a|-1$ transposiciones de esta forma. El último número es siempre impar. ■

7.2.4. Corolario. *La paridad de una permutación σ es precisamente la paridad de la longitud de alguna descomposición en transposiciones: si $\sigma = \tau_1 \cdots \tau_k$ para algunas transposiciones τ_i, entonces*

$$\operatorname{sgn}\sigma = (-1)^k.$$

7.2.5. Corolario. *Para dos diferentes descomposiciones en transposiciones*

$$\sigma = \tau_1 \cdots \tau_k = \tau'_1 \cdots \tau'_\ell$$

los números k y ℓ necesariamente tienen la misma paridad: $k \equiv \ell \pmod 2$.

7.2.6. Corolario. *El signo de k-ciclo viene dado por*

$$\operatorname{sgn}(i_1\ i_2 \cdots i_k) = (-1)^k.$$

Demostración. Se sigue de la descomposición en $k-1$ transposición:

$$(i_1\ i_2 \cdots i_k) = (i_1\ i_2)\,(i_2\ i_3) \cdots (i_{k-1}\ i_k).$$ ■

7.2.7. Corolario. *Para dos permutaciones $\sigma, \tau \in S_n$ se tiene*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

En otras palabras, el signo es un homomorfismo de grupos $S_n \to \{\pm 1\}$.

Demostración. Está claro de la interpretación del signo en 7.2.4. ■

El signo de permutaciones sale en varios contextos importantes, como por ejemplo la fórmula del determinante

$$\det\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Aquí la suma tiene $n!$ términos y está indexada por todas las permutaciones de n índices. Por ejemplo, si $n=2$, se recupera la fórmula

$$\det\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = x_{11}x_{22} - x_{12}x_{21}.$$

Dejo al lector escribir la fórmula correspondiente para $n=3$.

Otra aparición curiosa del signo es la siguiente. Para un primo p consideremos el grupo de los restos no nulos módulo p:

$$\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}.$$

Ahora para cualquier $a \in \mathbb{F}_p^\times$ la multiplicación por a es una biyección[*]

$$\mu_a \colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times, \quad x \mapsto ax.$$

De hecho, dado que a es invertible, se ve que

$$(\mu_a)^{-1} = \mu_{a^{-1}}.$$

Entonces, μ_a permuta de alguna manera los elementos de $\mathbb{F}_p^\times$, y sería interesante investigar qué signo tiene esta permutación.

[*] Ya que estamos hablando de homomorfismos de grupos, notamos que esta es una aplicación biyectiva, pero *no es* un homomorfismo.

7.2.8. Ejemplo. Para $p = 7$ tenemos

$$\mathbb{F}_7^\times = \{1,2,3,4,5,6\}.$$

Consideremos la multiplicación por $a = 1,2,3,4,5,6$ sobre $\mathbb{F}_7^\times$.

a	μ_a	$\operatorname{sgn}\mu_a$
1	id	$+1$
2	$\begin{pmatrix}1&2&3&4&5&6\\2&4&6&1&3&5\end{pmatrix} = (1\ 2\ 4)\,(3\ 6\ 5)$	$+1$
3	$\begin{pmatrix}1&2&3&4&5&6\\3&6&2&5&1&4\end{pmatrix} = (1\ 3\ 2\ 6\ 4\ 5)$	-1
4	$\begin{pmatrix}1&2&3&4&5&6\\4&1&5&2&6&3\end{pmatrix} = (1\ 4\ 2)\,(3\ 5\ 6)$	$+1$
5	$\begin{pmatrix}1&2&3&4&5&6\\5&3&1&6&4&2\end{pmatrix} = (1\ 5\ 4\ 6\ 2\ 3)$	-1
6	$\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix} = (1\ 6)\,(2\ 5)\,(3\ 4)$	-1

Entonces, $\operatorname{sgn}\mu_a = +1$ para $a = 1,2,4$. Casualmente, estos son los cuadrados módulo 7 (note que $3^2 \equiv 2$ (mód 7)). ▲

7.2.9. Ejemplo. Consideremos la multiplicación por 3 sobre $\mathbb{F}_{11}^\times$. Tenemos la permutación

$$\mu_3 = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&6&9&1&4&7&10&2&5&8\end{pmatrix} = (1\ 3\ 9\ 5\ 4)\,(2\ 6\ 7\ 10\ 8).$$

Su signo es $+1$, y $3 \equiv 5^2$ es un cuadrado módulo 11. Por otra parte, la multiplicación por 6 nos da la permutación

$$\mu_6 = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\6&1&7&2&8&3&9&4&10&5\end{pmatrix} = (1\ 6\ 3\ 7\ 9\ 10\ 5\ 8\ 4\ 2)$$

de signo $(-1)^{10-1} = -1$, y 6 no es un cuadrado módulo 11. Los cuadrados módulo 11 son 1, $3 \equiv 5^2$, 4, $5 \equiv 4^2$, 9. ▲

Resulta que el signo de la permutación μ_a siempre detecta los residuos cuadráticos.

7.2.10. Proposición. *Para cualquier $a \in \mathbb{F}_p^\times$ se tiene*

$$\operatorname{sgn}\mu_a = \left(\frac{a}{p}\right).$$

Demostración. Recordemos que el grupo $\mathbb{F}_p^\times$ es cíclico: existe un generador $x \in \mathbb{F}_p^\times$ tal que

$$\mathbb{F}_p^\times = \{1, x, x^2, \ldots, x^{p-1}\}$$

(véase 7.5.11 abajo para un resultado más general). Ahora la multiplicación por x permuta de manera cíclica todos los elementos de $\mathbb{F}_p^\times$. Tenemos entonces un ciclo de orden par $p-1$, así que

$$\operatorname{sgn}\mu_x = -1.$$

Ahora si $a = x^k$, entonces

$$\operatorname{sgn}\mu_{x^k} = \operatorname{sgn}(\mu_x)^k = (-1)^k = \left(\frac{a}{p}\right).$$

■

Esta observación pertenece a Zolotariov[*], y varias pruebas de la reciprocidad cuadrática se basan en ella. (De hecho, la interpretación se generaliza al **símbolo de Jacobi**[**]: para n compuesto hay que analizar la multiplicación por $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ sobre $(\mathbb{Z}/n\mathbb{Z})^\times$.)

7.3 Propiedades básicas

7.3.1. Observación. *La composición de dos homomorfismos $\phi\colon G \to H$ y $\psi\colon H \to K$ es también un homomorfismo $\psi \circ \phi\colon G \to K$.* □

7.3.2. Observación. *Ses $\phi\colon G \to H$ un homomorfismo de grupos. Entonces,*

1) *ϕ preserva la identidad: $\phi(1_G) = 1_H$;*
2) *ϕ preserva los elementos inversos: $\phi(g^{-1}) = \phi(g)^{-1}$ para todo $g \in G$;*
3) *para todo $n \in \mathbb{Z}$ y $g \in G$ se cumple $\phi(g^n) = \phi(g)^n$.*
4) *si $g^n = 1_G$, entonces $\phi(g)^n = 1_H$; en particular, todo homomorfismo preserva los elementos de orden finito.*

Demostración. Tenemos

$$\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G),$$

y la cancelación en H nos permite concluir que $\phi(1_G) = 1_H$. Para los inversos, basta notar que

$$\phi(g^{-1}) \cdot \phi(g) = \phi(g^{-1} g) = \phi(1_G) = 1_H.$$

La parte 3) se demuestra por inducción (si $n < 0$, hay que ocupar la parte 2)). En fin, 4) es una consecuencia de 1) y 3). ■

7.3.3. Ejemplo. El determinante cumple $\det(1) = 1$ y $\det(a^{-1}) = (\det a)^{-1}$ para toda matriz invertible a. ▲

7.3.4. Ejemplo. El signo cumple $\operatorname{sgn}(\mathrm{id}) = +1$ y $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}\sigma$ para toda permutación $\sigma \in S_n$. ▲

7.3.5. Definición. Se dice que un homomorfismo de grupos $\phi\colon G \to H$ es un **isomorfismo** si existe un homomorfismo $\phi^{-1}\colon H \to G$ tal que $\phi^{-1} \circ \phi = \mathrm{id}_G$ y $\phi \circ \phi^{-1} = \mathrm{id}_H$.

7.3.6. Observación. *Un homomorfismo $\phi\colon G \to H$ es un isomorfismo si y solamente si es biyectivo.*

Demostración. Para $h_1, h_2 \in H$ tenemos

$$\phi^{-1}(h_1 h_2) = \phi^{-1}\Big(\phi(\phi^{-1}(h_1)) \cdot \phi(\phi^{-1}(h_2))\Big) = \phi^{-1}\Big(\phi\big(\phi^{-1}(h_1) \cdot \phi^{-1}(h_2)\big)\Big)$$
$$= \phi^{-1}(h_1) \cdot \phi^{-1}(h_2),$$

donde la primera igualdad viene de $\phi \circ \phi^{-1} = \mathrm{id}_H$, la segunda igualdad se cumple porque ϕ es un homomorfismo, y la tercera igualdad viene de $\phi^{-1} \circ \phi = \mathrm{id}_G$. ■

7.3.7. Proposición. *Todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.*

[*] Yegor Ivánovich Zolotariov (1847–1878), matemático ruso, de San Petersburgo. Obtuvo varios resultados importantes, pero murió joven atropellado por un tren.

[**] Para recordar la reciprocidad cuadrática y los símbolos de Legendre y Jacobi, véanse mis apuntes
http://cadadr.org/san-salvador/2018-cp-tne/reciprocidad-cuadratica.pdf

Demostración. Si G es un grupo cíclico finito de orden n, entonces

$$G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

para algún $g \in G$. Definamos la aplicación

$$\phi\colon G \to \mathbb{Z}/n\mathbb{Z}, \quad g^k \mapsto [k]_n.$$

Esta aplicación está bien definida: $g^k = g^\ell$ si y solamente si $k \equiv \ell \pmod{n}$. Note que esto también demuestra que ϕ es una biyección. Este es un homomorfismo, ya que

$$\phi(g^k \cdot g^\ell) = \phi(g^{k+\ell}) = [k+\ell]_n = [k]_n + [\ell]_n = \phi(g^k) + \phi(g^\ell).$$

Ahora si

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

es un grupo cíclico infinito, entonces la aplicación

$$\phi\colon G \to \mathbb{Z}, \quad g^n \mapsto n$$

es visiblemente un isomorfismo. ■

7.3.8. Ejemplo. Para el grupo de las raíces n-ésimas de la unidad tenemos un isomorfismo

$$\mu_n(\mathbb{C}) \to \mathbb{Z}/n\mathbb{Z}, \quad \zeta_n^k \mapsto [k]_n.$$ ▲

7.3.9. Ejemplo. Un grupo puede ser isomorfo a un subgrupo propio. Obviamente, es imposible para grupos finitos, pero para grupos infinitos, por ejemplo, tenemos un isomorfismo

$$\mathbb{Z} \to 2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\}, \quad n \mapsto 2n.$$ ▲

Note que el isomorfismo construido en 7.3.7 no es canónico: para construirlo, hemos *escogido* un generador $g \in G$. Diferentes generadores nos darían diferentes isomorfismos. Los grupos específicos $\mathbb{Z}/n\mathbb{Z}$, $\mu_n(\mathbb{C})$, $\mathbb{Z}$ vienen con un generador canónico en cierto sentido: $[1]_n$, $\zeta_n := e^{2\pi i/n}$, y $+1$ respectivamente.

7.3.10. Definición. Un isomorfismo entre un grupo G y sí mismo se llama un **automorfismo** de G.

7.3.11. Observación. *Los automorfismos de G forman un grupo respecto a la composición. Este se denota por* $\mathrm{Aut}(G)$.

Demostración. Siempre existe el automorfismo identidad $\mathrm{id}\colon G \to G$ y es el elemento neutro de $\mathrm{Aut}(G)$. Si $\phi\colon G \to G$ y $\psi\colon G \to G$ son dos automorfismos, entonces su composición $\psi \circ \phi\colon G \to G$ es también un automorfismo. Todo automorfismo $\phi\colon G \to G$ posee una aplicación inversa $\phi^{-1}\colon G \to G$, y como hemos visto arriba, es automáticamente un automorfismo. ■

El estudio de automorfismos de un objeto es un tema fundamental en matemáticas. Aquí vamos a ver un ejemplo sencillo de automorfismos de grupos cíclicos.

