Estructuras Algebraicas

Victoria Torroja Rubio

8/9/2025

Índice general

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 $\mathbb{N} = \{1, 2, \ldots\}$ es el conjunto de los **números naturales** y $\mathbb{Z} = \{\ldots, -1, -1, 0, 1, 2, \ldots\}$ 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 bueno orden, por lo que existe un elemento mínimo r. Así, tenemos que existe $q \in \mathbb{Z}$ tal que

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

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, $\operatorname{mcd}(n, m)$ 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 $d = \operatorname{mcd}(a, b)$ 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 $d = \operatorname{mcd}(a, b)$. 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 $r|b$. 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 $d = \operatorname{mcd}(a, b)$. □

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

Demostración. Supongamos las condiciones del lema. Tenemos que, claramente $\operatorname{mcd}(a, b)\,|r$. Así, $\operatorname{mcd}(a, b)$ es divisor común de b y r, por lo que $\operatorname{mcd}(a, b) \leq \operatorname{mcd}(b, r)$. Por otro lado, tenemos que $\mathrm{mcd}\,(b,r)\,|a$, por lo que es divisor común de b y a y, consecuentemente, $\mathrm{mcd}\,(b,r) \leq \mathrm{mcd}\,(a,b)$. Así, tenemos que $\mathrm{mcd}\,(a,b) = \mathrm{mcd}\,(b,r)$. □

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 $b|a$ y $\mathrm{mcd}\,(a,b) = b$.
- Si $r_1 \neq 0$, entonces aplicando el lema tenemos que $\mathrm{mcd}\,(a,b) = \mathrm{mcd}\,(b,r_1)$. 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 $r_{k-1} = \mathrm{mcd}\,(a,b)$.

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 $a|bc \Rightarrow a|b \vee a|c$.
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 $a|bc$ pero a no divide a b, tenemos que $\mathrm{mcd}\,(a,b) = 1$. 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 $p_1, \ldots, p_k \in \mathbb{Z}$ y $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ tales que $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

[a] Si $n < 0$ consideramos la descomposición de $|n|$ y lo multiplicamos por -1.

Corolario 0.1. 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 $\mathrm{mcd}\,(a,b)$ como los enteros irreducibles comunes elevados al menor exponente. Es decir, si $p_i = q_i$ para $i = 1, \ldots, s$ con $s < t, k$, tenemos que

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

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 $k \in \mathbb{Z}$, $a \equiv m \mod n$.

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

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

$$a_1 + a_2 \equiv m_1 + m_2 \mod n.$$

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

$$ba_1 \equiv bm_1 \mod n.$$

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

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

tal que $a_1, \ldots, a_t \in \mathbb{Z}$, $n_1, \ldots, n_t \in \mathbb{N}$ tal que $\operatorname{mcd}(n_i, n_j) = 1$, $\forall i \neq j$. 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, $\cdot : G \times G \to G$ 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. $(\mathbb{R}/\left\{0\right\}, \cdot, 1)$ es un grupo abeliano.
3. $(\mathbb{Z}, +, 0)$ es un grupo abeliano.
4. $(\mathbb{N} \cup \left\{0\right\}, +, 0)$ 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 $b = c$. □

Observación.

1. De ahora en adelante, en vez de escribir $(G, \cdot, e)$ para nombrar el grupo, escribiremos sólamente 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. $\forall a \in G$, $\left(a^{-1}\right)^{-1} = a$.
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 $\left(a^{-1}\right)^{-1} = a$. Ahora demostramos **2**. Si $a, b \in G$,

$$(ab)\left(b^{-1}a^{-1}\right) = aea^{-1} = aa^{-1} = e.$$

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

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

$\square$

Ejemplo. 1. Consideremos un conjunto $X \neq \emptyset$ y el conjunto de sus biyecciones $\text{Biy}(X) = \{f : X \to X \ : \ f \text{ biyección}\}$. 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 $ab = a\left(b^{-1}\right)^{-1} \in H$. 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:

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

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

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

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 $\left(g_1^{-1}, g_2^{-1}\right) \in G_1 \times G_2$. En efecto,

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

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, $f : G_1 \to G_2$ 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 $f_1 : G_1 \to G_2$ y $f_2 : G_2 \to G_3$ 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

$$\begin{aligned} f : \mathbb{R}/\{0\} &\to \mathrm{GL}_n(\mathbb{R}) \\ t &\to \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & t \end{pmatrix} = t \cdot I_n. \end{aligned}$$

Está aplicación es un homomorfismo de grupos.

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

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

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

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

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

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

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

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

.

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

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

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

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 $f\left(ab^{-1}\right) \in f(H)$. Así,

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

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

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

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

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 $a \in \mathrm{Ker}(f)$. Entonces, tenemos que $f(a) = f(e_{G_1}) = e_{G_2}$, por lo que $a = e_{G_1}$ y $\mathrm{Ker}(f) = \{e_{G_1}\}$.

