

# Estructuras Algebraicas

Victoria Torroja Rubio

8/9/2025

# Índice general

<b>0. Preliminares</b>	<b>3</b>
0.1. Divisibilidad . . . . .	3
0.2. Factorización . . . . .	6
0.3. Aritmética modular . . . . .	7
<b>1. Grupos</b>	<b>8</b>

**Profesor:** Adrián Barcelo

**Correo:** abacelo@ucm.es

**Despacho:** 443

**Evaluación**

- 15 % Trabajo a entregar
- 20 % Ejercicios/prácticas a entregar/hacer
- 65 % Examen final (hay que sacar al menos un 4 para que haga media con la evaluación continua)

# Capítulo 0

## Preliminares

Recordamos que  $\mathbb{N} = \{1, 2, \dots\}$  es el conjunto de los **números naturales** y  $\mathbb{Z} = \{\dots, -1, -1, 0, 1, 2, \dots\}$  es el conjunto de **números enteros**. Tomamos la suma y el producto tal y como los conocemos  $(+, \cdot)$ . Además, dotas a  $\mathbb{N}$  y  $\mathbb{Z}$  del orden que conocemos  $(<)$ . En  $\mathbb{N}$ , tenemos el **principio del buen orden**.

**Teorema 0.1 (Principio del buen orden).** Todo subconjunto no vacío de  $\mathbb{N}$  tiene un elemento mínimo.

Recordemos también que dado  $z \in \mathbb{Z}$ , su valor absoluto  $|z|$  es asignar el valor positivo de  $z$ . En concreto,

$$|z| = \begin{cases} z, & z \geq 0 \\ -z, & z < 0 \end{cases}.$$

Además, se cumple que

$$|z_1| \leq |z_1 \cdot z_2|, \quad \forall z_1, z_2 \in \mathbb{Z} / \{0\}.$$

### 0.1. Divisibilidad

**Teorema 0.2.** Sean  $n, m \in \mathbb{Z}$  con  $m \neq 0$ . Así, existen  $q, r \in \mathbb{Z}$  únicos tales que  $n = mq + r$  y  $0 \leq r < |m|$ .

**Demostración.** Estudiemos primero la existencia. Supongamos que  $m > 0$  y consideremos el siguiente subconjunto

$$X = \{n - mk \mid k \in \mathbb{Z}, n - mk \geq 0\} \subset \mathbb{N}.$$

Tenemos que este subconjunto es no vacío. En efecto, si  $n \geq 0$  tenemos que  $n = n - m \cdot 0 \in X$ . Si  $n < 0$ , tenemos que  $n(1 - m) \in X$ . Así, tenemos que  $X \neq \emptyset$ . Así, podemos aplicar el principio del buen orden, por lo que existe un elemento mínimo  $r$ . Así, tenemos que existe  $q \in \mathbb{Z}$  tal que

$$r = n - mq, \quad r \geq 0.$$

Además, tenemos que

$$n - (q + 1)m = n - qm - m = r - m < r.$$

Por tanto,  $n - (q + 1)m \notin X$  por ser  $r$  el mínimo. Entonces, necesariamente tenemos que  $n - (q + 1)m < 0$ , por lo que  $r < m \leq |m|$ . Ahora, si  $m < 0$ , hemos visto que  $r_1, q_1 \in \mathbb{Z}$  tales que  $n = (-m)q_1 + r_1$  con  $0 \leq r_1 < |m|$ . Es trivial que esto demuestra el teorema, puesto que  $-q_1 \in \mathbb{Z}$ .

Ahora demostramos la unicidad. Supongamos que existen  $q_1, q_2, r_1, r_2 \in \mathbb{Z}$  tales que

$$n = mq_1 + r_1, \quad n = mq_2 + r_2.$$

Supongamos sin pérdida de generalidad que  $r_1 \leq r_2$ . Así, tenemos que

$$(q_1 - q_2)m = r_2 - r_1 \Rightarrow |q_1 - q_2||m| = r_2 - r_1.$$

Así, si  $r_1 \neq r_2$ , tenemos que  $|q_1 - q_2| \geq 1$ . Por tanto, se tiene que

$$|q_1 - q_2||m| \geq |m| > r_2 \geq r_2 - r_1.$$

Así, hemos obtenido una contradicción, por lo que debe ser que  $r_1 = r_2$  y, consecuentemente,  $q_1 = q_2$ .  $\square$

**Observación.** A los números  $n, m, q$  y  $r$  los llamamos **dividendo**, **divisor**, **cociente** y **resto**, respectivamente.

