Capítulo 5
Homomorfismos de grupos

> Les mathématiciens n'étudient pas des objets, mais des relations entre les objets.
>
> Poincaré

Hemos visto algunas nociones básicas de grupos y varios ejemplos. Para comparar grupos, estudiar construcciones sobre ellos e investigar sus propiedades más sutiles, hay que saber cómo estos se relacionan. Aquí el concepto clave es el de homomorfismo, una aplicación entre grupos que preserva su estructura (la operación del grupo).

5.0.1. Definición. Un **homomorfismo** de grupos G y H es una aplicación $f\colon G \to H$ tal que para cualesquiera $g_1, g_2 \in G$ se cumple:

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

5.1 Ejemplos de homomorfismos

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

5.1.2. Ejemplo. Para ver más homomorfismos familiares, podemos revisar algunas propiedades del análisis real y complejo conocidas a todo el mundo.

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

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

   donde $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ (resp. $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$) es el grupo de los números racionales (resp. reales) no nulos.

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 de los números reales respecto a la adición $\mathbb{R}$ y el grupo de los números reales positivos respecto a la multiplicación $\mathbb{R}_{>0}$. 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

$$e^{x+y} = e^x\, e^y.$$

En general, para $a > 0$, la aplicación

$$\mathbb{R} \to \mathbb{R}^\times, \quad x \mapsto a^x$$

es un homomorfismo: se cumple

$$a^{x+y} = a^x\, a^y.$$

4) Para los números complejos la exponencial 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 natural es un homomorfismo

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

para cualesquiera $x, y > 0$ se cumple

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

En general, para $a > 0$, $a \neq 1$ el logaritmo de base a

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

es un homomorfismo: para cualesquiera $x, y > 0$ se tiene

$$\log_a(xy) = \log_a(x) + \log_a(y).$$

6) La raíz n-ésima es un homomorfismo

$$\mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto \sqrt[n]{x}.$$

De hecho, tenemos

$$\sqrt[n]{xy} = \sqrt[n]{x} \cdot \sqrt[n]{y}.$$

En general, 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) La conjugación compleja $z \mapsto \overline{z}$ es un homomorfismo aditivo y multiplicativo a la vez:

$$\mathbb{C} \to \mathbb{C} \quad \text{y} \quad \mathbb{C}^\times \to \mathbb{C}^\times.$$

Para cualesquiera z, w se cumple

$$\overline{z+w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z}\,\overline{w}.$$

▲

5.1.3. Ejemplo. En el primer capítulo hemos estudiado el signo de permutación

$$\operatorname{sgn}\colon S_n \to \{\pm 1\}$$

que es un homomorfismo entre el grupo simétrico y el grupo multiplicativo $\{\pm 1\}$. De hecho, hemos visto que para cualesquiera $\sigma, \tau \in S_n$ se cumple

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

▲

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

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

▲

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

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ a &\mapsto [a]_n. \end{aligned}$$

En efecto, $[a+b]_n = [a]_n + [b]_n$ por la misma definición de la adición de los restos módulo n (recordemos que uno tiene que verificar por separado que esta adición no depende de los representantes particulares de las clases de equivalencia).

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

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ [a]_m &\mapsto [a]_n. \end{aligned}$$

De hecho, primero notamos que esta aplicación está bien definida: si $a \equiv a' \pmod{m}$, esto quiere decir que $m \mid (a - a')$, pero luego $n \mid (a - a')$, así que $a \equiv a' \pmod{n}$. Es un homomorfismo por la definición de la adición módulo m y n:

$$[a]_m + [b]_m = [a+b]_m = [a+b]_n = [a]_n + [b]_n.$$

De la misma manera, se ve que hay un homomorfismo de grupos multiplicativos

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times, \\ [a]_m &\mapsto [a]_n. \end{aligned}$$

▲

5.1.6. Ejemplo. Para un número entero no nulo $n \in \mathbb{Z} \setminus \{0\}$ su **valuación p-ádica** es el máximo número natural k tal que p^k divide a n:

$$v_p(n) := \text{máx}\{k \mid p^k \mid n\}.$$

(Para $n = 0$ normalmente se define $v_p(0) := +\infty$, pero no vamos a usar esta convención.)