7.3.12. Ejemplo. Consideremos el grupo cíclico $\mathbb{Z}/n\mathbb{Z}$. Notamos que todo automorfismo

$$\phi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

está definido por la imagen $\phi([1])$, puesto que $[1]$ es un generador. Para que ϕ sea sobreyectivo, $\phi([1])$ también debe ser un generador, y en este caso ϕ es automáticamente inyectivo. Podemos concluir que los automorfismos de $\mathbb{Z}/n\mathbb{Z}$ son precisamente

$$\mu_a\colon [x] \mapsto [ax],$$

donde $\mathrm{mcd}(a, n) = 1$; es decir, $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Además,

$$\mu_a \circ \mu_b = \mu_{ab},$$

lo que nos da un isomorfismo

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\cong} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad [a] \mapsto \mu_a.$$ ▲

7.3.13. Ejemplo. Las mismas consideraciones nos dicen que un grupo cíclico infinito tiene dos automorfismos:

$$\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\}.$$ ▲

7.3.14. Ejemplo. Sean X e Y dos conjuntos tales que existe una biyección $f\colon X \to Y$. Dejo al lector verificar que una elección de f induce un isomorfismo entre los grupos simétricos

$$S_X \to S_Y,$$
$$(X \xrightarrow{\sigma} X) \mapsto (Y \xrightarrow{f^{-1}} X \xrightarrow{\sigma} X \xrightarrow{f} Y).$$

En particular, el grupo de permutaciones de los elementos de un conjunto finito X es isomorfo a S_n donde $n = |X|$. ▲

7.3.15. Ejemplo. Dado un cuerpo k consideremos el espacio vectorial k^n junto con su base estándar

$$e_1 = (1,0,0,\ldots,0),\ e_2 = (0,1,0,\ldots,0),\ \ldots,\ e_n = (0,0,0,\ldots,1).$$

En los cursos de álgebra lineal se estudia que las aplicaciones lineales $k^n \to k^n$ pueden ser representadas por las matrices de $n \times n$, de tal modo que la composición de aplicaciones lineales corresponde a la multiplicación de matrices. Aplicaciones lineales invertibles corresponden a matrices invertibles. Esto nos da un isomorfismo de grupos

$$\mathrm{GL}(k^n) \cong \mathrm{GL}_n(k).$$

En general, si V es cualquier espacio vectorial sobre k de dimensión n, una *elección de base* nos da un isomorfismo de espacios vectoriales $f\colon V \xrightarrow{\cong} k^n$, y por lo tanto un isomorfismo de grupos

$$\mathrm{GL}(V) \xrightarrow{\cong} \mathrm{GL}(k^n),$$
$$(\phi\colon V \to V) \mapsto (f \circ \phi \circ f^{-1}\colon k^n \to k^n),$$

pero este no es canónico ya que depende de la base escogida. ▲

7.3.16. Ejemplo. La exponencial real

$$\exp\colon \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto \exp(x)$$

es un isomorfismo de grupos que posee una aplicación inversa, a saber el logaritmo:

$$\log\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto \log(x).$$

Como hemos visto, la aplicación inversa es automáticamente un homomorfismo:

$$\log(xy) = \log(x) + \log(y).$$ ▲

7.3.17. Ejemplo. Dejo como un ejercicio encontrar isomorfismos de grupos $D_3 \cong S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$. ▲

Cuando dos grupos son isomorfos, estos pueden ser identificados, salvo alguna permutación de elementos que respeta la operación del grupo. En particular, dos grupos isomorfos comparten las mismas propiedades.

7.3.18. Ejemplo. Los grupos $\mathbb{Z}/6\mathbb{Z}$ y S_3 tienen la misma cardinalidad $6 = 3!$. Sin embargo, $\mathbb{Z}/6\mathbb{Z}$ es un grupo abeliano, mientras que S_3 no lo es, y por lo tanto no son isomorfos.

De la misma manera, el grupo cíclico $\mathbb{Z}/8\mathbb{Z}$ y el grupo de cuaterniones Q_8 no son isomorfos: los cuaterniones Q_8 no son abelianos. El grupo diédrico

$$D_4 = \{\mathrm{id}, r, r^2, r^3, f, rf, r^2f, r^3f\}$$

es otro grupo no abeliano de 8 elementos que no es isomorfo a Q_8. Por ejemplo, podemos notar que en Q_8 se tiene

$$(\pm I)^2 = (\pm J)^2 = (\pm K)^2 = -1,$$

así que $\pm I, \pm J, \pm K$ tendrán orden 4. Además, -1 es el único elemento de orden 2. Los elementos del grupo D_4 tienen ordenes distintos: r^2 y todas las cuatro reflexiones f, rf, r^2f, r^3f tienen orden 2, mientras que r y r^3 tienen orden 4. ▲

Desde los inicios de la teoría de grupos los matemáticos estaban interesados en describir todos los grupos finitos salvo isomorfismo. Sin embargo, la estructura de grupo es muy básica, así que este problema es algo similar a compilar un atlas de botánica con todas las plantas del mundo... Sorprendentemente, la respuesta, aunque sea enorme, existe y se conoce como la **clasificación de los grupos simples*** **finitos**. Esta fue terminada en los años 2000. El mismo enunciado es muy complicado y sus pruebas están contenidas en centenas de artículos publicados a partir de los años 50 del siglo pasado. Entonces, aunque la clasificación de grupos finitos es un logro muy importante, es un área bastante peculiar.

7.3.19. Observación. *Sea $\phi\colon G \to H$ un homomorfismo de grupos. Definamos la **imagen** de ϕ por*

$$\operatorname{im}\phi := f(G) := \{\phi(g) \mid g \in G\}$$

*y el **núcleo** por*

$$\ker\phi := \{g \in G \mid \phi(g) = 1_H\}.$$

Entonces, $\operatorname{im}\phi$ es un subgrupo de H y $\ker\phi$ es un subgrupo de G. □

7.3.20. Observación. *Un homomorfismo $\phi\colon G \to H$ es inyectivo si y solamente si su núcleo es trivial; es decir, $\ker\phi = \{1_G\}$.* □

7.3.21. Ejemplo. El núcleo del homomorfismo $\operatorname{sgn}\colon S_n \to \{\pm\}$ consiste en todas las permutaciones pares $\sigma \in S_n$. Este se denota por

$$A_n := \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\}$$

y recibe el nombre del **grupo alternante**. Siendo un núcleo, este es un subgrupo de S_n.

Por ejemplo,

$$A_2 = \{\mathrm{id}\},$$
$$A_3 = \{\mathrm{id},\ (1\ 2\ 3),\ (1\ 3\ 2)\}.$$

En S_4 las permutaciones son de la forma

$$\mathrm{id}, \quad (\bullet\ \bullet), \quad (\bullet\ \bullet\ \bullet), \quad (\bullet\ \bullet)(\bullet\ \bullet), \quad (\bullet\ \bullet\ \bullet\ \bullet).$$

Luego, los elementos de A_4 son las permutaciones id, $(\bullet\ \bullet\ \bullet)$ y $(\bullet\ \bullet)(\bullet\ \bullet)$:

$$\mathrm{id},$$
$$(1\ 2\ 3), \quad (1\ 2\ 4), \quad (1\ 3\ 2), \quad (1\ 3\ 4), \quad (1\ 4\ 2), \quad (1\ 4\ 3), \quad (2\ 3\ 4), \quad (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), \quad (1\ 3)(2\ 4), \quad (1\ 4)(2\ 3).$$ ▲

7.3.22. Ejemplo. El núcleo del homomorfismo $\det\colon \mathrm{GL}_n(A) \to A^\times$ recibe el nombre del **grupo lineal especial** y se denota por

$$\mathrm{SL}_n(A) := \{a \in \mathrm{GL}_n(A) \mid \det a = 1\}.$$

Ya hemos visto un caso particular que es el grupo $\mathrm{SL}_2(\mathbb{Z})$. ▲

7.3.23. Ejemplo. Tenemos

$$\ker(\mathbb{R}^\times \xrightarrow{\operatorname{sgn}} \{\pm 1\}) = \mathbb{R}_{>0}.$$ ▲

*Véase la definición de grupo simple en §7.9.

7.3.24. Ejemplo. Por definición, el grupo de las n-ésimas raíces de la unidad $\mu_n(\mathbb{C})$ es el núcleo del homomorfismo $z \mapsto z^n$ sobre $\mathbb{C}^\times$:

$$\mu_n(\mathbb{C}) := \ker(\mathbb{C}^\times \xrightarrow{(-)^n} \mathbb{C}^\times). \qquad \blacktriangle$$

7.3.25. Ejemplo. Para la exponente compleja

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z$$

se tiene

$$\ker(\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times) = 2\pi i\,\mathbb{Z} = \{2\pi i n \mid n \in \mathbb{Z}\} \subset \mathbb{C}.$$

Por esto en el caso complejo, el logaritmo es más sutil: la exponencial toma el mismo valor en $z + 2\pi i n$ para todo $n \in \mathbb{Z}$, lo que impide definir una función inversa $\log\colon \mathbb{C}^\times \to \mathbb{C}$. $\blacktriangle$

Dado que la imagen de un homomorfismo $\phi\colon G \to H$ es un subgrupo de H, si ϕ es inyectivo, este puede ser visto como un isomorfismo entre G e $\operatorname{im} G$. En esta situación es común identificar G con $\operatorname{im} G$.

7.3.26. Ejemplo. Toda permutación $\sigma \in S_n$ puede ser extendida a una permutación de $\{1, \ldots, n, n+1\}$ poniendo

$$\sigma(n+1) := n+1.$$

Esto define un homomorfismo inyectivo

$$S_n \rightarrowtail S_{n+1}.$$

De este modo S_n se identifica con un subgrupo de S_{n+1}. En este sentido, tenemos una cadena de subgrupos

$$S_1 \subset S_2 \subset S_3 \subset S_4 \subset S_5 \subset \cdots$$

y podemos considerar su unión

$$S_\infty := \bigcup_{n \geq 1} S_n.$$

Este grupo permuta los elementos de $\{1, 2, 3, \ldots\}$, pero para cada $\sigma \in S_\infty$ tenemos $\sigma(i) = i$ para todo i, excepto un número finito. $\blacktriangle$

El último ejemplo es algo parecido al grupo $\mu_\infty(\mathbb{C}) := \bigcup_{n \geq 1} \mu_n(\mathbb{C})$.

7.3.27. Ejemplo. A una matriz invertible $a \in \mathrm{GL}_n(A)$ podemos asociar una matriz invertible $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_{n+1}(A)$ poniendo 1 en la entrada $(n+1, n+1)$. En este sentido se obtiene una cadena de subgrupos

$$\mathrm{GL}_1(A) \subset \mathrm{GL}_2(A) \subset \mathrm{GL}_3(A) \subset \mathrm{GL}_4(A) \subset \cdots$$

Luego, se obtiene un grupo

$$\mathrm{GL}_\infty(A) := \bigcup_{n \geq 1} \mathrm{GL}_n(A).$$

Este consiste en matrices infinitas, pero cada una de ellas afecta solamente la parte finita de $A \times A \times A \times \cdots$ y deja el resto intacto. $\blacktriangle$

7.4 Clases laterales

7.4.1. Notación. Para un subconjunto $S \subset G$ y un elemento fijo $g \in G$ escribamos

$$gS := \{gs \mid s \in S\}, \quad Sg := \{sg \mid s \in S\}.$$

En particular, para dos elementos fijos $g_1, g_2 \in G$ se tiene

$$g_1 S g_2 = g_1(Sg_2) = (g_1 S)g_2 = \{g_1\, s\, g_2 \mid s \in S\}.$$

Si G es un grupo abeliano, entonces $gS = Sg$ para cualquier $g \in G$. Cuando G no es abeliano, en general $gS \neq Sg$.

7.4.2. Observación. *Sea G un grupo y H su subgrupo. Consideremos la relación*

$$g_1 \equiv g_2 \pmod{H}$$

para $g_1, g_2 \in G$ dada por una de las siguientes condiciones equivalentes:

1) $g_1^{-1} g_2 \in H$.

2) $g_2 \in g_1 H$ *(es decir,* $g_2 = g_1 h$ *para algún* $h \in H$*).*

Esta es una relación de equivalencia. □

También podríamos considerar la relación

$$g_1 \sim g_2 \iff g_2 g_1^{-1} \in H.$$

Ya que el grupo G no es necesariamente abeliano, en general esta relación es diferente de la relación de arriba, pero es también una relación de equivalencia.

7.4.3. Observación. *Sea G un grupo y H su subgrupo. Consideremos la relación $g_1 \sim g_2$ para $g_1, g_2 \in G$ dada por una de las siguientes condiciones equivalentes:*

1) $g_2 g_1^{-1} \in H$.

2) $g_2 \in H g_1$ *(es decir,* $g_2 = h g_1$ *para algún* $h \in H$*).*

Esta es una relación de equivalencia. □

Como para toda relación de equivalencia, tenemos una descomposición de G en una unión disjunta de clases de equivalencia. Para la relación de 7.4.2 las clases de equivalencia son precisamente los conjuntos gH para $g \in G$, mientras que para la relación de 7.4.3 son los Hg.

7.4.4. Definición. Los subconjuntos $gH \subset G$ se llaman las **clases laterales izquierdas**[*] respecto a H. El conjunto de las clases laterales izquierdas se denota por G/H. Los subconjuntos Hg se llaman las **clases laterales derechas** respecto a H. El conjunto de las clases laterales derechas se denota por $H\backslash G$[**].

7.4.5. Observación. *Para todo $g \in G$ existen biyecciones de conjuntos*

$$gH \cong H \quad y \quad Hg \cong H.$$

En otras palabras, cada clase lateral izquierda (resp. derecha) tiene la misma cardinalidad que H.

Demostración. Por ejemplo, para las clases izquierdas, tenemos biyecciones

$$\begin{aligned} gH &\to H, \\ gh &\mapsto g^{-1} gh = h, \\ gh &\leftarrow\!\shortmid h. \end{aligned}$$

■

[*] En inglés "clase lateral" se traduce como "coset".

[**] No confundir la notación $H\backslash G$ con la diferencia de conjuntos $X \setminus Y$.

7.4.6. Observación. *La aplicación entre conjuntos*

$$\begin{aligned} i\colon G &\to G, \\ g &\mapsto g^{-1} \end{aligned}$$

induce una biyección canónica

$$\begin{aligned} G/H &\to H\backslash G, \\ gH &\mapsto Hg^{-1}. \end{aligned}$$

Demostración. La aplicación está bien definida sobre las clases de equivalencia: $g_1H = g_2H$ quiere decir que $g_2 = g_1h$ para algún $h \in H$. Luego, $g_2^{-1} = h^{-1}g_1^{-1}$, así que $Hg_2^{-1} = Hg_1^{-1}$. Entonces, la aplicación $g \mapsto g^{-1}$ envía la clase lateral izquierda gH a la clase lateral derecha Hg^{-1}.