**Definición 0.1.** Dados  $a, b \in \mathbb{Z}$ , decimos que  $a$  divide a  $b$ ,  $a|b$ , si existe  $c \in \mathbb{Z}$  tal que  $b = ac$ .

Recordemos que si  $c|a$  y  $c|b$ , entonces  $c|a + b$ . En efecto,

$$a + b = ck_1 + ck_2 = c(k_1 + k_2).$$

**Proposición 0.1.** Sean  $a, b, c \in \mathbb{Z}$ ,

**Reflexiva.**  $a|a$ .

**Antisimétrica.**  $a|b, b|a \Rightarrow a = b$ .

**Transitiva.**  $a|b, b|c \Rightarrow a|c$ .

**Demostración.** La propiedad reflexiva es trivial, puesto que  $a = a \cdot 1, \forall a \in \mathbb{Z}$ . En cuanto a la propiedad antisimétrica, tenemos que si  $a|b$  y  $b|a$ , entonces  $a = \lambda_1 b$  y  $b = \lambda_2 a$ . Así, tenemos que  $a \leq b$  pero también tenemos que  $b \leq a$ , por lo que debe ser que  $b = a$ . Finalmente, para demostrar la propiedad transitiva basta ver que si  $b = \lambda a$  y  $c = \mu b$ , se tiene que  $c = \mu\lambda a$ , por lo que  $a|c$ .  $\square$

**Observación.** Tenemos entonces, que la relación de divisibilidad es una **relación de orden parcial**.

**Definición 0.2 (Máximo común divisor).** Sean  $n, m \in \mathbb{Z}$  y  $d \in \mathbb{Z}$ . Diremos que  $d$  es **divisor común** de  $n$  y  $m$  si  $d|n$  y  $d|m$ . Llamaremos **máximo común divisor** de  $n$  y  $m$ ,  $\text{mcd}(n, m)$  al más grande de los divisores comunes positivos.

**Observación.** Dado que el máximo común divisor es positivo, es único.

**Proposición 0.2.** Sean  $a, b \in \mathbb{Z}$ , entonces se cumple:

1. Existe el máximo común divisor de  $a$  y  $b$ .
2. **Identidad de Bézout.** Existen  $x, y \in \mathbb{Z}$  tales que si  $d = \text{mcd}(a, b)$  entonces  $d = ax + by$ .

**Demostración.** La demostración de 1 y 2 es la misma. Sean  $a, b \in \mathbb{Z}$  y consideremos el siguiente conjunto:

$$S = \{\lambda a + \mu b : \lambda, \mu \in \mathbb{Z}, \lambda a + \mu b > 0\} \subset \mathbb{N}.$$

Está claro que  $S \neq \emptyset$ , pues supongamos sin pérdida de generalidad que  $a > b$ , entonces  $a - b > 0 \in S$ . Así, por el principio del buen orden, tenemos que existe un elemento mínimo de  $S$  al que llamaremos  $d$ . Así, existen  $x, y \in \mathbb{Z}$  tales que  $d = ax + by$ . Vamos a ver que  $d = \text{mcd}(a, b)$ . En primer lugar, vamos a ver que es divisor común de  $a$  y  $b$ . Tenemos que, por el algoritmo de la divisibilidad, existen  $q, r \in \mathbb{Z}$  con  $0 \leq r < d$  tales que

$$a = qd + r.$$

Si  $r > 0$ , tenemos que

$$r = a - qd = a - q(ax + by) = (1 - qx)a + yb \in S.$$

Así, tenemos que  $r \geq d$  pero también  $r < d$ , lo que es una contradicción. Por tanto, debe ser que  $r = 0$ , por lo que  $d|a$ . De manera análoga se demuestra que  $d|b$ . Así, queda demostrado que  $d$  es divisor común de  $a$  y  $b$ . Ahora, supongamos que  $d'$  es también divisor común de  $a$  y  $b$ . Así, existen  $k_1, k_2 \in \mathbb{Z}$  tales que  $a = k_1 d'$  y  $b = k_2 d'$ . De esta manera queda que

$$d = xa + yb = xk_1 d' + yk_2 d' = (xk_1 + yk_2) d'.$$

Así, tenemos que  $d' \leq d$ , por lo que  $d = \text{mcd}(a, b)$ . □

Así, sabemos que existe el máximo común divisor, pero ahora necesitamos una manera de calcularlo. Para ello haremos uso del algoritmo de Euclides, que nos va a permitir también encontrar una identidad de Bézout.