Ahora para dos números no nulos $m, n \in \mathbb{Z}$ se puede escribir

$$m = p^{v_p(m)}\, m', \quad n = p^{v_p(n)}\, n',$$

donde $p \nmid m'$ y $p \nmid n'$, y luego,

$$mn = p^{v_p(m)+v_p(n)}\, m'n',$$

donde $p \nmid (m'n')$, así que

$$v_p(mn) = v_p(m) + v_p(n).$$

Ahora todo número racional no nulo puede ser representado por una fracción m/n, donde $m, n \neq 0$ son algunos números enteros. Podemos definir

$$v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n).$$

Esta definición depende del número racional y no de su representación como fracción. De hecho, tenemos

$$\frac{m}{n} = \frac{m'}{n'} \iff mn' = m'n.$$

Ahora

$$v_p(m) + v_p(n') = v_p(mn') = v_p(m'n) = v_p(m') + v_p(n),$$

así que

$$v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n) = v_p(m') - v_p(n') =: v_p\left(\frac{m'}{n'}\right).$$

Esto significa que la función

$$\begin{aligned} v_p \colon \mathbb{Q}^\times &\to \mathbb{Z}, \\ \frac{m}{n} &\mapsto v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n) \end{aligned}$$

está bien definida. Es un homomorfismo entre el grupo multiplicativo $\mathbb{Q}^\times$ y el grupo aditivo $\mathbb{Z}$: para cualesquiera $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}^\times$ tenemos

$$\begin{aligned} v_p\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) = v_p\left(\frac{m_1 m_2}{n_1 n_2}\right) &= v_p(m_1 m_2) - v_p(n_1 n_2) \\ &= v_p(m_1) - v_p(n_1) + v_p(m_2) - v_p(n_2) = v_p\left(\frac{m_1}{n_1}\right) + v_p\left(\frac{m_2}{n_2}\right). \end{aligned}$$

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:

$$|x|_p := p^{-v_p(x)}.$$

Entonces, para cualesquiera $x, y \in \mathbb{Q}^\times$ se cumple

$$|x\,y|_p = p^{-v_p(xy)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p \cdot |y|_p.$$

De esta manera se obtiene un homomorfismo de grupos multiplicativos

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

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

5.1.7. Ejemplo. He aquí otro ejemplo curioso de la teoría de números. Para un número primo p, decimos que un entero $a \in \mathbb{Z}$ es un **resíduo cuadrático módulo** p si

$$a \equiv b^2 \pmod{p}$$

para algún $b \in \mathbb{Z}$. Podemos definir el **símbolo de Legendre** mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un resíduo cuadrático módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un resíduo cuadrático módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

Obviamente, si $a \equiv a' \pmod{p}$, entonces

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right),$$

así que el símbolo de Legedre está definido sobre los restos módulo p. Luego, para cualesquiera $a, b \in \mathbb{Z}$ se tiene

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(está claro que el producto de dos resíduos cuadráticos es un resíduo cuadrático; un poco menos claro que el producto de dos no-resíduos cuadráticos es un resíduo cuadrático, pero lo veremos más adelante). Esto quiere decir que el símbolo de Legendre es un homomorfismo de grupos multiplicativos

$$\begin{aligned} \left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times &\to \{\pm 1\}, \\ [a]_p &\mapsto \left(\frac{a}{p}\right). \end{aligned}$$

▲

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

5.1.8. Ejemplo.

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

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

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

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

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

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

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

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

3) Recordemos que para un anillo conmutativo R y un polinomio

$$f = \sum_{0 \le i \le n} a_i \, X^i \in R[X],$$

su valor en $c \in R$ viene dado por

$$f(c) = \sum_{0 \le i \le n} a_i \, c^i \in R.$$

Esto nos da un **homomorfismo de evaluación**

$$ev_c \colon R[X] \to R, \quad f \mapsto f(c).$$

▲

5.1.9. Digresión. En los ejercicios hemos mencionado el anillo de series de potencias $R[\![X]\!]$. En general, ya que una suma $f = \sum_{i \ge 0} a_i \, X^i \in R[\![X]\!]$ puede tener un número infinito de coeficientes no nulos, no tiene sentido evaluar f en un elemento $c \in R$. Lo que siempre podemos hacer es "evaluar f en 0":

$$\begin{aligned} R[\![X]\!] &\to R, \\ f = \sum_{i \ge 0} a_i \, X^i &\mapsto f(0) = a_0. \end{aligned}$$

En general, evaluación de una serie $f \in R[\![X]\!]$ en un elemento arbitrario $c \in R$ requiere de una noción de convergencia.