Está claro que i es una biyección, puesto que $i \circ i = \mathrm{id}$. ■

Aunque gH y Hg tienen la misma cardinalidad, en general $gH \neq Hg$ si el grupo G no es abeliano.

7.4.7. Ejemplo. En el grupo simétrico S_n consideremos las permutaciones que dejan el número n fijo. Estas forman un subgrupo que es isomorfo a S_{n-1}:

$$H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}.$$

Dos permutaciones σ y τ pertenecen a la misma clase lateral *izquierda* si $\sigma^{-1}\tau \in H$; es decir, si $\sigma(n) = \tau(n)$. Entonces, tenemos n diferentes clases laterales izquierdas S_n/H

$$L_i := \{\sigma \in S_n \mid \sigma(n) = i\}, \quad 1 \leq i \leq n.$$

Por otro lado, σ y τ pertenecen a la misma clase lateral *derecha* si $\tau\sigma^{-1} \in H$; es decir, si $\sigma^{-1}(n) = \tau^{-1}(n)$. Hay n diferentes clases laterales derechas $H\backslash S_n$

$$R_i := \{\sigma \in S_n \mid \sigma(i) = n\}, \quad 1 \leq i \leq n.$$

Ahora si $L_i = R_i$ para algún i, tenemos

$$\sigma(n) = i \iff \sigma(i) = n,$$

entonces $i = n$. ▲

7.4.8. Ejemplo. Consideremos el grupo aditivo $\mathbb{C}$ e identifiquemos $\mathbb{R}$ con el subgrupo de los números complejos z tales que $\operatorname{Im} z = 0$. De la misma manera, consideremos el grupo multiplicativo $\mathbb{C}^\times$ y sus subgrupos

$$\mathbb{S}^1 := \{z \in \mathbb{C}^\times \mid |z| = 1\}$$

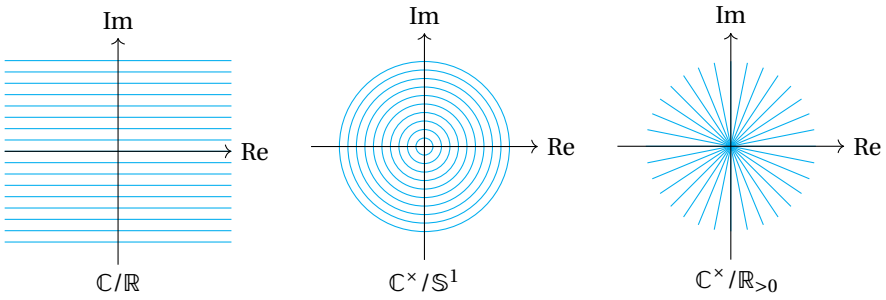
(el grupo del círculo) y

$$\mathbb{R}_{>0} = \{z \in \mathbb{C}^\times \mid \operatorname{Im} z = 0, \operatorname{Re} z > 0\}.$$

Los dibujos de abajo representan las clases laterales

$$\begin{aligned} \mathbb{C}/\mathbb{R} &= \{z + \mathbb{R} \mid z \in \mathbb{C}\}, \\ \mathbb{C}^\times/\mathbb{S}^1 &= \{z\mathbb{S}^1 \mid z \in \mathbb{C}^\times\}, \\ \mathbb{C}^\times/\mathbb{R}_{>0} &= \{z\mathbb{R}_{>0} \mid z \in \mathbb{C}^\times\} \end{aligned}$$

en el plano complejo.



▲

7.4.9. Ejemplo. Sea A un anillo conmutativo. Consideremos el grupo $\mathrm{GL}_n(A)$ y su subgrupo $\mathrm{SL}_n(A) := \{a \in \mathrm{GL}_n(A) \mid \det a = 1\}$. Para $a, b \in \mathrm{GL}_n(A)$ tenemos

$$a\,\mathrm{SL}_n(A) = b\,\mathrm{SL}_n(A) \iff a^{-1}b \in \mathrm{SL}_n(A) \iff \det(a^{-1}\,b) = \det(a)^{-1} \cdot \det(b) = 1$$
$$\iff \det a = \det b.$$

De la misma manera,

$$\mathrm{SL}_n(A)\,a = \mathrm{SL}_n(A)\,b \iff ab^{-1} \in \mathrm{SL}_n(A) \iff \det(a\,b^{-1}) = \det(a) \cdot \det(b)^{-1} = 1$$
$$\iff \det a = \det b.$$

Entonces, las clases laterales izquierdas y derechas coinciden:

$$a\,\mathrm{SL}_n(A) = \mathrm{SL}_n(A)\,a \quad \text{para todo } a \in \mathrm{GL}_n(A),$$

y corresponden a las matrices de determinante fijo:

$$M_c = \{a \in \mathrm{GL}_n(A) \mid \det a = c\} \quad \text{para algún } c \in A^\times.$$ ▲

7.4.10. Ejemplo. Para el grupo simétrico $G = S_n$ y el grupo alternante $H = A_n$ tenemos

$$\sigma\,A_n = \tau\,A_n \iff \sigma^{-1}\tau \in A_n \iff \operatorname{sgn}(\sigma^{-1}\tau) = 1 \iff \operatorname{sgn}\sigma = \operatorname{sgn}\tau,$$

y de la misma manera,

$$A_n\,\sigma = A_n\,\tau \iff \sigma\,\tau^{-1} \in A_n \iff \operatorname{sgn}(\sigma\,\tau^{-1}) = 1 \iff \operatorname{sgn}\sigma = \operatorname{sgn}\tau.$$

Entonces, $\sigma\,A_n = A_n\,\sigma$, y hay solamente dos clases laterales: una formada por las permutaciones pares y la otra por las permutaciones impares:

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\}, \quad (1\ 2)\,A_n = A_n\,(1\ 2) = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = -1\}.$$

Notamos que esto demuestra que $|A_n| = n!/2$. ▲

7.4.11. Ejemplo. El mismo razonamiento demuestra que para el grupo $\mathbb{R}^\times$ y el subgrupo $\mathbb{R}_{>0}$ hay dos clases laterales:

$$\mathbb{R}_{>0} = \{x \in \mathbb{R}^\times \mid x > 0\}, \quad -1 \cdot \mathbb{R}_{>0} = \mathbb{R}_{<0} = \{x \in \mathbb{R}^\times \mid x < 0\}.$$ ▲

7.5 Teorema de Lagrange

7.5.1. Definición. Si la cardinalidad $|G/H| = |H\backslash G|$ es finita, este número se llama el **índice** de H en G y se denota por $|G : H|$.

7.5.2. Ejemplo. Tenemos $|S_n : A_n| = 2$ y $|\mathbb{R}^\times : \mathbb{R}_{>0}| = 2$. Note en particular que un grupo infinito puede tener subgrupos de índice finito. ▲

7.5.3. Proposición (Teorema de Lagrange). *Si G es un grupo finito y H es su subgrupo, entonces*

$$|G| = |G : H| \cdot |H|.$$

Demostración. G se descompone en una unión disjunta de clases de equivalencia. En total hay $|G : H|$ clases de equivalencia y cada una tiene $|H|$ elementos como vimos en 7.4.5. ■

7.5.4. Corolario. *Si G es un grupo finito y $H \subset G$ es un subgrupo, entonces $|G|$ es divisible por $|H|$.*

7.5.5. Ejemplo. En el capítulo anterior hemos visto que un grupo cíclico de orden n tiene precisamente un subgrupo de orden d para cada $d \mid n$. ▲

7.5.6. Corolario. *Si G es un grupo finito, entonces el orden de todo elemento $g \in G$ divide a $|G|$.*

Demostración. El orden de g es el orden del subgrupo $\langle g \rangle$ generado por g. ■

7.5.7. Corolario. *Si $|G| = n$, entonces $g^n = 1$ para todo $g \in G$.*

Demostración. Se sigue del hecho de que el orden de todo $g \in G$ divide a $|G|$. ■

7.5.8. Ejemplo. Para el anillo $\mathbb{Z}/n\mathbb{Z}$ el grupo de unidades viene dado por

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \operatorname{mcd}(a, n) = 1\}.$$

Su cardinalidad es la función ϕ de Euler:

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n).$$

Entonces, se tiene

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{si } \operatorname{mcd}(a, n) = 1.$$

Esta congruencia se conoce como el **teorema de Euler**. En particular, si $n = p$ es primo, se obtiene el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{si } p \nmid a.$$ ▲

7.5.9. Corolario. *Todo grupo de orden primo p es cíclico.*

Demostración. Si $|G| = p$, entonces los subgrupos de G son de orden 1 o $|G|$; es decir, G no tiene subgrupos propios. Sea $g \in G$ un elemento tal que $g \neq 1$. Entonces $\langle g \rangle \neq \{1\}$, y por lo tanto $\langle g \rangle = G$. ■

7.5.10. Ejemplo. Para el grupo alternante A_4 tenemos $|A_4| = 4!/2 = 12$, así que los subgrupos necesariamente tienen orden $1, 2, 3, 4, 6, 12$. Cada subgrupo de orden 2 es de la forma $\{\mathrm{id}, \sigma\}$ donde $\operatorname{ord}\sigma = 2$. En este caso los elementos de orden 2 son productos de dos transposiciones disjuntas. Tenemos entonces los siguientes tres subgrupos de orden 2:

$$\langle (1\,2)\,(3\,4) \rangle, \quad \langle (1\,3)\,(2\,4) \rangle, \quad \langle (1\,4)\,(2\,3) \rangle.$$

Cada subgrupo de orden 3 es cíclico, generado por un elemento de orden 3, en este caso un 3-ciclo. Tenemos los siguientes cuatro subgrupos de orden 3:

$$\langle (1\,2\,3) \rangle = \langle (1\,3\,2) \rangle, \quad \langle (1\,2\,4) \rangle = \langle (1\,4\,2) \rangle, \quad \langle (1\,3\,4) \rangle = \langle (1\,4\,3) \rangle, \quad \langle (2\,3\,4) \rangle = \langle (2\,4\,3) \rangle.$$

Ahora si $H \subset A_4$ es un subgrupo de orden 4, sus elementos necesariamente tienen orden 2 o 4. En A_4 no hay elementos de orden 4, y la única opción que nos queda es de considerar todos los tres elementos de orden 2 junto con la permutación identidad:

$$V = \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}.$$

Se ve que este es un subgrupo. El grupo V se conoce como el **grupo de cuatro** (*Vierergruppe* en alemán) o el **grupo de Klein**. Este grupo es abeliano.

$\circ$	id	$(1\ 2)\,(3\ 4)$	$(1\ 3)\,(2\ 4)$	$(1\ 4)\,(2\ 3)$
id	id	$(1\ 2)\,(3\ 4)$	$(1\ 3)\,(2\ 4)$	$(1\ 4)\,(2\ 3)$
$(1\ 2)\,(3\ 4)$	$(1\ 2)\,(3\ 4)$	id	$(1\ 4)\,(2\ 3)$	$(1\ 3)\,(2\ 4)$
$(1\ 3)\,(2\ 4)$	$(1\ 3)\,(2\ 4)$	$(1\ 4)\,(2\ 3)$	id	$(1\ 2)\,(3\ 4)$
$(1\ 4)\,(2\ 3)$	$(1\ 4)\,(2\ 3)$	$(1\ 3)\,(2\ 4)$	$(1\ 2)\,(3\ 4)$	id

De hecho, es fácil verificar que todo grupo de orden 4 es cíclico (y entonces es isomorfo a $\mathbb{Z}/4\mathbb{Z}$), o isomorfo a V; haga el ejercicio 7.1.

En fin, si $H \subset A_4$ es un subgrupo de orden 6, sus elementos necesariamente tienen orden 2 o 3; es decir, son 3-ciclos o permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$. Junto con cada 3-ciclo H debe contener su inverso. Las posibles opciones son

$$\{\mathrm{id}, (a\ b\ c), (a\ c\ b), (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}$$

y

$$\{\mathrm{id}, (a\ b\ c), (a\ c\ b), (i\ j\ k), (i\ k\ j), (p\ q)\,(r\ s)\}.$$

Podemos descartar el primer caso: conjugando $(a\ b\ c)$ por una de las permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet)$ se obtiene otro 3-ciclo $(a'\ b'\ c') \neq (a\ b\ c), (a\ c\ b)$. De la misma manera, en el segundo caso, conjugando $(p\ q)\,(r\ s)$ por un 3-ciclo se obtiene $(p'\ q')\,(r'\ s') \neq (p\ q)\,(r\ s)$.

Podemos concluir que en A_4 no hay subgrupos de orden 6. Este ejemplo en particular demuestra que si $d \mid |G|$, entonces G no necesariamente tiene subgrupos de orden d. ▲

Terminemos esta sección por el siguiente resultado importante.

7.5.11. Proposición. *Sea k un cuerpo. Entonces, todo subgrupo finito de su grupo de unidades $k^\times$ es cíclico.*

Para demostrarlo, necesitamos el siguiente lema.

7.5.12. Lema. *Sea G un grupo de orden finito n. Supongamos que para todo $d \mid n$ se cumple*

$$\#\{x \in G \mid x^d = 1\} \leq d. \tag{7.1}$$

Entonces G es cíclico.