**Lema 0.1.** Sean  $a, b, r \in \mathbb{Z}$  tales que  $0 \leq r < b$ . Si existe  $q \in \mathbb{Z}$  tal que  $a = bq + r$ , entonces  $\text{mcd}(a, b) = \text{mcd}(b, r)$ .

**Demostración.** Supongamos las condiciones del lema. Tenemos que, claramente  $\text{mcd}(a, b) | r$ . Así,  $\text{mcd}(a, b)$  es divisor común de  $b$  y  $r$ , por lo que  $\text{mcd}(a, b) \leq \text{mcd}(b, r)$ . Por otro la-

do, tenemos que  $\text{mcd}(b, r) \mid a$ , por lo que es divisor común de  $b$  y  $a$  y, consecuentemente,  $\text{mcd}(b, r) \leq \text{mcd}(a, b)$ . Así, tenemos que  $\text{mcd}(a, b) = \text{mcd}(b, r)$ .  $\square$

**Teorema 0.3 (Algoritmo de Euclides).** Sean  $a, b \in \mathbb{Z}$ ,  $a > b$  y vamos a dividir  $a$  entre  $b$ . Así,  $a = bq_1 + r_1$ ,  $q_1 \in \mathbb{Z}$ ,  $0 < r_1 < |b|$ .

- Si  $r_1 = 0$ , entonces  $b \mid a$  y  $\text{mcd}(a, b) = b$ .
- Si  $r_1 \neq 0$ , entonces aplicando el lema tenemos que  $\text{mcd}(a, b) = \text{mcd}(b, r_1)$ . Así, dividimos  $b$  entre  $r_1$  y obtenemos  $b = r_1q_2 + r_2$ , y aplicamos el mismo razonamiento de antes hasta obtener un  $r_k = 0$  y tendremos que  $r_{k-1} = \text{mcd}(a, b)$ .

Sabemos que este proceso es finito por el principio del buen orden y porque  $r_i$  se hace cada vez más pequeño.

Reconstruyendo las igualdades obtenidas en el algoritmo de Euclides podemos obtener una identidad de Bézout.

## 0.2. Factorización

**Definición 0.3.** Sea  $a \in \mathbb{Z} / \{-1, 0, 1\}$ .

1. Diremos que  $a$  es **primo** si  $a \mid bc \Rightarrow a \mid b \vee a \mid c$ .
2. Diremos que  $a$  es **irreducible** si  $a = bc \Rightarrow b = \pm 1 \vee c = \pm 1$ .

**Observación.** Si  $a \in \mathbb{N}$ ,  $a$  es irreducible si sus únicos divisores son 1 y  $a$ . Además, si  $a \in \mathbb{Z}$ , entonces  $a$  es primo si y solo si es irreducible. En efecto, si  $a$  es irreducible y  $a \mid bc$  pero  $a$  no divide a  $b$ , tenemos que  $\text{mcd}(a, b) = 1$ . Así, existen  $\lambda, \mu \in \mathbb{Z}$  tales que

$$1 = \lambda a + \mu b.$$

De esta forma, se tiene que, dado que  $bc = ak$  con  $k \in \mathbb{Z}$ ,

$$c = c\lambda a + c\mu b = c\lambda a + k\mu a = (c\lambda + k\mu) a.$$

Así, tenemos que  $a$  es primo.

**Teorema 0.4 (Teorema fundamental de la aritmética).** Sea  $n \in \mathbb{Z} / \{-1, 0, 1\}^a$ , entonces  $n$  es producto finito de enteros irreducibles de forma única salvo reordenación. Esto es, existen  $p_1, \dots, p_k \in \mathbb{Z}$  y  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$  tales que  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ .

<sup>a</sup>Si  $n < 0$  consideramos la descomposición de  $|n|$  y lo multiplicamos por  $-1$ .