5.1.10. 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 $g, h \in G$. ▲

5.1.11. Ejemplo. En particular, si R es un anillo conmutativo y $n \in \mathbb{Z}$, entonces la n-ésima potencia es un homomorfismo de grupos multiplicativos

$$R^\times \to R^\times, \quad x \mapsto x^n.$$

Para el grupo aditivo subyacente, tenemos

$$(x+y)^n = \sum_{0 \le i \le n} \binom{n}{i} x^i \, y^{n-i},$$

y esta expresión normalmente no es igual a $x^n + y^n$. Sin embargo, si en R se cumple $p \cdot x$ para cualesquiera $x \in R$, por ejemplo para $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, entonces

$$(x+y)^p = x^p + y^p.$$

Por ejemplo,

$$\mathbb{F}_p \to \mathbb{F}_p, \quad x \mapsto x^n$$

es un homomorfismo de grupos aditivos. ▲

5.2 Propiedades básicas de homomorfismos

5.2.1. Observación. *La composición de dos homomorfismos $f_1 \colon G \to G'$ y $f_2 \colon G' \to G''$ es un homomorfismo $f_2 \circ f_1 \colon G \to G''$.*

Demostración. Para cualesquiera $g_1, g_2 \in G$ tenemos

$$\begin{aligned}(f_2 \circ f_1)(g_1 g_2) = f_2(f_1(g_1 g_2)) = f_2(f_1(g_1)\, f_1(g_2)) = f_2(f_1(g_1)) \cdot f_2(f_1(g_2)) \\ = (f_2 \circ f_1)(g_1) \cdot (f_2 \circ f_1)(g_2).\end{aligned}$$

■

5.2.2. Observación (Homomorfismos preservan el elemento neutro). *Si $f \colon G \to H$ es un homomorfismo, entonces*

$$f(1_G) = 1_H$$

Demostración. Tenemos

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

y por lo tanto $f(1_G)$ es el elemento neutro. ■

5.2.3. Observación (Homomorfismos preservan los elementos inversos). *Si $f \colon G \to H$ es un homomorfismo, entonces para todo $g \in G$*

$$f(g^{-1}) = f(g)^{-1}.$$

Demostración.

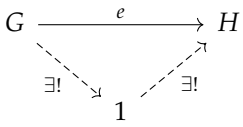
$$f(g^{-1}) \cdot f(g) = f(g^{-1} g) = f(1) = 1.$$

■

5.2.4. Observación. *Sea 1 el grupo trivial. Para todo grupo G existe un homomorfismo único $1 \to G$ y un homomorfismo único $G \to 1$.*

Note que la situación con conjuntos es diferente: allí para todo X existe una aplicación única $\emptyset \to X$ y una aplicación única $X \to \{\bullet\}$. Los conjuntos $\emptyset$ y $\{\bullet\}$ son diferentes (entre ellos no hay biyección). En el caso de grupos, el mismo grupo trivial 1 satisface ambas propiedades $1 \xrightarrow{\exists!} G$ y $G \xrightarrow{\exists!} 1$.

5.2.5. Corolario. *Para dos grupos G y H existe un homomorfismo único $e\colon G \to H$ que se factoriza por el grupo trivial:*



Este se llama el ***homomorfismo trivial*** *y está definido por*

$$e(g) = 1_H \quad \textit{para todo } g \in G.$$

5.2.6. Ejemplo. Para el signo de permutaciones tenemos

$$\operatorname{sgn}(\mathrm{id}) = +1$$

y

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

▲

5.2.7. Observación (Homomorfismos preservan potencias). *Para todo $n \in \mathbb{Z}$ tenemos*

$$f(g^n) = f(g)^n.$$

Demostración. Inducción sobre n. La base es el caso de $n = 0$ que corresponde a 5.2.2. Si $n < 0$, aplicamos 5.2.3. ■

5.2.8. Corolario. *Si $g^n = 1$, entonces $f(g)^n = 1$.*

5.3 Mono, epi, iso

5.3.1. Definición (clásica). Sea $f\colon G \to H$ un homomorfismo de grupos.

1) Si f es una aplicación inyectiva, se dice que f es un **monomorfismo** y se escribe $f\colon G \rightarrowtail H$.

2) Si f es una aplicación sobreyectiva, se dice que f es un **epimorfismo** y se escribe $f\colon G \twoheadrightarrow H$.