Demostración. Si G tiene un elemento g de orden d, entonces este genera el subgrupo $\langle g \rangle$ que es cíclico de orden d. Todo elemento $h \in G$ tal que $h^d = 1$ pertenece a este subgrupo gracias a la hipótesis (7.1), y si h tiene orden d, entonces es otro generador de $\langle g \rangle$. En total este subgrupo tiene $\phi(d)$ generadores. Entonces, el número de elementos de orden d es igual a 0 o $\phi(d)$. De hecho, el primer caso no es posible: la fórmula

$$\sum_{d \mid n} \phi(d) = n$$

demuestra que si para algún $d \mid n$ el grupo G no tiene elementos de orden d, entonces $|G| < n$. En particular, G debe tener un elemento de orden n y por lo tanto es cíclico. ■

Demostración de 7.5.11. Sobre un cuerpo, la ecuación polinomial $x^d - 1 = 0$ tiene como máximo d soluciones, y por lo tanto podemos aplicar el lema anterior. ■

7.5.13. Ejemplo. Para $k = \mathbb{R}$ los únicos elementos de orden finito en $\mathbb{R}^\times$ son ± 1. ▲

7.5.14. Ejemplo. Para $k = \mathbb{C}$ los elementos de orden finito en $\mathbb{C}^\times$ forman el subgrupo de las raíces de la unidad $\mu_\infty(\mathbb{C})$. El resultado de 7.5.11 nos dice que todos los subgrupos finitos de $\mathbb{C}^\times$ son cíclicos. Sin embargo, el grupo infinito $\mu_\infty(\mathbb{C})$ no es cíclico y de hecho no es finitamente generado. ▲

7.5.15. Ejemplo. Si $k = \mathbb{F}_q$ es un cuerpo finito entonces 7.5.11 implica que el grupo $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ es cíclico de orden $q-1$. Note que la demostración de 7.5.11 no es constructiva: un conteo implica que $\mathbb{F}_{p^k}^\times$ posee un generador, pero no dice cuál elemento particular es. En este sentido, aunque se puede escribir

$$\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z},$$

el grupo aditivo $\mathbb{Z}/(q-1)\mathbb{Z}$ tiene un generador distinguido $[1]$, mientras que para $\mathbb{F}_q^\times$ no está claro cuál generador hay que escoger (y hay $\phi(q-1)$ posibilidades). El isomorfismo de arriba dependería de esta elección.

Para dar un ejemplo particular, el grupo $\mathbb{F}_4^\times$ es cíclico de orden 3 y puede ser escrito como

$$\mathbb{F}_4^\times = \{1, a, a^2\}$$

donde a es un generador y a^2 sería el otro generador. Luego la tabla de adición en $\mathbb{F}_4$ viene dada por

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

Note que este grupo es isomorfo al grupo V. ▲

7.5.16. Ejemplo. Para el cuerpo $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, el grupo

$$\mathbb{F}_5^\times = \{[1], [2], [3], [4]\}$$

es cíclico. Sus generadores son $[2]$ y $[3]$: tenemos

$$2^2 \equiv 4 \pmod 5, \quad 2^3 \equiv 3 \pmod 5, \quad 2^4 \equiv 1 \pmod 5$$

y

$$3^2 \equiv 4 \pmod 5, \quad 3^3 \equiv 2 \pmod 5, \quad 3^4 \equiv 1 \pmod 5.$$ ▲

7.5.17. Ejemplo. El anillo cociente $k := \mathbb{F}_2[x]/(x^3+x+1)$ es un cuerpo de 8 elementos, dado que el polinomio x^3+x+1 es irreducible en $\mathbb{F}_2[x]$. Entonces, $k^\times$ es un grupo cíclico de 7 elementos. Este tiene 6 generadores; es decir, como generador se puede tomar cualquier polinomio entre

$$\overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}.$$

Por ejemplo, tenemos

$$k^\times = \{1, \overline{x}, \overline{x}^2, \overline{x}^3 = \overline{x+1}, \overline{x}^4 = \overline{x^2+x}, \overline{x}^5 = \overline{x^2+x+1}, \overline{x}^6 = \overline{x^2+1}\}.$$ ▲

7.5.18. Ejemplo. El anillo cociente $k := \mathbb{F}_3[x]/(x^2+1)$ es un cuerpo de 9 elementos, dado que el polinomio x^2+1 es irreducible en $\mathbb{F}_3[x]$. Entonces, $k^\times$ es un grupo cíclico de 8 elementos, y $\phi(8) = 4$ son sus generadores. Dejo al lector verificar cuáles elementos entre

$$\overline{x}, \overline{x}+1, \overline{x}+2, 2\overline{x}, 2\overline{x}+1, 2\overline{x}+2$$

generan a $k^\times$. ▲

7.6 Grupos cociente

Si G no es abeliano y $H \subset G$ es un subgrupo, en general tenemos $gH \neq Hg$. Cuando esto se cumple, se dice que H es un subgrupo normal. Esto también puede ser formulado en términos de **conjugación**. Cuando para dos elementos h y h' se cumple $h' = g\,h\,g^{-1}$ para algún $g \in G$, se dice que h y h' son **conjugados**, o que h' es el resultado de la **conjugación de** h **por** g.

7.6.1. Definición (Galois, 1832). Sea G un grupo y $H \subset G$ un subgrupo. Se dice que H es **normal** si se cumple una de las propiedades equivalentes:

1) toda clase lateral izquierda coincide con la clase lateral derecha correspondiente:

$$gH = Hg \quad \text{para todo } g \in G;$$

2) la conjugación de H por los elementos de G coincide con H:

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\} = H \quad \text{para todo } g \in G;$$

3) una variación de 2):

$$ghg^{-1} \in H \quad \text{para todo } g \in G \text{ y } h \in H.$$

La equivalencia de 1) y 2) está clara. La condición 3) significa que $gHg^{-1} \subseteq H$ para todo $g \in G$ y por lo tanto 2) implica 3). Por fin, si se cumple 3), entonces para cualesquiera g y h tenemos $g^{-1}hg \in H$, y luego $g\,(g^{-1}hg)\,g^{-1} = h$, lo que implica $H \subseteq gHg^{-1}$. Entonces, 3) implica 2).

Cuidado: si tenemos una cadena de subgrupos

$$K \subset H \subset G$$

y K es normal en H, esto no quiere decir que K es normal en G.

7.6.2. Observación. *Para una familia de subgrupos normales $H_i \subseteq G$ la intersección $\bigcap_i H_i$ es también un subgrupo normal.* □

7.6.3. Ejemplo. Si G es un grupo abeliano, todo subgrupo es normal. ▲

7.6.4. Ejemplo. Los subgrupos $\{1\}$ y G son normales. ▲

7.6.5. Ejemplo. En el grupo simétrico S_3 hay 3 subgrupos de orden 2 que corresponden a las transposiciones:

$$\langle(1\ 2)\rangle,\ \langle(1\ 3)\rangle,\ \langle(2\ 3)\rangle.$$

Luego, tenemos el grupo alternante, que es el único subgrupo de orden 3:

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}.$$

El subgrupo A_3 es normal, ya que para todo $\tau \in S_3$, si σ es un 3-ciclo, entonces $\tau\sigma\tau^{-1}$ es también un 3-ciclo. Las relaciones

$$(1\ 3)\,(1\ 2)\,(1\ 3)^{-1} = (2\ 3),$$
$$(1\ 2)\,(1\ 3)\,(1\ 2)^{-1} = (2\ 3),$$
$$(1\ 2)\,(2\ 3)\,(1\ 2)^{-1} = (1\ 3)$$

demuestran que los subgrupos de orden 2 no son normales. ▲

7.6.6. Ejemplo. De nuestra descripción de los subgrupos del grupo alternante A_4 en 7.5.10 se ve que el único subgrupo normal (salvo 1 y el mismo A_4) es

$$V = \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}.$$ ▲

7.6.7. Ejemplo. El subgrupo de S_n

$$H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$$

considerado en 7.4.7 no es normal para $n \geq 3$, puesto que $\sigma H = H\sigma$ solo para $\sigma = \mathrm{id}$. ▲

7.6.8. Observación. *Para todo grupo G su centro $Z(G)$ es un subgrupo normal.*

Demostración. Tenemos

$$Z(G) := \{x \in G \mid xg = gx \text{ para todo } g \in G\} = \{x \in G \mid x = gxg^{-1} \text{ para todo } g \in G\},$$

y en particular, para todo $g \in G$ tenemos

$$gZ(G)g^{-1} = Z(G).$$ ■

7.6.9. Observación. *Para todo homomorfismo $\phi\colon G \to H$ el núcleo $\ker\phi$ es un subgrupo normal de G.*

Demostración. Para todo $g \in G$ y $k \in \ker\phi$ tenemos

$$\phi(g\,k\,g^{-1}) = \phi(g)\cdot\phi(k)\cdot\phi(g)^{-1} = \phi(g)\cdot\phi(g)^{-1} = 1,$$

así que $g\cdot(\ker\phi)\cdot g^{-1} \subseteq \ker\phi$. ■

7.6.10. Ejemplo. A_n es un subgrupo normal de S_n, siendo el núcleo del homomorfismo $\mathrm{sgn}\colon S_n \to \{\pm 1\}$. ▲

7.6.11. Ejemplo. $\mathrm{SL}_n(R)$ es un subgrupo normal de $\mathrm{GL}_n(R)$, siendo el núcleo del homomorfismo $\det\colon \mathrm{GL}_n(R) \to R^\times$. ▲

7.6.12. Ejemplo. El signo de un número real es un homomorfismo $\mathrm{sgn}\colon \mathbb{R}^\times \to \{\pm 1\}$. Consideremos el homomorfismo

$$\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm 1\}.$$

Su núcleo es el subgrupo normal

$$\mathrm{GL}_n(\mathbb{R})^+ := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A > 0\}.$$ ▲

7.6.13. Comentario. A diferencia del núcleo $\ker\phi \subset G$, la imagen $\mathrm{im}\,\phi \subset H$ de un homomorfismo $\phi\colon G \to H$ en general no es un subgrupo normal. De hecho, si $K \subset H$ no es un subgrupo normal, entonces la inclusión $i\colon K \rightarrowtail H$ tiene K como su imagen. En los grupos abelianos, todos subgrupos son normales, así que si $\phi\colon A \to B$ es un homomorfismo de grupos abelianos, entonces $\mathrm{im}\,\phi \subset B$ es un subgrupo normal. Es una diferencia fundamental entre los grupos abelianos y no abelianos.

El siguiente resultado explica el significado de la noción de subgrupo normal. La normalidad de $H \subset G$ significa precisamente que la multiplicación en G es compatible con la relación de equivalencia módulo H.

7.6.14. Proposición. *Sea $H \subset G$ un subgrupo. Para cualesquiera $g_1, g_1', g_2, g_2' \in G$ se tiene*

$$g_1 \equiv g_1' \pmod{H},\quad g_2 \equiv g_2' \pmod{H} \implies g_1 g_2 \equiv g_1' g_2' \pmod{H} \tag{7.2}$$

si y solamente si H es normal.

Demostración. Recordemos que por la definición de la relación de equivalencia módulo H, la condición (7.2) nos dice que para cualesquiera $g_1, g_1', g_2, g_2' \in G$

$$g_1' \in g_1 H, \quad g_2' \in g_2 H \quad \Longrightarrow \quad g_1 g_2 \equiv g_1' g_2' \pmod{H}.$$

Es decir, para cualesquiera $g_1, g_2 \in G$, $h_1, h_2 \in H$

$$g_1 g_2 \equiv (g_1 h_1)(g_2 h_2) \pmod{H},$$

los que es equivalente a

$$(g_1 g_2)^{-1} (g_1 h_1)(g_2 h_2) \in H$$

Luego,

$$(g_1 g_2)^{-1} (g_1 h_1)(g_2 h_2) = g_2^{-1} h_1 g_2 h_2,$$

entonces la condición es

$$g_2^{-1} h_1 g_2 \in H.$$

Esto es equivalente a la normalidad de H. ■

7.6.15. Definición. Si $H \subset G$ es un subgrupo normal, entonces el **grupo cociente** correspondiente es el conjunto de las clases laterales G/H junto con la operación

$$g_1 H \cdot g_2 H = (g_1 g_2) H.$$

En otras palabras, el producto de las clases de equivalencia de g_1 y g_2 módulo H es la clase de equivalencia de $g_1 g_2$.

Como acabamos de ver, la fórmula de arriba tiene sentido: si H es normal, entonces la clase lateral $(g_1 g_2)H$ no depende de g_1 y g_2, sino de las clases laterales $g_1 H$ y $g_2 H$. Esta operación es asociativa, puesto que la operación en G lo es; la identidad en G/H es la clase lateral $1H = H$; los inversos vienen dados por $(gH)^{-1} = g^{-1} H$.

Por la definición del producto en el grupo cociente, se tiene un homomorfismo sobreyectivo

$$\pi \colon G \to G/H, \quad g \mapsto gH.$$

Notamos que $\ker \pi = H$. A veces en lugar de "gH" se escribe "$\overline{g}$" o "$[g]$", dado que se trata de las clases de equivalencia módulo H.

7.6.16. Ejemplo. Si A es un anillo y $\mathfrak{a} \subset A$ un ideal, entonces por la definición, el anillo cociente $A/\mathfrak{a}$ respecto a la adición es el cociente del grupo aditivo A por el subgrupo $\mathfrak{a}$.

Un caso muy particular de esta situación son los grupos $\mathbb{Z}/n\mathbb{Z}$. ▲

7.6.17. Ejemplo. En el grupo alternante A_4 el único subgrupo normal propio es V. Tenemos

$$|A_4/V| = |A_4|/|V| = \frac{4!/2}{4} = 3,$$

así que $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$ (todo grupo de orden primo es cíclico). En efecto, en este caso las tres clases laterales son

$$\begin{aligned} V &= \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}, \\ (1\,2\,3)\,V &= \{(1\,2\,3), (1\,3\,4), (2\,4\,3), (1\,4\,2)\}, \\ (1\,3\,2)\,V &= \{(1\,3\,2), (2\,3\,4), (1\,2\,4), (1\,4\,3)\}. \end{aligned}$$

Tenemos la siguiente tabla de multiplicación módulo V.