**Corolario.** Sean  $a, b \in \mathbb{Z}$  y  $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  y  $b = q_1^{\beta_1} \cdots q_t^{\beta_t}$ , con  $p_i, q_i \in \mathbb{Z}$  irreducibles y  $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$ . Así, definimos el  $\text{mcd}(a, b)$  como los enteros irreducibles comunes elevados al menor exponente. Es decir, si  $p_i = q_i$  para  $i = 1, \dots, s$  con  $s < t, k$ , tenemos que

$$\text{mcd}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_s^{\min\{\alpha_s, \beta_s\}}.$$

### 0.3. Aritmética modular

**Definición 0.4.** Sean  $a, m \in \mathbb{Z}$  y  $n \in \mathbb{N}$ . Diremos que  $a$  es **congruente** con  $m$  módulo  $n$  si  $a - m = kn$  para  $k \in \mathbb{Z}$ ,  $a \equiv m \pmod{n}$ .

**Observación.** También podemos decir que  $m$  es el resto de dividir  $a$  entre  $n$ .

Las congruencias respetan las operaciones, es decir si  $a_1 \equiv m_1 \pmod{n}$  y  $a_2 \equiv m_2 \pmod{n}$  tenemos que

$$a_1 + a_2 \equiv m_1 + m_2 \pmod{n}.$$

Con la resta funciona igual. Además, si  $b \in \mathbb{Z}$ ,

$$ba_1 \equiv bm_1 \pmod{n}.$$

**Teorema 0.5 (Teorema chino del resto).** Sea el sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_t \pmod{n_t} \end{cases},$$

tal que  $a_1, \dots, a_t \in \mathbb{Z}$ ,  $n_1, \dots, n_t \in \mathbb{N}$  tal que  $\text{mcd}(n_i, n_j) = 1$ ,  $\forall i \neq j$ . Entonces, el sistema tiene solución y estas soluciones están en la misma clase de equivalencia módulo  $n = n_1 \cdots n_t$ .



# Capítulo 1

## Grupos

**Definición 1.1 (Grupo).** Sea la terna  $(G, \cdot, e)$  donde  $G$  es un conjunto no vacío,  $\cdot : G \times G \rightarrow G$  una operación interna y  $e \in G$ . Diremos que la terna  $(G, \cdot, e)$  es un **grupo** si se cumple:

**Asociativa.**  $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ .

**Elemento neutro.**  $\forall a \in G, a \cdot e = e \cdot a = a$ .

**Inversa.**  $\forall a \in G, \exists b \in G, a \cdot b = b \cdot a = e$ .

Además, diremos que  $(G, \cdot, e)$  es **abeliano** si se cumple la propiedad conmutativa, es decir,  $\forall a, b \in G, a \cdot b = b \cdot a$ .

**Definición 1.2 (Orden de un grupo).** Dado un grupo  $(G, \cdot, e)$ , llamamos **orden** del grupo a la cardinalidad de  $G$ ,  $|G|$ .

**Ejemplo.** Algunos ejemplos de grupos son:

1.  $(\mathbb{R}, +, 0)$  es un grupo abeliano.
2.  $(\mathbb{R}/\{0\}, \cdot, 1)$  es un grupo abeliano.
3.  $(\mathbb{Z}, +, 0)$  es un grupo abeliano.
4.  $(\mathbb{N} \cup \{0\}, +, 0)$  no es un grupo por no haber inversos.

**Proposición 1.1.** Sea  $(G, \cdot, e)$  un grupo. Entonces se tiene que:

1. El elemento neutro es único.
2. Dado  $a \in G$ , existe un único elemento inverso.

**Demostración.** Demostremos 1. Supongamos que  $e$  y  $e'$  son ambos elementos neutros.

Tenemos que

$$e = e \cdot e' = e' \cdot e = e'.$$

Así, hemos visto que  $e = e'$ . Ahora, demostremos **2**. Si  $a \in G$ , supongamos que  $b, c \in G$  son sus inversos. Entonces tenemos que

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

Así, tenemos que  $b = c$ .  $\square$

**Observación.** 1. De ahora en adelante, en vez de escribir  $(G, \cdot, e)$  para nombrar el grupo, escribiremos sólo  $G$ . De manera similar, no escribiremos  $a \cdot b$  sino  $ab$ .