3) Si f es una aplicación biyectiva, se dice que f es un **isomorfismo** y se escribe $f\colon G \xrightarrow{\cong} H$.

   Cuando entre G y H existe un isomorfismo $G \xrightarrow{\cong} H$, se dice que G y H son grupos **isomorfos** y se escribe $G \cong H$.

En lugar de los sustantivos *monomorfismo*, *epimorfismo*, *isomorfismo* a veces se usan los adjetivos *mono*, *epi*, *iso*, por ejemplo "f es mono".

5.3.2. Ejemplo. Si $G \subset H$ es un subgrupo, la inclusión $G \hookrightarrow H$ es un monomorfismo de grupos. ▲

5.3.3. Ejemplo. Los homomorfismos

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

y

$$\mathrm{sgn}\colon S_n \to \{\pm 1\}$$

son epi. ▲

5.3.4. Ejemplo. La exponencial compleja

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

es epi, pero no es mono: para cualesquiera $z \in \mathbb{C}$, $k \in \mathbb{Z}$ tenemos $e^z = e^{z+2\pi k\sqrt{-1}}$. ▲

5.3.5. Ejemplo. Se ve que la aplicación $f\colon x \mapsto x^p$ es un isomorfismo de grupos aditivos $\mathbb{F}_p \to \mathbb{F}_p$ y grupos multiplicativos $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$. De hecho,

$$f(x) = f(y) \iff x^p = y^p \iff (x-y)^p = x - y = 0,$$

donde la igualdad $(x-y)^p = x - y$ es el pequeño teorema de Fermat. ▲

5.3.6. 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

$$\begin{aligned} &\mathbb{Z} \to 2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\},\\ &n \mapsto 2n. \end{aligned}$$

▲

5.3.7. Ejemplo. Sean X e Y dos conjuntos tales que existe una biyección $f\colon X \to Y$. Una elección de f induce un isomorfismo entre los grupos simétricos

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

De hecho, es un homomorfismo de grupos:

$$f \circ (\sigma \circ \tau) \circ f^{-1} = (f \circ \sigma \circ f^{-1}) \circ (f \circ \tau \circ f^{-1}).$$

Es inyectivo, ya que f y f^{-1} son cancelables, siendo biyecciones:

$$f \circ \sigma \circ f^{-1} = f \circ \tau \circ f^{-1} \Rightarrow \sigma = \tau.$$

Es sobreyectivo: para toda biyección $\phi\colon Y \to Y$, consideremos la biyección $\sigma\colon X \to X$ dada por

$$X \xrightarrow{f} Y \xrightarrow{\phi} Y \xrightarrow{f^{-1}} X$$

Entonces

$$f \circ \sigma \circ f^{-1} = f \circ (f^{-1} \circ \phi \circ f) \circ f^{-1} = \phi.$$

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

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

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

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

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

Cuidado: 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

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

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

5.3.9. Observación. *$f\colon G \to H$ es iso si y solamente si es invertible: existe otro homomorfismo de grupos $f^{-1}\colon H \to G$ tal que*

$$f^{-1} \circ f = \mathrm{id}_G, \quad f \circ f^{-1} = \mathrm{id}_H.$$

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

$$\begin{aligned}f^{-1}(h_1h_2) = f^{-1}\Big(f(f^{-1}(h_1)) \cdot f(f^{-1}(h_2))\Big) = f^{-1}\Big(f\big(f^{-1}(h_1) \cdot f^{-1}(h_2)\big)\Big)\\ = f^{-1}(h_1) \cdot f^{-1}(h_2),\end{aligned}$$

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

5.3.10. 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:

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

▲

5.3.11. Corolario. *La isomorfía de grupos es una relación de equivalencia en el sentido de que para cualesquiera G, H, K tenemos*

$$G \cong G, \quad G \cong H \Rightarrow H \cong G, \quad G \cong H, H \cong K \Rightarrow G \cong K.$$

5.3.12. Ejemplo. Salvo isomorfismo, los primeros grupos finitos son

1) el grupo trivial 1;

2) el grupo $\mathbb{Z}/2\mathbb{Z}$;

3) el grupo $\mathbb{Z}/3\mathbb{Z}$;

4) el grupo $\mathbb{Z}/4\mathbb{Z}$ y el grupo de cuatro $V = \{\mathrm{id}, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\} \subset A_4$;

5) el grupo $\mathbb{Z}/5\mathbb{Z}$;

6) el grupo simétrico S_3, que es isomorfo al grupo diédrico D_3;

7) el grupo $\mathbb{Z}/7\mathbb{Z}$;

8) hay tres grupos abelianos de orden 8: uno de ellos es $\mathbb{Z}/8\mathbb{Z}$ y otros dos que vamos a construir más adelante; además, hay dos grupos no abelianos que ya conocemos: el grupo diédrico D_4 y el grupo de cuaterniones Q_8.