$\circ$	id	(1 2 3)	(1 3 2)
id	id	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	id	(1 2 3)

▲

7.6.18. Ejemplo. En el grupo de cuaterniones Q_8 el subgrupo $\{\pm 1\}$ es normal. El cociente $Q_8/\{\pm 1\}$ es un grupo de orden 4 que no es cíclico, así que es isomorfo al grupo V (véase el ejercicio 7.1). Específicamente, la tabla de multiplicación en $Q_8/\{\pm 1\}$ viene dada por

$\cdot$	$\overline{1}$	$\overline{I}$	$\overline{J}$	$\overline{K}$
$\overline{1}$	$\overline{1}$	$\overline{I}$	$\overline{J}$	$\overline{K}$
$\overline{I}$	$\overline{I}$	$\overline{1}$	$\overline{K}$	$\overline{J}$
$\overline{J}$	$\overline{J}$	$\overline{K}$	$\overline{1}$	$\overline{I}$
$\overline{K}$	$\overline{K}$	$\overline{J}$	$\overline{I}$	$\overline{1}$

Esta es la multiplicación habitual de cuaterniones, solo hemos olvidado los signos ± 1 (por este motivo el producto se volvió conmutativo). ▲

7.7 Primer teorema de isomorfía

El siguiente resultado es análogo al teorema de isomorfía para anillos conmutativos que hemos probado en el capítulo 4.

7.7.1. Proposición (Primer teorema de isomorfía). *Todo homomorfismo de grupos $\phi\colon G \to H$ induce un isomorfismo canónico*

$$\begin{aligned} \overline{\phi}\colon G/\ker\phi &\xrightarrow{\cong} \operatorname{im}\phi, \\ g\cdot\ker\phi &\mapsto \phi(g). \end{aligned}$$

Demostración. Primero notamos que la aplicación $\overline{\phi}$ está bien definida:

$$g_1\cdot\ker\phi = g_2\cdot\ker\phi \iff g_1^{-1}g_2 \in \ker\phi \iff \phi(g_1) = \phi(g_2).$$

Esta verificación también establece que la aplicación $\overline{\phi}$ es inyectiva. Es sobreyectiva por la definición. En fin, $\overline{\phi}$ es un homomorfismo, dado que ϕ lo es. ■

También hay segundo y tercer teorema de isomorfía, pero los vamos a ver en los ejercicios.

7.7.2. Corolario. *Si G es un grupo finito, entonces para todo homomorfismo $f\colon G \to H$ tenemos*

$$|G| = |\operatorname{im} f|\cdot|\ker f|.$$

7.7.3. Comentario. El último resultado es un análogo de la fórmula

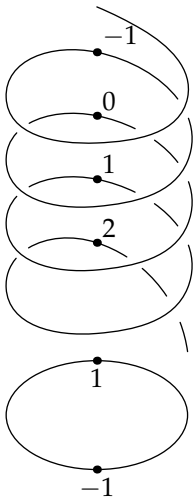
$$\dim_k U = \dim_k(\operatorname{im} f) + \dim_k(\ker f)$$

que tenemos para una aplicación lineal $f\colon U \to V$, donde U es un k-espacio vectorial de dimensión finita.

7.7.4. Ejemplo. Compilemos una tabla con ejemplos familiares de homomorfismos.

homomorfismo	núcleo	imagen	isomorfismo
$\mathbb{R}^\times \xrightarrow{x\mapsto\lvert x\rvert} \mathbb{R}_{>0}$	$\{\pm 1\}$	$\mathbb{R}_{>0}$	$\mathbb{R}^\times/\{\pm1\} \cong \mathbb{R}_{>0}$
$\mathbb{C}^\times \xrightarrow{z\mapsto z^n} \mathbb{C}^\times$	$\mu_n(\mathbb{C})$	$\mathbb{C}^\times$	$\mathbb{C}^\times/\mu_n(\mathbb{C}) \cong \mathbb{C}^\times$
$\mathbb{R} \xrightarrow{x\mapsto e^{2\pi i x}} \mathbb{C}^\times$	$\mathbb{Z}$	$\mathbb{S}^1$	$\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$
$\mathbb{Q} \xrightarrow{x\mapsto e^{2\pi i x}} \mathbb{C}^\times$	$\mathbb{Z}$	$\mu_\infty(\mathbb{C})$	$\mathbb{Q}/\mathbb{Z} \cong \mu_\infty(\mathbb{C})$
$\mathrm{GL}_n(R) \xrightarrow{\det} R^\times$	$\mathrm{SL}_n(R)$	$R^\times$	$\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \cong R^\times$
$\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm1\}$	$\mathrm{GL}_n(\mathbb{R})^+$	$\{\pm1\}$	$\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{R})^+ \cong \{\pm1\}$
$S_n \xrightarrow{\mathrm{sgn}} \{\pm1\}$	A_n	$\{\pm1\}$	$S_n/A_n \cong \{\pm1\}$
$\mathbb{C}^\times \xrightarrow{z\mapsto\lvert z\rvert} \mathbb{R}_{>0}$	$\mathbb{S}^1$	$\mathbb{R}_{>0}$	$\mathbb{C}^\times/\mathbb{S}^1 \cong \mathbb{R}_{>0}$
$\mathbb{C}^\times \xrightarrow{z\mapsto z/\lvert z\rvert} \mathbb{S}^1$	$\mathbb{R}_{>0}$	$\mathbb{S}^1$	$\mathbb{C}^\times/\mathbb{R}_{>0} \cong \mathbb{S}^1$

En el isomorfismo $R/\mathbb{Z} \cong \mathbb{S}^1$ la aplicación $x \mapsto e^{2\pi i x}$ puede ser visualizada como una hélice que se proyecta al círculo:



Los isomorfismos $\mathbb{C}^\times/\mathbb{S}^1 \cong \mathbb{R}_{>0}$ y $\mathbb{C}^\times/\mathbb{R}_{>0} \cong \mathbb{S}^1$ vienen nada más de la representación canónica de un número complejo $z = r\,e^{i\phi}$ donde $r \in \mathbb{R}_{>0}$ y $0 \le \phi < 2\pi$.

Cuidado: $\mathbb{Q}/\mathbb{Z}$ y $\mathbb{R}/\mathbb{Z}$ de arriba son *grupos cociente*, no son anillos cociente: $\mathbb{Z}$ es un subgrupo aditivo en $\mathbb{Q}$ y $\mathbb{R}$, pero no es un ideal. ▲

7.7.5. Ejemplo. Sea p un primo impar. Consideremos el homomorfismo dado por el símbolo de Legendre

$$\left(\frac{\cdot}{p}\right)\colon \mathbb{F}_p^\times \to \{\pm1\}.$$

Este homomorfismo es sobreyectivo: en $\mathbb{F}_p^\times$ hay por lo menos un cuadrado y un no-cuadrado. El núcleo consiste en el subgrupo de cuadrados

$$(\mathbb{F}_p^\times)^2 := \{a^2 \mid a \in \mathbb{F}_p^\times\}.$$

El primer teorema de isomorfía nos dice entonces que

$$\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm1\}.$$ ▲

7.7.6. Ejemplo. Para dar un ejemplo más interesante, consideremos el grupo simétrico S_4 y el subgrupo

$$V := \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Este subgrupo es normal: para todo $\sigma \in S_4$ se tiene

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

Calculemos entonces el grupo cociente S_4/V. Notamos que

$$|S_4/V| = |S_4|/|V| = 24/4 = 6.$$

Salvo isomorfismo, existen dos grupos de orden 6: el grupo cíclico $\mathbb{Z}/6\mathbb{Z}$ y el grupo simétrico S_3 (véase el ejercicio 7.2). En este caso el cociente no puede ser cíclico, así que es isomorfo a S_3. A saber, para que S_4/V sea cíclico, necesitamos un elemento de orden 6, que correspondería a una permutación $\sigma \in S_4$ tal que

$$\sigma \notin V, \sigma^2 \notin V, \sigma^3 \notin V, \sigma^4 \notin V, \sigma^5 \notin V, \sigma^6 \in V.$$

Sin embargo, toda permutación $\sigma \in S_4$ tiene orden ≤ 4, así que esto es imposible.

Para dar un isomorfismo explícito $S_4/V \cong S_3$, podemos encontrar un homomorfismo sobreyectivo $\phi\colon S_4 \to S_3$ que tiene V como su núcleo. Notamos que hay tres diferentes particiones del conjunto $\{1,2,3,4\}$ en dos conjuntos de 2 elementos:

$$A = \{\{1,2\},\{3,4\}\},\quad B = \{\{1,3\},\{2,4\}\},\quad C = \{\{1,4\},\{2,3\}\}.$$

Ahora una permutación $\sigma \in S_4$ envía cada una de las particiones

$$\{\{i,j\},\{k,\ell\}\}$$

a una partición

$$\{\{\sigma(i),\sigma(j)\},\{\sigma(k),\sigma(\ell)\}\}.$$

Esto define un homomorfismo

$$\phi\colon S_{\{1,2,3,4\}} \to S_{\{A,B,C\}}.$$

Por ejemplo, a la permutación $(1\ 4)$ corresponde

$$A \mapsto \{\{4,2\},\{3,1\}\} = B,\quad B \mapsto \{\{4,3\},\{2,1\}\} = A,\quad C \mapsto \{\{4,1\},\{2,3\}\} = C,$$

así que

$$\phi(1\ 4) = (A\ B).$$

De la misma manera, a la permutación $(1\ 2\ 4)$ corresponde

$$A \mapsto \{\{2,4\},\{3,1\}\} = B,\quad B \mapsto \{\{2,3\},\{4,1\}\} = C,\quad C \mapsto \{\{2,1\},\{4,3\}\} = A,$$

y luego

$$\phi(1\ 2\ 4) = (A\ B\ C).$$

Dado que en la imagen de ϕ están las permutaciones $(A\ B)$ y $(A\ B\ C)$, podemos concluir que ϕ es un homomorfismo sobreyectivo (una transposición y un 3-ciclo generan S_3). El núcleo de ϕ consiste en las permutaciones que preservan las particiones A, B, C, y no es difícil ver que

$$\ker\phi = V.$$

Entonces, ϕ induce un isomorfismo

$$\begin{aligned}\overline{\phi}\colon S_4/V &\to S_{\{A,B,C\}},\\ \sigma V &\mapsto \phi(\sigma).\end{aligned}$$

Las seis clases laterales en S_4/V son las siguientes:

$$\begin{aligned}
V &= \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},\\
(1\,2)\,V &= \{(1\,2), (3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\},\\
(1\,3)\,V &= \{(1\,3), (1\,2\,3\,4), (2\,4), (1\,4\,3\,2)\},\\
(1\,4)\,V &= \{(1\,4), (1\,2\,4\,3), (1\,3\,4\,2), (2\,3)\},\\
(1\,2\,3)\,V &= \{(1\,2\,3), (1\,3\,4), (2\,4\,3), (1\,4\,2)\},\\
(1\,2\,4)\,V &= \{(1\,2\,4), (1\,4\,3), (1\,3\,2), (2\,3\,4)\}.
\end{aligned}$$

Entonces, el isomorfismo en cuestión viene dado por

$$\begin{aligned}
\mathrm{id}\,V &\mapsto \mathrm{id},\\
(1\,2)\,V &\mapsto (B\ C),\\
(1\,3)\,V &\mapsto (A\ C),\\
(1\,4)\,V &\mapsto (A\ B),\\
(1\,2\,3)\,V &\mapsto (A\ C\ B),\\
(1\,2\,4)\,V &\mapsto (A\ B\ C).
\end{aligned}$$

▲

7.7.7. Ejemplo. En el capítulo anterior hemos contado el número de matrices invertibles de $n \times n$ con coeficientes en un cuerpo finito $\mathbb{F}_q$:

$$\#\mathrm{GL}_n(\mathbb{F}_q) = (q^n - 1)\cdot(q^n - q)\cdots(q^n - q^{n-1}).$$

Ahora gracias al isomorfismo $\mathrm{GL}_n(\mathbb{F}_q)/\mathrm{SL}_n(\mathbb{F}_q) \cong \mathbb{F}_q^\times$, sabemos que

$$|\mathrm{SL}_n(\mathbb{F}_q)| = \frac{1}{|\mathbb{F}_q^\times|}\cdot|\mathrm{GL}_n(\mathbb{F}_q)| = \frac{1}{q-1}(q^n - 1)\cdot(q^n - q)\cdots(q^n - q^{n-1}).$$

▲

7.7.8. Ejemplo (Subrupos de congruencia principales). Para $n = 2,3,4,5,\ldots$ consideremos la aplicación

$$\phi\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$$

que reduce módulo n los coeficientes de una matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Es fácil verificar que se trata de un homomorfismo de grupos (esencialmente porque la reducción módulo n es un homomorfismo $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$). Este homomorfismo es sobreyectivo.

A saber, una matriz en $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ se representa por una matriz con coeficientes enteros

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \quad \text{tal que } ad - bc \equiv 1 \pmod{n}.$$

La sobreyectividad de ϕ quiere decir que existe una matriz $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tal que

$$a' \equiv a,\ b' \equiv b,\ c' \equiv c,\ d' \equiv d \pmod{n}.$$

Hay que trabajar un poco para probarlo.