2. Dado  $a \in G$  finito, a su inverso lo denotaremos por  $a^{-1}$ .

3. Dado un grupo  $G$ , va a estar totalmente definido por su tabla de multiplicación (tabla de Cayley). Esta será de la forma

	$e$	$a_1$	$\cdots$	$a_n$
$e$	$e$	$a_1$	$\cdots$	$a_n$
$a_1$	$a_1$	$a_1^2$	$\cdots$	$a_1 a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_n$	$a_n$	$a_n a_1$	$\cdots$	$a_n^2$

**Ejemplo.** Consideremos el grupo  $(\mathbb{Z}_5 / \{0\}, \cdot)$ . Su tabla de Cayley será:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

**Proposición 1.2.** Sea  $G$  un grupo. Entonces,

1.  $\forall a \in G, (a^{-1})^{-1} = a$ .
2.  $\forall a, b, c \in G, (ab)^{-1} = b^{-1}a^{-1}$ .
3.  $\forall a, b, c \in G$ , si  $ba = ca$  o  $ab = ac$ , entonces  $b = c$ .

**Demostración.** Demostramos **1**. Si  $a \in G$ , tenemos que

$$a^{-1}a = a \cdot a^{-1} = e.$$

Dado que el inverso es único, tenemos que  $(a^{-1})^{-1} = a$ . Ahora demostramos **2**. Si  $a, b \in G$ ,

$$(ab)(b^{-1}a^{-1}) = aeb^{-1} = aa^{-1} = e.$$

Por la inversa del inverso, tenemos que  $(ab)^{-1} = b^{-1}a^{-1}$ . Finalmente, demostramos **3**. Si  $a, b, c \in G$  y, sin pérdida de generalidad,  $ba = ca$ , dado que existe  $a^{-1} \in G$ , tenemos

que

$$ba = ca \iff baa^{-1} = caa^{-1} \iff be = ce \iff b = c.$$

□

**Ejemplo.** 1. Consideremos un conjunto  $X \neq \emptyset$  y el conjunto de sus biyecciones  $\text{Biy}(X) = \{f : X \rightarrow X : f \text{ biyección}\}$ . Como operación tomamos la composición de funciones. Entonces,  $(\text{Biy}(X), \circ)$  es un grupo. En efecto:

**Asociativa.** La composición de funciones es asociativa.

**Elemento neutro.** Tomamos como elemento neutro la función identidad. En efecto,  $id \in \text{Biy}(X)$  y  $\forall f \in \text{Biy}(X)$ ,

$$(f \circ id)(x) = f(id(x)) = f(x).$$

$$(id \circ f)(x) = id(f(x)) = f(x).$$

**Inverso.** Si  $f \in \text{Biy}(X)$ , sabemos que por ser  $f$  biyectiva existe  $f^{-1} \in \text{Biy}(X)$  tal que  $f \circ f^{-1} = id$  y  $f^{-1} \circ f = id$ .

Así, hemos visto que  $(\text{Biy}(X), \circ)$  es un grupo, pero no tiene por qué ser abeliano.

2. Sea  $\mathcal{M}_n(\mathbb{R})$ ,  $n \geq 1$ , el conjunto de matrices reales cuadradas con coeficientes en  $\mathbb{R}$ , y consideremos el producto de matrices usual. El par  $(\mathcal{M}_n, \cdot)$  no es un grupo, puesto que las matrices con determinante nulo no tienen inverso.

Tomemos así solo las matrices cuyo determinante es distinto de cero, y por tanto sabemos que tienen inverso. A este conjunto lo llamamos **grupo lineal general**,  $\text{GL}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : |A| \neq 0\}$ . Así,  $(\text{GL}_n(\mathbb{R}), \cdot)$  forma un grupo.

De manera similar, el conjunto  $\text{SL}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : |A| = 1\}$ , al que llamamos **grupo lineal especial**, también forma un grupo con la multiplicación.

**Observación.** Se puede ver que  $\text{SL}_n(\mathbb{R}) \subset \text{GL}_n(\mathbb{R})$ .

**Definición 1.3 (Subgrupo).** Sea  $G$  un grupo y  $H \subset G$ . Diremos que  $H$  es **subgrupo** de  $G$ ,  $H \leq G$ , si  $H$  es cerrado para la operación de  $G$ , esto es

- $H \neq \emptyset$ .
- $\forall a, b \in H, ab \in H$ .
- $\forall a \in H, a^{-1} \in H$ .

**Ejemplo.** (i) Sea  $G$  un grupo. Tenemos que  $\{e\} \leq G$  es el **subgrupo trivial**.

(ii)  $\text{SL}_n(\mathbb{R}) \leq \text{GL}_n(\mathbb{R})$ .

(iii)  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ .

(iv)  $\mathbb{Q}/\{0\} \leq \mathbb{R}/\{0\} \leq \mathbb{C}/\{0\}$ .

**Proposición 1.3.** Sea  $G$  un grupo y  $H \subset G$ . Así,  $H \leq G$  si y solo si  $e \in H$  y  $\forall a, b \in H$  se cumple que  $ab^{-1} \in H$ .

**Demostración.** Demostremos la primera implicación. Si  $H \leq G$ , tenemos que  $H \neq \emptyset$  por lo que existe  $a \in H$ , por lo que  $a^{-1} \in H$  y  $e = aa^{-1} \in H$ . Ahora, si  $a, b \in H$ , tenemos que  $b^{-1} \in H$ , por lo que  $ab^{-1} \in H$ . Recíprocamente,  $H \neq \emptyset$  puesto que  $e \in H$ . Sea  $a \in H$ . Tenemos que  $a^{-1} = e \cdot a^{-1} \in H$ . Falta que si  $a, b \in H$ , entonces  $ab \in H$ . Sean  $a, b \in H$ , entonces  $a^{-1}, b^{-1} \in H$ . Entonces  $ab = a(b^{-1})^{-1} \in H$ . Así, demostramos las tres propiedades.  $\square$

**Ejemplo (Producto cartesiano de dos grupos).** Sean  $(G_1, \cdot_{G_1}, e_{G_1})$  y  $(G_2, \cdot_{G_2}, e_{G_2})$  dos grupos. Vamos a ver que su producto cartesiano también es un grupo. Definimos la siguiente operación para el producto cartesiano:

$$\begin{aligned} \cdot : (G_1 \times G_2) \times (G_1 \times G_2) &\rightarrow G_1 \times G_2 \\ (g_1, g_2) \times (g'_1, g'_2) &\rightarrow (g_1 \cdot_{G_1} g'_1, g_2 \cdot_{G_2} g'_2). \end{aligned}$$

Está claro que  $G = G_1 \times G_2 \neq \emptyset$  y que se trata de una operación interna.

**Asociatividad.** Si  $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ , tenemos que

$$\begin{aligned} ((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) &= (a_1 \cdot b_1, a_2 \cdot b_2) \cdot (c_1, c_2) = (a_1 \cdot b_1 \cdot c_1, a_2 \cdot b_2 \cdot c_2) \\ &= (a_1, a_2) \cdot (b_1 \cdot c_1, b_2 \cdot c_2) = (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2)). \end{aligned}$$

**Elemento neutro.** Tenemos que  $e = (e_{G_1}, e_{G_2})$ . En efecto, si  $(g_1, g_2) \in G_1 \times G_2$ , tenemos que

$$\begin{aligned} (e_{G_1}, e_{G_2}) \cdot (g_1, g_2) &= (g_1, g_2) \\ (g_1, g_2) \cdot (e_{G_1}, e_{G_2}) &= (g_1, g_2). \end{aligned}$$

**Inverso.** Si  $(g_1, g_2) \in G_1 \times G_2$ , tenemos que su inverso será  $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$ . En efecto,

$$\begin{aligned} (g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) &= (e_{G_1}, e_{G_2}) \\ (g_1^{-1}, g_2^{-1}) \cdot (g_1, g_2) &= (e_{G_1}, e_{G_2}). \end{aligned}$$

Así, está claro que  $G_1 \times G_2$  es un grupo.

**Definición 1.4.** Sea  $G$  un grupo. Entonces,

(a) Llamamos **centro** de  $G$  al conjunto

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\}.$$

(b) Llamamos **centralizador** de  $x \in G$  al conjunto

$$C_G(x) = \{a \in G : ax = xa\}.$$

**Observación.** Los conjuntos  $Z(G)$  y  $C_G(x)$  son subgrupos. En efecto:

- (i) Tenemos que  $e \in Z(G)$  y si  $a \in Z(G)$ , también tenemos que  $a^{-1} \in Z(G)$ . En efecto,

$$a^{-1}x = xa^{-1} \iff aa^{-1}x = axa^{-1} \iff x = xaa^{-1} = xe = x.$$

Así, si  $a, b \in Z(G)$ , tenemos que  $b^{-1} \in Z(G)$  y  $\forall x \in G$ ,

$$ab^{-1}x = axb^{-1} = xab^{-1}.$$

Por lo que  $ab^{-1} \in Z(G)$  y se trata de un subgrupo.