Más adelante veremos que para todo primo p hay un grupo único de orden p salvo isomorfismo y es el grupo $\mathbb{Z}/p\mathbb{Z}$. También vamos a describir todos los grupos *abelianos* finitos salvo isomorfismo. Es muy difícil clasificar los grupos *no abelianos* finitos y no vamos a tocar el tema. ▲

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

5.3.13. Observación. *Si $G \cong H$, entonces G es abeliano si y solamente si H es abeliano.*

5.3.14. Ejemplo. Ya que todo isomorfismo $G \xrightarrow{\cong} H$ es una biyección de conjuntos, si G y H tienen diferente cardinalidad, estos no pueden ser isomorfos. 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. ▲

5.3.15. Definición. Fijemos un grupo G. Un isomorfismo entre G y sí mismo se llama un **automorfismo**.

5.3.16. 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 $f_1\colon G \to G$ y $f_2\colon G \to G$ son dos automorfismos, entonces su composición $f_2 \circ f_1\colon G \to G$ es también un automorfismo. Todo automorfismo $f\colon G \to G$ posee una aplicación inversa $f^{-1}\colon G \to G$, y como hemos visto arriba, es automáticamente un automorfismo. ■

5.3.17. Ejemplo. El grupo $\mathbb{Z}/3\mathbb{Z}$ respecto a la adición tiene dos automorfismos: id y un automorfismo no trivial

$$f\colon [0] \mapsto [0], \quad [1] \mapsto [2], \quad [2] \mapsto [1].$$

Tenemos $f \circ f = \mathrm{id}$ y luego $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. ▲

5.4 Imágenes

5.4.1. Definición. Sea $f\colon G \to H$ un homomorfismo de grupos. El conjunto

$$\mathrm{im}\, f := \{f(g) \mid g \in G\}$$

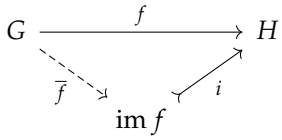
se llama la **imagen** de f.

5.4.2. Observación. *Para todo homomorfismo $f\colon G \to H$ la imagen* $\mathrm{im}\, f$ *es un subgrupo de H.*

Demostración. Como hemos notado en 5.2.2, tenemos $1_H \in \operatorname{im} f$. Luego, si $f(g_1), f(g_2) \in \operatorname{im} f$, entonces $f(g_1)\,f(g_2) = f(g_1 g_2) \in \operatorname{im} f$. En fin, gracias a 5.2.3, si $f(g) \in \operatorname{im} f$, entonces $f(g)^{-1} = f(g^{-1}) \in \operatorname{im} f$. ■

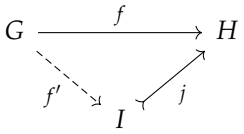
5.4.3. Proposición (Propiedad universal de la imagen). *Sea $f\colon G \to H$ un homomorfismo de grupos.*

1) *Existe una factorización de f por el monomorfismo canónico $i\colon \operatorname{im} f \rightarrowtail H$ (inclusión de subgrupo):*



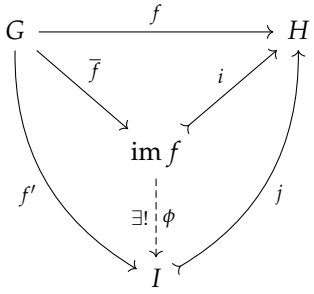
$$f = i \circ \overline{f}.$$

2) *Supongamos que hay otro grupo I junto con un monomorfismo $j\colon I \rightarrowtail H$ y una factorización de f por I:*



$$f = j \circ f'.$$

Luego existe un único homomorfismo $\phi\colon \operatorname{im} f \to I$ que hace conmutar el siguiente diagrama:



$$\phi \circ \overline{f} = f', \quad j \circ \phi = i.$$

(ϕ es mono, puesto que $i = j \circ \phi$ lo es).