1) Primero notamos que c y d son **coprimos módulo** n en el sentido de que si para algún $\alpha \in \mathbb{Z}$ se cumple $\alpha c \equiv \alpha d \equiv 0 \pmod{n}$, entonces $\alpha \equiv 0 \pmod{n}$. En efecto, en este caso tenemos

$$a(\alpha d) - b(\alpha c) \equiv \alpha \pmod{n}.$$

2) Ahora probemos el siguiente lema aritmético: *si c y d son coprimos módulo n, entonces existen $c', d' \in \mathbb{Z}$ tales que*

$$c' \equiv c,\ d' \equiv d \pmod{n}, \quad \operatorname{mcd}(c', d') = 1.$$

En efecto, uno de los números c y d debe ser distinto de cero. Sin pérdida de generalidad, $d \neq 0$. Por el teorema chino del resto, existe $\alpha \in \mathbb{Z}$ tal que para todo divisor primo $p \mid d$ se tiene

$$\alpha \equiv \begin{cases} 0, & p \nmid c, \\ 1, & p \mid c \end{cases} \pmod{p}$$

Ahora notamos que

$$\operatorname{mcd}(c + \alpha n, d) = 1.$$

De hecho, si $p \mid d$, entonces $p \nmid (c + \alpha n)$. Para verlo, analicemos los siguientes dos casos.

- Si $p \mid c$, entonces $c + \alpha n \equiv c + n \pmod{p}$ por la elección de α, pero $p \nmid n$, dado que c y d son coprimos módulo n.
- Si $p \nmid c$, entonces $c + \alpha n \equiv c \pmod{p}$.

Entonces, podemos remplazar (c, d) por $(c', d') = (c + \alpha n, d)$.

3) Ahora bien, según lo que acabamos de ver, una matriz en $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ puede ser representada por

$$\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}, \quad \text{donde } \operatorname{mcd}(c', d') = 1, \quad ad' - bc' \equiv 1 \pmod{n}.$$

Tenemos la identidad de Bézout

$$\alpha c' + \beta d' = 1.$$

Ahora para algún $k \in \mathbb{Z}$ se tiene

$$ad' - bc' = 1 + nk,$$

y entonces

$$ad' - bc' - nk = ad' - bc' - nk(\alpha c' + \beta d') = 1.$$

Podemos escribir esta identidad como

$$(a - nk\beta)\, d' - (b + nk\alpha)\, c' = 1.$$

Entonces, remplazando (a, b) por

$$(a', b') = (a - nk\beta,\ b + nk\alpha)$$

se obtiene una matriz

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{tal que } \phi \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Notamos que también se puede considerar el homomorfismo $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, pero este no será sobreyectivo: toda matriz en $\mathrm{GL}_2(\mathbb{Z})$ tiene determinante ± 1, así que su imagen en $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ necesariamente tiene determinante $\pm 1 \pmod{n}$. Así que basta tomar, por ejemplo, $n = 5$ y una matriz en $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ de determinante 2 o 3, como por ejemplo $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

Ahora bien, $\phi\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ es un homomorfismo sobreyectivo, y podemos considerar su núcleo:

$$\Gamma(n) := \ker \phi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod{n} \right\}.$$

Por el primer teorema de isomorfía, se tiene

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(n) \cong \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Notamos que si $n = p$ es primo, entonces ya sabemos que

$$|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{1}{p-1}(p^2-1)(p^2-p) = (p^2-1)\,p.$$

En general, si n es compuesto, tenemos los siguientes valores:

n:	2	3	4	5	6	7	8	9	10	11
$\lvert\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\rvert$:	6	24	48	120	144	336	384	648	720	1320

Véase https://oeis.org/A000056 ▲

7.7.9. Ejemplo. Gracias al isomorfismo $S_n/A_n \cong \{\pm 1\}$, sabemos que

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$ ▲

7.8 Subgrupos en el cociente

Para los subgrupos en el grupo cociente G/H existe una descripción muy parecida a la descripción de ideales en el anillo cociente $A/\mathfrak{a}$ que hemos visto en el capítulo 4.

7.8.1. Lema. *Sea $\phi\colon G \to H$ un homomorfismo de grupos.*

1) *Si $G' \subseteq G$ es un subgrupo, entonces $\phi(G')$ es un subgrupo de H.*
   Además, si ϕ es sobreyectivo y G' es un subgrupo normal, entonces $\phi(G')$ es también normal.
2) *Si $H' \subseteq H$ es un sugrupo, entonces $\phi^{-1}(H')$ es un subgrupo de G.*
   Además, si H' es normal, entonces $\phi^{-1}(H')$ es también normal. □

7.8.2. Teorema. *Sean G un grupo y $H \subseteq G$ un subgrupo normal. Hay una biyección natural entre los subgrupos de G/H y los subgrupos de G que contienen a H. Esta biyección preserva las inclusiones. A saber, si $\pi\colon G \to G/H$ es la proyección canónica, entonces la biyección viene dada por*

$$H \subseteq K \subseteq G \mapsto \pi(K),$$
$$\pi^{-1}(\overline{K}) \mapsfrom \overline{K} \subseteq G/H.$$

Bajo esta correspondencia, los subgrupos normales corresponden a subgrupos normales.

Demostración. Dado que $\pi\colon G \to G/H$ es un homomorfismo, las preimagenes e imagenes de subgrupos respecto a π son también subgrupos. Notamos que si $\overline{K}$ es un subgrupo de G/H, entonces

$$H = \pi^{-1}(1) \subseteq \pi^{-1}(\overline{K}).$$

Podemos concluir que las aplicaciones de arriba están bien definidas. Son mutualmente inversas: claramente, $\pi(\pi^{-1}(\overline{K})) = \overline{K}$, y luego,

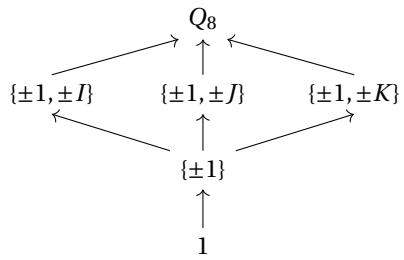
$$\pi^{-1}(\pi(K)) = \{g \in G \mid \pi(g) \in \pi(K)\} = \{g \in G \mid \pi(g) = \pi(k) \text{ para algún } k \in K\}$$
$$= \{g \in G \mid g\,k^{-1} \in \ker\pi = H \text{ para algún } k \in K\} = K$$

(usando que $K \supseteq H$). ■

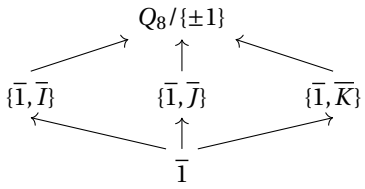
7.8.3. Ejemplo. Volvamos al ejemplo 7.6.18 donde hemos observado que

$$Q_8/\{\pm 1\} \cong V.$$

En general, el grupo de cuaterniones tiene los siguientes subgrupos.



Todos los subgrupos de Q_8 son normales. La estructura de subgrupos en $Q_8/\{\pm 1\} \cong V$ es la siguiente.



▲

7.8.4. Ejemplo. Para n par, consideremos el grupo diédrico D_n. En este caso $\langle r^2 \rangle$ es un subgrupo de D_n que consiste en la mitad de las rotaciones $1, r^2, r^4, \ldots, r^{n-2}$. El grupo $D_n/\langle r^2 \rangle$ consiste en 4 elementos que pueden ser representados por id, r, f, rf. Este grupo es isomorfo a V.

$\cdot$	$\overline{\mathrm{id}}$	$\overline{r}$	$\overline{f}$	$\overline{rf}$
$\overline{\mathrm{id}}$	$\overline{\mathrm{id}}$	$\overline{r}$	$\overline{f}$	$\overline{rf}$
$\overline{r}$	$\overline{r}$	$\overline{\mathrm{id}}$	$\overline{rf}$	$\overline{f}$
$\overline{f}$	$\overline{f}$	$\overline{rf}$	$\overline{\mathrm{id}}$	$\overline{r}$
$\overline{rf}$	$\overline{rf}$	$\overline{f}$	$\overline{r}$	$\overline{\mathrm{id}}$

Entonces, los subgrupos de D_n que contienen $\langle r^2 \rangle$ corresponden a los subgrupos de V. Excepto el mismo D_n y $\langle r^2 \rangle$, son

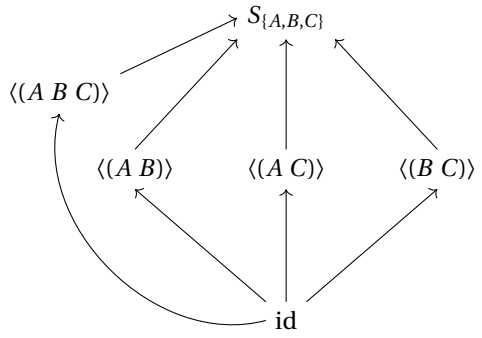
$$\begin{aligned}
\langle r \rangle &= \{\mathrm{id}, r, r^2, \ldots, r^{n-1}\},\\
\langle r^2, f \rangle &= \{\mathrm{id}, r^2, \ldots, r^{n-2}, f, r^2 f, \ldots, r^{n-2} f\},\\
\langle r^2, rf \rangle &= \{\mathrm{id}, r^2, \ldots, r^{n-2}, rf, r^3 f, \ldots, r^{n-1} f\}.
\end{aligned}$$

Todos estos subgrupos son normales. ▲

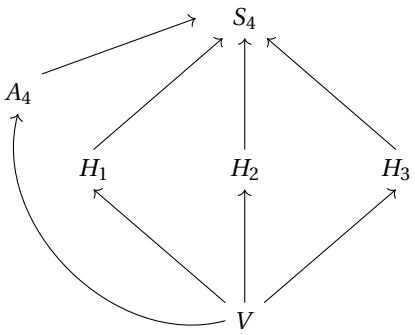
7.8.5. Ejemplo. Volvamos al ejemplo 7.7.6 donde hemos establecido un isomorfismo

$$\phi\colon S_4/V \cong S_{\{A,B,C\}}.$$

La estructura de subgrupos en $S_{\{A,B,C\}}$ es la siguiente.



A estos subgrupos en $S_{\{A,B,C\}}$ corresponden los siguientes subgrupos en S_4 que contienen a V:



Aquí

$$\begin{aligned}
A_4 &= \phi^{-1}\langle(A\ B\ C)\rangle,\\
H_1 &= \phi^{-1}\langle(A\ B)\rangle = V \cup (1\ 4)\,V = \langle(1\ 4), (1\ 2)\,(3\ 4)\rangle,\\
H_2 &= \phi^{-1}\langle(A\ C)\rangle = V \cup (1\ 3)\,V = \langle(1\ 3), (1\ 2)\,(3\ 4)\rangle,\\
H_3 &= \phi^{-1}\langle(B\ C)\rangle = V \cup (1\ 2)\,V = \langle(1\ 2), (1\ 3)\,(2\ 4)\rangle.
\end{aligned}$$

Entre estos grupos los únicos normales son A_4 y V. (En total, en S_4 hay 30 subgrupos y no es muy instructivo enumerarlos todos.) ▲

7.9 Grupos simples

Los grupos simples tienen importancia inestimable en la teoría de grupos, pero por falta de tiempo, vamos a ver solamente algunos ejemplos de ellos.

7.9.1. Definición. Se dice que un grupo G es **simple** si los únicos subgrupos normales de G son $\{1\}$ y el mismo G.

7.9.2. Ejemplo. Un grupo abeliano es simple si y solamente si es isomorfo al grupo cíclico $\mathbb{Z}/p\mathbb{Z}$ de orden primo p. ▲

7.9.3. Ejemplo. Los grupos $\mathrm{SL}_n(k)$ no son simples, puesto que estos tienen centro que consiste en las matrices escalares

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}, \quad a^n = 1.$$

Se puede pasar al grupo cociente

$$\mathrm{PSL}_n(k) := \mathrm{SL}_n(k)/Z(\mathrm{SL}_n(k))$$

llamado el **grupo lineal especial proyectivo**. Notamos que en el caso de $n=2$ se tiene $Z(\mathrm{SL}_n(k)) = \{\pm 1\}$.

Resulta que el grupo $\mathrm{PSL}_n(k)$ es simple con dos excepciones:

1) $n=2$ y $k=\mathbb{F}_2$, donde

$$\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$$

y S_3 tiene un subgrupo normal A_3;

2) $n=2$ y $k=\mathbb{F}_3$, donde

$$\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4 \tag{7.3}$$

y A_4 tiene un subgrupo normal V. ▲

Para las demostraciones de simplicidad de $\mathrm{PSL}_n(k)$, refiero a [Lan2002, §§XIII.8–9][*].

Junto con (7.3), se tiene otro "isomorfismo excepcional"

$$\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5, \tag{7.4}$$

y este grupo es simple. Vamos a explicar los isomorfismos (7.3) y (7.4) más adelante[**]. Por el momento, solo notamos que para q impar

$$|\mathrm{PSL}_2(\mathbb{F}_q)| = |\mathrm{SL}_2(\mathbb{F}_q)|/|\{\pm 1\}| = \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{|\{\pm 1\}|\cdot|\mathbb{F}_q^\times|} = \frac{(q^2-1)(q^2-q)}{2(q-1)} = \frac{1}{2}(q^3-q).$$

En particular,

$$|\mathrm{PSL}_2(\mathbb{F}_3)| = 12, \quad |\mathrm{PSL}_2(\mathbb{F}_5)| = 60.$$

En esta sección probaremos que el grupo alternante A_n es simple para todo $n \geq 5$. Este resultado tiene mucha importancia, aunque sus pruebas no son muy reveladoras.