- (ii) El argumento para demostrar que  $C_G(x)$  es un subgrupo de  $G$  es análogo al anterior.

**Observación.** Se puede comprobar que  $Z(G) = \bigcap_{x \in G} C_G(x)$ . En efecto:

- (i) Si  $x \in Z(G)$  tenemos que  $\forall g \in G, xg = gx$ , por lo que  $\forall g \in G, x \in C_G(g) \iff x \in \bigcap_{g \in G} C_G(g)$ .

- (ii) Si  $x \in \bigcap_{g \in G} C_G(g)$ ,  $x \in C_G(g)$ ,  $\forall g \in G$ . Por lo que  $xg = gx$ ,  $\forall g \in G$  y  $x \in Z(G)$ .

**Definición 1.5 (Homomorfismo).** Sean  $G_1$  y  $G_2$  grupos tales que  $\cdot_{G_1}$  y  $\cdot_{G_2}$  son sus operaciones y  $e_{G_1}$  y  $e_{G_2}$  sus elementos neutros. Entonces,  $f : G_1 \rightarrow G_2$  es un **homomorfismo** de grupos si  $\forall a, b \in G_1$ ,

$$f(a \cdot_{G_1} b) = f(a) \cdot_{G_2} f(b).$$

**Observación.** Si  $f_1 : G_1 \rightarrow G_2$  y  $f_2 : G_2 \rightarrow G_3$  son homomorfismos de grupos, entonces  $f_2 \circ f_1$  es un homomorfismo de grupos. Es decir, la composición de homomorfismos de grupos sigue siendo homomorfismo de grupos. En efecto, si  $a, b \in G_1$ ,

$$f_2 \circ f_1(ab) = f_2(f_1(ab)) = f_2(f_1(a)f_1(b)) = f_2(f_1(a))f_2(f_1(b)) = f_2 \circ f_1(a)f_2 \circ f_1(b).$$

**Ejemplo.** Consideremos la aplicación

$$f : \mathbb{R}/\{0\} \rightarrow \text{GL}_n(\mathbb{R})$$

$$t \rightarrow \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & t & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t \end{pmatrix} = t \cdot I_n.$$

Esta aplicación es un homomorfismo de grupos.

**Definición 1.6.** Sea  $f : G_1 \rightarrow G_2$  homomorfismo de grupos. Entonces:

- (a) Llamamos **núcleo** de  $f$  al conjunto

$$\text{Ker}(f) = \{a \in G_1 : f(a) = e_{G_2}\}.$$

- (b) Llamamos **imagen** de  $f$  al conjunto

$$\text{Im}(f) = \{b \in G_2 : \exists a \in G_1, f(a) = b\}.$$

**Proposición 1.4.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Entonces:

1.  $f(e_{G_1}) = e_{G_2}$ .
2.  $\forall a \in G_1, f(a^{-1}) = f(a)^{-1}$ .
3. Si  $H \leq G_1$ , entonces  $f(H) \leq G_2$ . En particular, tenemos que  $\text{Im}(f) \leq G_2$ .
4.  $f$  es inyectiva si y solo si  $\text{Ker}(f) = \{e_{G_1}\}$ .
5. Si  $N \leq G_2$ , entonces  $f^{-1}(N) \leq G_1$  que contiene a  $\text{Ker}(f)$ .

**Demostración.** 1. Sabemos que  $e_{G_1} = e_{G_1} \cdot e_{G_1}$ , por lo que:

$$f(e_{G_1}) = f(e_{G_1} \cdot e_{G_1}) = f(e_{G_1}) f(e_{G_1}).$$

Así, tenemos que

$$\begin{aligned} e_{G_2} &= f(e_{G_1})^{-1} f(e_{G_1}) = f(e_{G_1})^{-1} (f(e_{G_1}) f(e_{G_1})) \\ &= (f(e_{G_1})^{-1} f(e_{G_1})) f(e_{G_1}) = e_{G_2} f(e_{G_1}) = f(e_{G_1}). \end{aligned}$$

2. Sea  $a \in G_1$ , entonces por la unicidad del inverso y por **1**:

$$f(a) f(a^{-1}) = f(aa^{-1}) = f(e_{G_1}) = e_{G_2}.$$

3. Si  $H \leq G_1$ , tenemos que  $e_{G_1} \in H$ , por lo que  $e_{G_2} \in f(H)$ . Además, tenemos que  $\forall a, b \in H$  se cumple que  $ab^{-1} \in H$ . Por tanto, si  $x, y \in f(H)$ ,  $\exists a, b \in H$  tales que  $x = f(a)$  y  $y = f(b)$ , de esta manera, tenemos que  $ab^{-1} \in H$ , por lo que  $f(ab^{-1}) \in f(H)$ . Así,

$$xy^{-1} = f(a) f(b)^{-1} = f(a) f(b^{-1}) = f(ab^{-1}) \in f(H).$$

Así, queda demostrado que  $f(H) \leq G_2$ .