Demostración. La parte 1) está clara de la definición de la imagen: ya que f toma sus valores en $\operatorname{im} f \subset H$, en realidad f puede ser vista como una aplicación $\overline{f}\colon G \to \operatorname{im} f$. Es un homomorfismo, puesto que f es un homomorfismo. Su composición con la inclusión del subgrupo $i\colon \operatorname{im} f \rightarrowtail H$ coincide con f.

En 2), la única opción para ϕ para que se cumpla $\phi \circ \overline{f} = f'$ es definir

$$\begin{aligned} \phi\colon \operatorname{im} f &\to I, \\ f(g) &\mapsto f'(g). \end{aligned}$$

Esta aplicación está bien definida: si tenemos $f(g_1) = f(g_2)$, entonces

$$j(f'(g_1)) = f(g_1) = f(g_2) = j(f'(g_2)) \Rightarrow f'(g_1) = f'(g_2).$$

También se cumple $i = j \circ \phi$. En efecto, para $h = f(g) \in \operatorname{im} f$ tenemos

$$j(\phi(h)) = j(f'(g)) = f(g).$$

■

5.4.4. Observación. *Todo monomorfismo $f\colon G \rightarrowtail H$ corresponde a un isomorfismo*

$$G \xrightarrow{\cong} \operatorname{im} f \subset H.$$

5.4.5. 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 monomorfismo

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

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. ▲

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

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

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

Luego, se obtiene un grupo

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

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

5.5 Núcleos

5.5.1. Definición. Sea $f\colon G \to H$ un homomorfismo de grupos. El conjunto

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

se llama el **núcleo** de f.

A priori f es un subconjunto de G, pero en realidad, es su subgrupo.

5.5.2. Observación. *Para todo homomorfismo $f\colon G \to H$ el núcleo* $\ker f$ *es un subgrupo de G.*

Demostración. Primero, $f(1_G) = 1_H$ (véase 5.2.2), entonces $1_G \in \ker f$. Luego, $f(g_1g_2) = f(g_1)\,f(g_2)$, así que

$$g_1, g_2 \in \ker f \Rightarrow g_1g_2 \in \ker f.$$

Por último, para todo $x \in \ker f$ tenemos

$$f(g^{-1}) = f(g)^{-1} = (1_H)^{-1} = 1_H,$$

así que también $g^{-1} \in \ker f$. ■

5.5.3. Ejemplo. Por la definición, el grupo alternante es el núcleo del homomorfismo de signo:

$$A_n := \ker(S_n \xrightarrow{\text{sgn}} \{\pm 1\}).$$

▲

5.5.4. Ejemplo. Tenemos

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

▲

5.5.5. Ejemplo. Por definición, el grupo $\mathrm{SL}_n(R)$ es el núcleo del homomorfismo del determinante sobre $\mathrm{GL}_n(R)$:

$$\mathrm{SL}_n(R) := \ker(\mathrm{GL}_n(R) \xrightarrow{\det} R^\times).$$

▲

5.5.6. 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 $\mathbb{C}^\times$:

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

▲

5.5.7. Observación. *Un homomorfismo $f\colon G \to H$ es mono si y solamente si* $\ker f = \{1_G\}$.

Demostración. Tenemos que ver que f es una aplicación inyectiva. Primero notamos que si $\ker f$ contiene otro elemento $g \neq 1_G$, entonces

$$f(g) = f(1_G) = 1_H,$$

así que f no es inyectiva. Entonces, la condición $\ker f = \{1_G\}$ es necesaria. Para ver que es también suficiente, notamos que si $f(g_1) = f(g_2)$ para $g_1, g_2 \in G$, entonces

$$f(g_1\,g_2^{-1}) = f(g_1)\,f(g_2^{-1}) = f(g_1)\,f(g_2)^{-1} = 1_H,$$

así que $g_1 = g_2$. ■

5.5.8. Ejemplo. Para la exponente compleja

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

se tiene

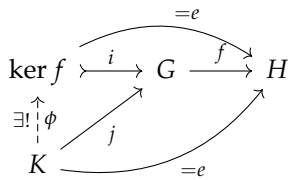
$$\ker(\exp\colon \mathbb{C} \to \mathbb{C}^\times) = 2\pi\sqrt{-1}\,\mathbb{Z} = \{2\pi n\sqrt{-1} \mid n \in \mathbb{Z}\} \subset \mathbb{C}.$$