7.9.4. Lema. *Para $n \geq 5$ todos los 3-ciclos son conjugados en A_n. A saber, si $(a\ b\ c)$ y $(a'\ b'\ c')$ son dos 3-ciclos en A_n, entonces existe $\sigma \in A_n$ tal que*

$$(a'\ b'\ c') = \sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Demostración. A priori sabemos que $(a\ b\ c)$ y $(a'\ b'\ c')$ son conjugados en S_n: existe $\sigma \in S_n$ tal que

$$(a'\ b'\ c') = \sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Ahora si $\operatorname{sgn}\sigma = +1$, entonces $\sigma \in A_n$ y no hay nada que probar. Si $\operatorname{sgn}\sigma = -1$, entonces gracias a nuestra hipótesis que $n \geq 5$, existen índices $1 \leq i < j \leq n$ tales que $i, j \notin \{a, b, c\}$. Tenemos $\sigma \cdot (i\ j) \in A_n$, y luego

$$(\sigma\,(i\ j))\,(a\ b\ c)\,(\sigma\,(i\ j))^{-1} = \sigma\,(i\ j)\,(a\ b\ c)\,(i\ j)\,\sigma^{-1} = \sigma\,(i\ j)\,(i\ j)\,(a\ b\ c)\,\sigma^{-1}$$
$$= \sigma\,(a\ b\ c)\,\sigma^{-1} = (a'\ b'\ c'),$$

usando que $(a\ b\ c)$ e $(i\ j)$ conmutan, siendo ciclos disjuntos. ■

[*] ¿Tal vez volveremos a este asunto cuando hablaremos del conmutador $[\mathrm{SL}_n, \mathrm{SL}_n]$?

[**] Cuando vamos a estudiar acciones de grupos.

7.9.5. Comentario. En el grupo A_4, por ejemplo, los 3-ciclos $(1\ 2\ 3)$ y $(1\ 3\ 2)$ no son conjugados: si

$$(1\ 3\ 2) = \sigma \cdot (1\ 2\ 3) \cdot \sigma^{-1},$$

Entonces $(1\ 3\ 2) = (\sigma(1)\ \sigma(2)\ \sigma(3))$, lo que nos deja las siguientes opciones:

$$\sigma = (2\ 3),\ (1\ 3),\ (1\ 2).$$

Pero ninguna de estas permutaciones está en A_4.

7.9.6. Comentario. En general, dos permutaciones con el mismo tipo de ciclo no son necesariamente conjugadas en A_n. Por ejemplo, los 5-ciclos $(1\ 2\ 3\ 4\ 5)$ y $(1\ 2\ 3\ 5\ 4)$ no son conjugados en A_5.

7.9.7. Corolario. *Si $H \subseteq A_n$ un subgrupo normal que contiene un 3-ciclo, entonces $H = A_n$.*

Demostración. Si H es normal, junto con todo elemento $\sigma \in H$, este debe contener todos sus conjugados $\tau\sigma\tau^{-1}$ para $\tau \in A_n$. Entonces, la hipótesis implica que H contiene todos los 3-ciclos. Estos generan A_n. ■

7.9.8. Proposición. *El grupo A_5 es simple.*

Demostración. Bastaría demostrar que todo subgrupo normal no trivial $H \subseteq A_5$ contiene un 3-ciclo. Los elementos de A_5 tienen forma

$$\mathrm{id}, \quad (\bullet\ \bullet\ \bullet), \quad (\bullet\ \bullet)(\bullet\ \bullet), \quad (\bullet\ \bullet\ \bullet\ \bullet\ \bullet).$$

Asumamos que $\sigma = (a\ b)(c\ d) \in H$. Luego, para $\tau := (a\ b\ e) \in A_5$ tenemos necesariamente

$$\sigma\tau\sigma\tau^{-1} \in H$$

Por la normalidad de H. Calculamos que

$$\sigma\tau\sigma\tau^{-1} = (a\ b)(c\ d)(a\ b\ e)(a\ b)(c\ d)(a\ e\ b) = (a\ b\ e).$$

De la misma manera, si $\sigma = (a\ b\ c\ d\ e) \in H$, entonces podemos tomar $\tau = (a\ b)(c\ d) \in A_5$, y luego calcular que

$$\sigma\tau\sigma\tau^{-1} = ((a\ b\ c\ d\ e)(a\ b)(c\ d))^2 = (a\ e\ c) \in H.$$ ■

7.9.9. Teorema. *El grupo alternante A_n es simple para $n \geq 5$.*

Demostración. Ya probamos este resultado para $n = 5$. Sean $n \geq 6$ y H un subgrupo normal en A_n tal que $H \neq \mathrm{id}$. Vamos a ver que usando cierto truco, la simplicidad de A_n se sigue de la simplicidad de A_5.

Sea $\sigma \in H$ una permutación no trivial. Esto significa que $b = \sigma(a) \neq a$ para algunos $a, b \in \{1, \ldots, n\}$. Escojamos un elemento $c \in \{1, \ldots, n\}$ tal que $c \neq a, b, \sigma(b)$. Consideremos la permutación

$$\tau = (a\ c\ b)\,\sigma\,(a\ c\ b)^{-1}\,\sigma^{-1} = (a\ c\ b)\,\sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Por nuestra hipótesis que H es un subgrupo normal, se tiene $(a\ c\ b)\,\sigma\,(a\ c\ b)^{-1} \in H$, y por lo tanto $\tau \in H$. Ahora notamos que para

$$i \notin \{a, b, c, \sigma(b), \sigma(c)\}$$

se cumple $\sigma^{-1}(i) \notin \{a, b, c\}$ y luego $\tau(i) = i$. Esto significa que τ pertenece al subgrupo

$$H_0 := \{\sigma \in A_n \mid \sigma(i) = i \text{ para } i \notin \{a, b, c, \sigma(b), \sigma(c)\}\}.$$

Ya que $\tau(b) = (a\ c\ b)\,\sigma(b) \neq b$, la permutación τ no es trivial.

Ahora H es normal en A_n, y entonces $H \cap H_0$ es un subgrupo normal no trivial en H_0. Pero $H_0 \cong A_5$, y este grupo es simple, así que se puede concluir que $H \cap H_0 = H_0$. En particular, $(a\ b\ c) \in H$, pero esto implica que $H = A_n$. ■

7.9.10. Corolario. $Z(A_n) = \{\mathrm{id}\}$ *para* $n \geq 4$.

Demostración. Es suficiente notar que $Z(A_n)$ es un subgrupo normal y $Z(A_n) \neq A_n$, ya que A_n no es abeliano para $n \geq 4$. Ahora si $n \geq 5$, la simplicidad de A_n implica que $Z(A_n)$ es trivial. Para $n = 4$ el centro se puede calcular directamente (ejercicio 7.15), o bastaría verificar que $Z(A_4) \neq V$. ■

7.9.11. Corolario. *Para* $n \geq 5$ *los únicos subgrupos normales de* S_n *son* $\{\mathrm{id}\}$, A_n y S_n.

Demostración. Sea $H \subseteq S_n$ un subgrupo normal. El grupo $H \cap A_n$ es un subgrupo normal de A_n y por lo tanto es igual a A_n o $\{\mathrm{id}\}$.

Si $H \cap A_n = A_n$, entonces $H = A_n$, o H contiene una permutación impar junto con todos los elementos de A_n y luego $H = S_n$.

Si $H \cap A_n = \{\mathrm{id}\}$, entonces H no contiene permutaciones pares no triviales. Pero si σ y τ son dos permutaciones impares, entonces $\sigma\tau$ es par, así que la única posibilidad es $H = \{\mathrm{id}, \sigma\}$, donde σ es una permutación impar de orden 2. Pero este subgrupo está muy lejos de ser normal: conjugando σ por los elementos de S_n, se puede obtener cualquier permutación del mismo tipo de ciclo y así salir de H. ■

7.9.12. Comentario. Para $n = 4$ el subgrupo

$$V = \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}$$

es normal en S_4, dado que sus elementos no triviales son todas las permutaciones del tipo de ciclo $(\bullet\ \bullet)\,(\bullet\ \bullet)$.

7.10 Ejercicios

Ejercicio 7.1. Demuestre que todo grupo de orden 4 es cíclico, o es isomorfo a $V \subset A_4$.

Ejercicio 7.2. Demuestre que todo grupo de orden 6 es cíclico, o es isomorfo a S_3.

Ejercicio 7.3. Encuentre el signo de las siguientes permutaciones:

a) $(1\ 2)\,(2\ 5\ 3)\,(1\ 5\ 7\ 3\ 2\ 6\ 4)\,(4\ 7\ 6) \in S_7$;

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 5 & 1 & 4 & 2 & 3 & 10 & 8 & 9 \end{pmatrix} \in S_{10}$.

Ejercicio 7.4. Demuestre que si $\sigma \in S_n$ afecta m elementos (en el sentido de que $\sigma(i) \neq i$ para m números i) y tiene una descomposición en s ciclos disjuntos, entonces

$$\operatorname{sgn}\sigma = (-1)^{m-s}.$$

Por ejemplo, $\sigma = (1\ 2)\,(3\ 6\ 4)\,(5\ 11\ 8)$ afecta $1,2,3,4,5,6,8,11$, entonces $m = 8$, y en la expresión hay $s = 3$ ciclos disjuntos. Luego, $\operatorname{sgn}\sigma = (-1)^{8-3} = -1$.

Ejercicio 7.5. Para $n = 1,2,3,\ldots$ consideremos el espacio vectorial $\mathbb{Q}^n$ con la base estándar $e_1,\ldots,e_n$.
Para una permutación $\sigma \in S_n$ definamos la aplicación lineal

$$\phi_\sigma \colon \mathbb{Q}^n \to \mathbb{Q}^n, \quad e_i \mapsto e_{\sigma(i)}.$$

a) Demuestre que la matriz que corresponde a ϕ_σ en cada fila y cada columna tiene todas las entradas nulas, salvo una que es igual a 1. Tales matrices se llaman las **matrices de permutación**.

b) Demuestre que las matrices de permutación forman un subgrupo de $\mathrm{GL}_n(\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{Q})$ que es isomorfo a S_n.

c) Escriba las matrices de permutación para $n = 3$.

d) Demuestre que $\det\phi_\sigma = \operatorname{sgn}\sigma$.

Ejercicio 7.6. Sea A un anillo conmutativo. Para una matriz invertible $a \in \mathrm{GL}_n(A)$ definamos su matriz **transpuesta inversa** por $a^{-t} := (a^{-1})^t = (a^t)^{-1}$. Demuestre que la aplicación $a \mapsto a^{-t}$ es un automorfismo $\mathrm{GL}_n(A) \to \mathrm{GL}_n(A)$.

Ejercicio 7.7. Encuentre un subgrupo de S_4 isomorfo al grupo diédrico D_4.

Ejercicio 7.8. En los ejercicios para el capítulo anterior hemos mencionado el grupo de matrices ortogonales

$$\mathrm{O}_n(k) = \{a \in \mathrm{GL}_n(k) \mid a^t\, a = a\, a^t = 1\}.$$

a) Demuestre que el determinante de una matriz ortogonal es igual a ± 1.

b) Demuestre que las matrices ortogonales de determinante $+1$ forman un subgrupo normal

$$\mathrm{SO}_n(k) := \{a \in \mathrm{GL}_n(k) \mid a^t\, a = a\, a^t = 1,\ \det a = +1\} \subset \mathrm{O}_n(k).$$

Este se llama el **grupo ortogonal especial**.

c) Calcule el cociente $\mathrm{O}_n(k)/\mathrm{SO}_n(k)$.

d) Demuestre que el grupo $\mathrm{SO}_2(\mathbb{R})$ es isomorfo al grupo del círculo $\mathbb{S}^1$.

Ejercicio 7.9. Demuestre que el conjunto de matrices

$$G := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R},\ x^2 + y^2 > 0 \right\}.$$

es un subgrupo de $\mathrm{GL}_2(\mathbb{R})$ que es isomorfo a $\mathbb{C}^\times$.

Ejercicio 7.10. Demuestre que los grupos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos.

Ejercicio 7.11. Demuestre que el subgrupo de $\mathrm{GL}_2(\mathbb{R})$ generado por las matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

es isomorfo al grupo diédrico D_4.

Ejercicio 7.12. Encuentre isomorfismos de grupos $D_3 \cong S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$.
¿Puede haber isomorfismos $D_n \cong S_n$ para $n \neq 3$? ¿$S_n \cong \mathrm{GL}_m(\mathbb{F}_p)$?

Ejercicio 7.13. Consideremos las **matrices triangulares superiores invertibles** (es decir, las matrices invertibles que tienen ceros debajo de la diagonal) y las matrices diagonales invertibles. Note que en ambos casos se tiene un subgrupo de $\mathrm{GL}_n(A)$. Demuestre que la aplicación

$$\begin{pmatrix} x_{11} & * & * & \cdots & * & * \\ 0 & x_{22} & * & \cdots & * & * \\ 0 & 0 & x_{33} & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x_{n-1,n-1} & * \\ 0 & 0 & 0 & \cdots & 0 & x_{nn} \end{pmatrix} \longmapsto \begin{pmatrix} x_{11} & 0 & 0 & \cdots & 0 & 0 \\ 0 & x_{22} & 0 & \cdots & 0 & 0 \\ 0 & 0 & x_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x_{n-1,n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & x_{nn} \end{pmatrix}$$

que deja las entradas diagonales intactas y aplica el resto de las entradas a 0 es un homomorfismo de grupos.

Ejercicio 7.14. La función exponencial puede ser definida para cualquier matriz $a \in M_n(\mathbb{R})$ mediante la serie habitual $e^a := \sum_{n \geq 0} \frac{1}{n!} a^n$, donde $a^n := \underbrace{a \cdots a}_{n}$ son productos de matrices iterados. Esta serie siempre converge a alguna matriz invertible. Demuestre que para $n > 1$ la exponencial no es un homomorfismo $M_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$; es decir, en general $e^{a+b} \neq e^a \cdot e^b$.