4. Si  $\text{Ker}(f) = \{e_{G_1}\}$  y  $f(a) = f(b)$ , tenemos que

$$f(a) f(b)^{-1} = e_{G_2} \iff f(ab^{-1}) = e_{G_2}.$$

Por tanto,  $ab^{-1} = e_{G_1}$ , por lo que  $a = b$ . Así, hemos visto que  $f$  es inyectiva. Supongamos que  $f$  es inyectiva y que  $a \in \text{Ker}(f)$ . Entonces, tenemos que  $f(a) = f(e_{G_1}) = e_{G_2}$ , por lo que  $a = e_{G_1}$  y  $\text{Ker}(f) = \{e_{G_1}\}$ .

5. Supongamos que  $N \leq G_2$ . Tenemos que  $e_{G_2} \in N$ , por lo que  $e_{G_1} \in f^{-1}(N)$ . Si  $x, y \in f^{-1}(N)$  tenemos que  $f(x), f(y) \in N$ , así,

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

Por tanto,  $\forall x, y \in f^{-1}(N)$ , tenemos que  $xy^{-1} \in f^{-1}(N)$ , por lo que  $f^{-1}(N) \leq G_1$ . Ahora, si  $x \in \text{Ker}(f)$ , tenemos que  $f(x) = e_{G_2} \in N$ , por lo que  $x \in f^{-1}(N)$  y consecuentemente  $\text{Ker}(f) \leq f^{-1}(N)$ .  $\square$

**Ejemplo.** 1. Consideremos  $f_m : \mathbb{Z} \rightarrow \mathbb{Z}$  con  $m \in \mathbb{Z}$ , con la suma, tal que  $f(z) = mz$ . Tenemos que  $f_m$  es un homomorfismo de grupos. Por proposición anterior, tenemos que

$$m\mathbb{Z} := f(\mathbb{Z}) = \{z \in \mathbb{Z} : z = km, k \in \mathbb{Z}\} \leq \mathbb{Z}.$$

Similarmente, tenemos que  $\text{Ker}(f_m)$  es el subgrupo trivial si  $m \neq 0$  y es  $\mathbb{Z}$  si  $m = 0$ .

2. Es homomorfismo la aplicación  $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}/\{0\} : M \rightarrow \det(M)$ . En concreto, se trata de un homomorfismo sobreyectivo. Además, podemos ver que  $\text{Ker}(\det) = \text{SL}_n(\mathbb{R})$ .

**Definición 1.7 (Isomorfismo y automorfismo).** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Si  $f$  es biyectiva, entonces  $f$  es un **isomorfismo** y lo escribimos  $G_1 \cong G_2$ . Si  $f : G_1 \rightarrow G_1$  es un isomorfismo, se llama **automorfismo**.

**Observación.** 1. Si  $G_1 \cong G_2$  tenemos que  $|G_1| = |G_2|$  y tienen la misma tabla de Cayley.

2. Si  $f : G_1 \rightarrow G_2$  es un isomorfismo, tenemos que  $f^{-1} : G_2 \rightarrow G_1$  también lo es. En efecto, Si  $x, y \in G_2$  existen  $a, b \in G_1$  tales que  $x = f(a)$  e  $y = f(b)$ . Así,

$$f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y).$$

3. Si  $f : G_1 \rightarrow G_2$  es un homomorfismo sobreyectivo, tenemos que  $f(G_1) \cong G_2$ , es decir,  $\text{Im}(f) \cong G_2$ .
4. Si  $f : G_1 \rightarrow G_2$  es un homomorfismo inyectivo, entonces  $G_1 \cong \text{Im}(f)$ .
5. La relación de ser isomorfo es una relación de equivalencia.
6. El conjunto de automorfismos de  $G$ ,  $\text{Aut}(G)$ , es un subgrupo de  $\text{Biy}(G)$ .