Por esto en el caso complejo, el logaritmo es más sutil: la exponencial toma el mismo valor en $z + 2\pi n\sqrt{-1}$ para todo $n \in \mathbb{Z}$, lo que impide definir una función inversa $\log\colon \mathbb{C}^\times \to \mathbb{C}$. ▲

5.5.9. Proposición (Propiedad universal del núcleo). *Para un homomorfismo de grupos $f\colon G \to H$, sea* $\ker f$ *su núcleo y sea* $i\colon \ker f \rightarrowtail G$ *la inclusión.*

1) *La composición* $\ker f \xrightarrow{i} G \xrightarrow{f} H$ *es el homomorfismo trivial.*

2) *Si $j\colon K \to G$ es otro morfismo tal que la composición $K \xrightarrow{j} G \xrightarrow{f} H$ es trivial, entonces existe un único homomorfismo de grupos $\phi\colon K \to \ker f$ tal que $i \circ \phi = j$.*



Demostración. La parte 1) es evidente de la definición de $\ker f$. En la parte 2), tenemos $f(j(x)) = 1$ para todo $x \in K$. Entonces, $\operatorname{im} j \subseteq \ker f$, y esto nos da la factorización única de $j\colon K \to G$ por $\ker f$. ■

5.5.10. Observación. *Si tenemos un diagrama conmutativo de homomorfismos de grupos*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ G' & \xrightarrow[f']{} & H' \end{array}$$

entonces existe una único homomorfismo $\ker f \to \ker f'$ *que hace conmutar el diagrama*

$$\begin{array}{ccccc} \ker f & \rightarrowtail & G & \xrightarrow{f} & H \\ \downarrow{\scriptstyle\exists!} & & {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \ker f' & \rightarrowtail & G' & \xrightarrow[f']{} & H' \end{array}$$

Demostración. La flecha punteada existe y es única gracias a la propiedad universal de $\ker f'$, pero es nada más la restricción de ϕ a $\ker f$. Tenemos que comprobar que su imagen pertenece a $\ker f'$. Si $g \in \ker f$, entonces $f(g) = 1$, y por lo tanto $f'(\phi(g)) = \psi(f(g)) = 1$ y $\phi(g) \in \ker f'$, y la aplicación $g \mapsto \phi(g)$ se restringe correctamente a $\ker f \to \ker f'$. ■

5.6 Caracterización de mono, epi, iso

5.6.1. Proposición. *Un homomorfismo de grupos $f\colon G \to H$ es inyectivo si y solamente si es cancelable por la izquierda: para todo par de homomorfismos de grupos*

$$g, g'\colon G' \to G$$

tenemos

$$f \circ g = f \circ g' \Rightarrow g = g'.$$

Demostración. Si $f\colon G \to H$ es una aplicación inyectiva, entonces es cancelable por la izquierda para todas *aplicaciones entre conjuntos* g, g' (no necesariamente homomorfismos de grupos) como hemos notado en el capítulo 0.

La otra dirección es un poco más sútil: necesitamos ver que si un homomorfismo f es cancelable por la izquierda para homomorfismos de grupos g, g', entonces es inyectivo. Consideramos la inclusión canónica $i\colon \ker f \to G$ y el homomorfismo trivial $e\colon \ker f \to G$. Entonces,

$$f \circ i = f \circ e$$

—ambas composiciones nos dan un homomorfismo trivial $\ker f \to H$. Si f es cancelable por la izquierda, esto implica $i = e$; es decir, que $\ker f = \{1_G\}$ y por lo tanto f es inyectivo gracias a 5.5.7. ■

Entonces, para homomorfismos de grupos $f\colon G \to H$ tenemos las equivalencias

$$\begin{aligned} f \text{ es un homomorfismo inyectivo} &\iff f \text{ es cancelable por la izquierda} \\ &\qquad (f \circ g = f \circ g' \Rightarrow g = g' \text{ para homomorfismos } g, g'), \\ f \text{ es un homomorfismo biyectivo} &\iff f \text{ es invertible (existe homomorfismo } f^{-1}). \end{aligned}$$

El lector puede adivinar que también existe otra equivalencia

$$\begin{aligned} f \text{ es un homomorfismo sobreyectivo} &\iff f \text{ es cancelable por la derecha} \\ &\qquad (g \circ f = g' \circ f \Rightarrow g = g' \text{ para homomorfismos } g, g'). \end{aligned}$$

Aquí la implicación "$\Rightarrow$" es fácil (véase el capítulo 0), pero la otra implicación "$\Leftarrow$" es más difícil y no la vamos a probar.