Ejercicio 7.15. Demuestre que $Z(A_4) = \{\mathrm{id}\}$.

Ejercicio 7.16 (Generadores del grupo alternante). Consideremos el grupo alternante A_n para $n \geq 3$.

a) Demuestre que el producto de dos diferentes transposiciones en S_n es un 3-ciclo o un producto de dos 3-ciclos. Deduzca que todos los 3-ciclos generan A_n.

b) Demuestre que todo 3-ciclo puede ser expresado como un producto de 3-ciclos de la forma $(1\ i\ j)$. Deduzca que los 3-ciclos de esta forma generan A_n.

c) Demuestre que los 3-ciclos de la forma $(1\ 2\ i)$ generan A_n. (Escriba $(1\ i\ j)$ en términos de estos 3-ciclos.)

d) Demuestre que los 3-ciclos de la forma $(i\ i+1\ i+2)$ generan A_n.
Indicación: demuestre primero la identidad

$$(1\ 2\ i) = (1\ 2\ i-2)\,(1\ 2\ i-1)\,(i-2\ i-1\ i)\,(1\ 2\ i-2)\,(1\ 2\ i-1).$$

e) Demuestre que A_n puede ser generado por dos permutaciones:

- (1 2 3) y (2 3 $\cdots$ n), si n es par;
- (1 2 3) y (1 2 $\cdots$ n), si n es impar.

Indicación: use d).

Ejercicio 7.17. Construya un homomorfismo inyectivo $\phi\colon S_n \to A_{n+2}$.

Ejercicio 7.18. Sean G un grupo finito y $H, K \subset G$ dos subgrupos tales que $\mathrm{mcd}(|H|, |K|) = 1$. Demuestre que $H \cap K = 1$.

Ejercicio 7.19. Sean G y H dos grupos finitos tales que $\mathrm{mcd}(|G|, |H|) = 1$. Demuestre que el único posible homomorfismo $\phi\colon G \to H$ es trivial (envía todo $g \in G$ a $1 \in H$).

Ejercicio 7.20. Demuestre que para $n \geq 5$ el grupo A_n no tiene subgrupos propios de índice $< n$.

Ejercicio 7.21. Sean G un grupo y $H \subseteq G$ un subgrupo. Demuestre que las siguientes condiciones son equivalentes:

a) H es normal;

b) para cualesquiera $g_1, g_2 \in G$ se cumple

$$g_1 g_2 \in H \Longrightarrow g_1^2 g_2^2 \in H.$$

Ejercicio 7.22. Sean G un grupo y $H \subset G$ un subgrupo de índice 2.

a) Demuestre que H es normal.

b) Demuestre que para todo $g \in G$ se tiene $g^2 \in H$.

Ejercicio 7.23. Demuestre que A_n es el único subgrupo de índice 2 en S_n.

Ejercicio 7.24. Sean G un grupo finito y $H \subseteq G$ un subgrupo.

a) Demuestre que para todo $g \in G$ el conjunto

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

es también un subgrupo y es isomorfo a H.

b) Demuestre que si en G no hay otros subgrupos de índice $|G : H|$, entonces H es normal.

Ejercicio 7.25. Demuestre que si G es un grupo cíclico y $H \subset G$ es un subgrupo, entonces el grupo cociente G/H es también cíclico.

Ejercicio 7.26. Sean G un grupo y $H, K \subseteq G$ dos subgrupos. Definamos su **producto** como el subconjunto

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

a) Demuestre que HK es un subgrupo si y solo si $HK = KH$.

b) Demuestre que si H y K son subgrupos normales, entonces HK es también un subgrupo normal.

Ejercicio 7.27. Sean $H, K \subseteq G$ dos subgrupos normales tales que $H \cap K = 1$.

a) Demuestre que $hk = kh$ para cualesquiera $h \in H$, $k \in K$.

b) Demuestre que si los grupos cociente G/H y G/K son abelianos, entonces G es abeliano.

Ejercicio 7.28 (Segundo teorema de isomorfía). Sean G un grupo, $H \subset G$ un subgrupo y $K \subset G$ un subgrupo normal.

a) Demuestre que $HK := \{hk \mid h \in H,\ k \in K\}$ es un subgrupo de G y K es un subgrupo normal de HK.

b) Demuestre que $H/(H \cap K) \cong HK/K$.

Sugerencia: considere la aplicación $H \to HK/K$ definida por $h \mapsto hK$.

Ejercicio 7.29. Sea k un cuerpo. Demuestre que $\mathrm{GL}_2(k)/k^\times \cong \mathrm{SL}_2(k)/\{\pm I\}$, donde $k^\times \subset \mathrm{GL}_2(k)$ denota el subgrupo de matrices diagonales invertibles.

Ejercicio 7.30 (Tercer teorema de isomorfía). Sea G un grupo. Sea K un subgrupo normal de G y sea N un subgrupo de K tal que N es normal en G. Demuestre que $(G/N)/(K/N) \cong G/K$.

Sugerencia: considere la aplicación definida por $gN \mapsto gK$.

Ejercicio 7.31. Sean m y n dos enteros positivos tales que $n \mid m$, así que $m\mathbb{Z} \subset n\mathbb{Z}$. Demuestre que

$$(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

Ejercicio 7.32. Sean L un cuerpo y $K \subset L$ un subcuerpo. Consideremos el conjunto

$$H := \{a \in \mathrm{GL}_n(L) \mid \det a \in K\}.$$

a) Demuestre que H es un subgrupo normal de $\mathrm{GL}_n(L)$.

b) Encuentre un isomorfismo

$$\mathrm{GL}_n(L)/H \cong L^\times/K^\times.$$

Ejercicio 7.33. Demuestre que $H := \{a \in \mathrm{GL}_n(\mathbb{R}) \mid \det a = \pm 1\}$ es un subgrupo normal de $\mathrm{GL}_n(\mathbb{R})$ y $\mathrm{GL}_n(\mathbb{R})/H \cong \mathbb{R}_{>0}$.

Ejercicio 7.34. Demuestre que los grupos $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ no tienen subgrupos propios de índice finito.

Ejercicio 7.35. Encuentre el subgrupo de torsión de $\mathbb{R}/\mathbb{Z}$ (el subgrupo formado por los elementos de orden finito).

Ejercicio 7.36. Demuestre que cualquier homomorfismo $\phi\colon \mathbb{C}^\times \to \mathbb{R}$ tiene núcleo infinito.

Ejercicio 7.37. Demuestre que $\mathbb{R}_{>0} \cong \mathbb{R}$, pero $\mathbb{Q}_{>0} \ncong \mathbb{Q}$.

Ejercicio 7.38. Para una cadena de subgrupos (no necesariamente normales) $K \subseteq H \subseteq G$, demuestre que $|G : K| = |G : H| \cdot |H : K|$.

Ejercicio 7.39. Sean G un grupo finito y $g, h \in G$ dos elementos de orden 2 tales que $G = \langle g, h\rangle$.
Demuestre que $G \cong D_n$, donde $n = \mathrm{ord}(gh)$.

Ejercicio 7.40. Consideremos el grupo diédrico D_n y $m \mid n$.

a) Demuestre que $\langle r^m\rangle$ es un subgrupo normal de D_n.

b) Demuestre que $D_n/\langle r^m\rangle \cong D_m$.

Ejercicio 7.41. Sea G un grupo.

a) Demuestre que si el cociente $G/Z(G)$ es cíclico, entonces G es un grupo abeliano.

b) Demuestre que si G es un grupo finito de orden pq donde p y q son primos, entonces $Z(G) = 1$ o G es abeliano.

Ejercicio 7.42. Para un cuerpo k, consideremos

$$H(k) := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in k \right\}.$$

a) Demuestre que $H(k)$ es un subgrupo de $\mathrm{GL}_3(k)$. ¿Es normal?

b) Demuestre que $Z(H(k)) \cong k$.

c) Encuentre un isomorfismo $H(\mathbb{F}_2) \cong D_4$.

Ejercicio 7.43. Sean G un grupo y $H, K \subset G$ subgrupos tales que sus índices $m := [G : H]$ y $n := [G : K]$ son finitos.

a) Demuestre que si m y n son coprimos, entonces

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

b) Demuestre que $[G : H \cap K] \leq mn$.

Ejercicio 7.44. Sean G un grupo finito y n un número comprimo con $|G|$. Demuestre que la aplicación $g \mapsto g^n$ es sobreyectiva.

Ejercicio 7.45. Para $n = 1, 2, 3, \ldots$, consideremos

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a, d \equiv 1 \pmod{n},\, b, c \equiv 0 \pmod{n} \right\}.$$

Verifique directamente que $\Gamma(n)$ es un subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$. (Véase también 7.7.8.)

Ejercicio 7.46. Sea G un grupo y $g \in G$ un elemento fijo.

a) Demuestre que la aplicación $\phi_g \colon x \mapsto gxg^{-1}$ define un automorfismo $G \to G$.

b) Demuestre que $g \mapsto \phi_g$ define un homomorfismo $G \to \operatorname{Aut} G$. ¿Cuál es su núcleo? Demuestre que la imagen es un subgrupo normal de $\operatorname{Aut} G$.

Grupos abelianos

Ejercicio 7.47. Demuestre que si A y B son grupos abelianos, entonces los homomorfismos $A \to B$ forman un grupo abeliano respecto a la operación

$$(\phi + \psi)(a) := \phi(a) + \psi(a).$$

Vamos a denotar este grupo por $\mathrm{Hom}(A, B)$.

Ejercicio 7.48. Sea A un grupo abeliano.

a) Demuestre que todo homomorfismo $\phi \colon \mathbb{Z} \to A$ está definido de modo único por el valor de $\phi(1) \in G$, y esto nos da un isomorfismo de grupos

$$\mathrm{Hom}(\mathbb{Z}, G) \xrightarrow{\cong} G, \quad \phi \mapsto \phi(1).$$

b) Demuestre que todo homomorfismo $\phi \colon \mathbb{Q} \to \mathbb{Q}$ está definido de modo único por el valor $\phi(1) \in \mathbb{Q}$, y esto nos da un isomorfismo de grupos

$$\mathrm{Hom}(\mathbb{Q}, \mathbb{Q}) \xrightarrow{\cong} \mathbb{Q}, \quad \phi \mapsto \phi(1).$$

Ejercicio 7.49. Calcule el grupo $\mathrm{Aut}(\mathbb{Q})$.

Ejercicio 7.50. Sea A un grupo abeliano.

1) Demuestre que para todo homomorfismo $f\colon \mathbb{Z}/m\mathbb{Z} \to A$ se tiene necesariamente $f([1]_m) \in A[m]$.

2) Demuestre que
$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \to A[m], \quad f \mapsto f([1]_m)$$
es un isomorfismo de grupos.

3) Describa los grupos abelianos
$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}), \quad \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}), \quad \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$
para diferentes $m, n = 2, 3, 4, 5, \ldots$

Ejercicio 7.51. Encuentre todos los homomorfismos entre el grupo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n respecto a la adición y el grupo $\mathbb{C}^\times$ de los números complejos no nulos respecto a la multiplicación.

Ejercicio 7.52. Se dice que un grupo abeliano A un elemento $x \in A$ es **divisible** si para todo $a \in A$ y todo entero positivo $n = 1, 2, 3, \ldots$ existe $y \in A$ (no necesariamente único) tal que $ny = x$. Si todos los elementos de A son divisibles, se dice que A es un **grupo divisible**.

a) Demuestre que los grupos aditivos $\mathbb{Q}$ y $\mathbb{R}$ son divisibles.

b) Demuestre que un grupo abeliano finito no nulo no puede ser divisible.

Ejercicio 7.53. Sea p un número primo. El **p-grupo de Prüfer** es el grupo de las raíces de la unidad de orden p^n para $n \in \mathbb{N}$:
$$\mu_{p^\infty}(\mathbb{C}) := \bigcup_{n \geq 0} \mu_{p^n}(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^{p^n} = 1 \text{ para algún } n = 0, 1, 2, \ldots\}$$
Demuestre que existe un isomorfismo $\mu_{p^\infty}(\mathbb{C}) \cong \mathbb{Z}[1/p]/\mathbb{Z}$ donde
$$\mathbb{Z}[1/p] := \{a/p^n \mid a \in \mathbb{Z},\ n = 0, 1, 2, \ldots\}.$$

Ejercicio 7.54. Sea A un grupo abeliano.

a) Demuestre que $x \in A$ es divisible si y solamente es divisible por cualquier *número primo* $p = 2, 3, 5, 7, 11, \ldots$

b) Usando la observación anterior, demuestre que el grupo de Prüfer $\mu_{p^\infty}(\mathbb{C}) \cong \mathbb{Z}[1/p]/\mathbb{Z}$ es divisible.

Ejercicio 7.55.

a) Sea $f\colon A \to B$ un homomorfismo de grupos abelianos. Demuestre que si $a \in A$ es divisible, entonces $f(a) \in B$ es también divisible.

b) Demuestre que no hay homomorfismos no triviales $\mathbb{Q} \to \mathbb{Z}$ y $\mathbb{Q}/\mathbb{Z} \to \mathbb{Z}$.

c) Demuestre que todo grupo cociente de un grupo divisible es también divisible. En particular, $\mathbb{Q}/\mathbb{Z}$ y $\mathbb{R}/\mathbb{Z}$ son divisibles.

Bibliografía

[Lan2002] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
http://dx.doi.org/10.1007/978-1-4613-0041-0