5.7 Ejercicios

Ejercicio 5.1. *Sea $f\colon G \to H$ un homomorfismo de grupos y sea $K \subset H$ un subgrupo. Demuestre que $f^{-1}(K)$ es un subgrupo de G.*

Ejercicio 5.2. *Sea R un anillo conmutativo. Para una matriz invertible $A \in \mathrm{GL}_n(R)$ 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 $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R)$.*

Ejercicio 5.3. *Sea G cualquier grupo, $\mathbb{Z}$ el grupo aditivo de los números enteros y $\mathbb{Q}$ el grupo aditivo de los números racionales.*

1) *Demuestre que todo homomorfismo $f\colon \mathbb{Z} \to G$ está definido de modo único por el valor de $f(1) \in G$. Esto nos da una biyección natural*

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

donde $\mathrm{Hom}(\mathbb{Z}, G)$ es el conjunto de homomorfismos $\mathbb{Z} \to G$.

2) *Demuestre que todo homomorfismo $f\colon \mathbb{Q} \to \mathbb{Q}$ del grupo aditivo de los números racionales está definido de modo único por el valor $f(1) \in \mathbb{Q}$. Esto nos da una biyección natural*

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

donde $\mathrm{Hom}(\mathbb{Q}, \mathbb{Q})$ es el conjunto de homomorfismos $\mathbb{Q} \to \mathbb{Q}$.

Ejercicio 5.4.

1) *Encuentre los grupos $\ker f$ e $\mathrm{im}\, f$ para el homomorfismo*

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}, \quad x \mapsto nx$$

donde $n = 2, 3, 4, 5$.

2) *Calcule los grupos $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ y $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$.*

Ejercicio 5.5. *Consideremos el conjunto de matrices*

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

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

Ejercicio 5.6. *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 5.7. *Demuestre que los grupos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos.*

Ejercicio 5.8. *Asociemos a cada elemento del grupo de cuaterniones Q_8 una matriz compleja de la siguiente manera:*

$$\pm 1 \mapsto \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \pm i \mapsto \begin{pmatrix} \pm\sqrt{-1} & 0 \\ 0 & \mp\sqrt{-1} \end{pmatrix},$$
$$\pm j \mapsto \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \quad \pm k \mapsto \begin{pmatrix} 0 & \pm\sqrt{-1} \\ \pm\sqrt{-1} & 0 \end{pmatrix}.$$

Demuestre que esta correspondencia es un monomorfismo $Q_8 \rightarrowtail \mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C})$.

Ejercicio 5.9. *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* $\mathrm{GL}_n(R)$*. Demuestre que la aplicación*

$$\begin{pmatrix} * & * & * & \cdots & * & * \\ 0 & * & * & \cdots & * & * \\ 0 & 0 & * & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & * & * \\ 0 & 0 & 0 & \cdots & 0 & * \end{pmatrix} \mapsto \begin{pmatrix} * & 0 & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & \cdots & 0 & 0 \\ 0 & 0 & * & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & * & 0 \\ 0 & 0 & 0 & \cdots & 0 & * \end{pmatrix}$$

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

Ejercicio 5.10. *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* $e^{A+B} \neq e^A \cdot e^B$*.*

Indicación: considere $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *y* $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$*.*

Ejercicio 5.11. *En los ejercicios para el capítulo anterior hemos mencionado el grupo de matrices ortogonales*

$$O_n(k) = \{A \in \mathrm{GL}_n(k) \mid A^t A = A A^t = I\}.$$

1) *Demuestre que el determinante de una matriz ortogonal es igual a* ± 1*.*
   Indicación: el determinante es un homomorfismo y $\det A^t = \det A$*.*

2) *Demuestre que las matrices ortogonales de determinante* $+1$ *forman un subgrupo*

$$SO_n(k) := \{A \in \mathrm{GL}_n(k) \mid A^t A = A A^t = I,\ \det A = +1\} \subset O_n(k).$$

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

3) *Demuestre que el grupo* $\mathrm{SO}_2(\mathbb{R})$ *es isomorfo al grupo del círculo* $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$*.*