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,

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

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 $x \in \operatorname{Ker}(f)$, tenemos que $f(x) = e_{G_2} \in N$, por lo que $x \in f^{-1}(N)$ y consecuentemente $\operatorname{Ker}(f) \leq f^{-1}(N)$.

$\square$

Ejemplo.

1. Consideremos $f_m : \mathbb{Z} \to \mathbb{Z}$ 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 $\operatorname{Ker}(f_m)$ es el subgrupo trivial si $m \neq 0$ y es $\mathbb{Z}$ si $m = 0$.
2. Es homomorfismo la aplicación $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}/\{0\} : M \to \det(M)$. En concreto, se trata de un homomorfismo sobreyectivo. Además, podemos ver que $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$.

Definición 1.7 (Isomorfismo y automorfismo)**.** Sea $f : G_1 \to G_2$ un homomorfismo de grupos. Si f es biyectiva, entonces f es un **isomorfismo** y lo escribimos $G_1 \cong G_2$. Si $f : G_1 \to G_1$ 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 $f : G_1 \to G_2$ es un isomorfismo, tenemos que $f^{-1} : G_2 \to G_1$ 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 $f : G_1 \to G_2$ es un homomorfismo sobreyectivo, tenemos que $f(G_1) \cong G_2$, es decir, $\operatorname{Im}(f) \cong G_2$.
4. Si $f : G_1 \to G_2$ es un homomorfismo inyectivo, entonces $G_1 \cong \operatorname{Im}(f)$.
5. La relación de ser isomorfo es una relación de equivalencia.
6. El conjunto de automorfismos de G, $\operatorname{Aut}(G)$, es un subgrupo de $\operatorname{Biy}(G)$.

1.1. Grupos cíclicos

Notación. Sea $(G, \cdot)$ un grupo, $a \in G$ y $k \in \mathbb{Z}$. Entonces utilizaremos la siguiente notación:
$$a^0 = e, \quad a^n = \underbrace{a \cdot a \cdots a}_{n \text{ veces}}, \quad a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ veces}}.$$

Lema 1.1. Sea $(G, \cdot)$ un grupo, $a \in G$ y $k, l \in \mathbb{Z}$. Entonces $a^{l+k} = a^l a^k$ y $\left(a^{-1}\right)^k = a^{-k} = \left(a^k\right)^{-1}$.

Demostración. Está claro que, por la propiedad asociativa, si $l, k \in \mathbb{N}$ (o $l, k \leq 0$, se procede igual):
$$a^{l+k} = \underbrace{a \cdot a \cdots a}_{l+k \text{ veces}} = \underbrace{a \cdot a \cdots a}_{l \text{ veces}} \cdot \underbrace{a \cdot a \cdots a}_{k \text{ veces}} = a^l a^k.$$

Sin pérdida de generalidad, supongamos que $l \leq 0$ y $k > 0$. Entonces, es evidente que

$$a^l a^k = a \cdots a \cdot a^{-1} \cdots a^{-1} = a^{l-k}.$$

Por otro lado, tenemos que

$$\left(a^{-1}\right)^k a^k = \left(a^{-1} \cdots a^{-1}\right) \cdot (a \cdots a) = a^{-1} \cdots a^{-1} \cdot \left(a^{-1} \cdot a\right) \cdot a \cdots a = e.$$

Al haber el mismo número de a^{-1} que de a, está claro que el resultado será el elemento neutro. Por la unicidad del inverso, tenemos que $\left(a^k\right)^{-1} = \left(a^{-1}\right)^k$. $\square$

Notación. Dado un grupo $(G, \cdot)$ y $a \in G$, utilizaremos la siguiente notación:

$$\langle a \rangle = \left\{a^k \ : \ k \in \mathbb{Z}\right\}.$$

Proposición 1.5. Si G es un grupo y $a \in G$, se tiene que $\langle a \rangle \leq G$ y $\langle a \rangle$ es abeliano.

Demostración. Dado que G es un grupo, su operación es cerrada, por lo que $\langle a \rangle \subset G$. Tenemos que $e \in \langle a \rangle$. Por otro lado, si $x, y \in \langle a \rangle$, existen $n, m \in \mathbb{Z}$ tales que $x = a^n$ e $y = a^m$. Así, tenemos que $y^{-1} = a^{-m}$, así, $xy^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$, puesto que $n - m \in \mathbb{Z}$. Además, es abeliano, puesto que

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$$

$\square$

Notación. Si la operación del grupo fuera aditiva, en lugar de a^k escribiríamos ka.

Observación. Está claro que $\langle a \rangle = \left\langle a^{-1} \right\rangle$. En efecto,

$$x \in \langle a \rangle \iff x = a^n, n \in \mathbb{Z} \iff x = \left(a^{-1}\right)^{-n}, n \in \mathbb{Z} \iff x \in \left\langle a^{-1} \right\rangle.$$

Definición 1.8 (Grupo cíclico)**.** Un grupo G es **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$. Decimos que a es **generador** de G o que G **está generado** por a.

Ejemplo. Consideremos el grupo $(\mathbb{Z}, +)$. Tenemos que este grupo es cíclico y tiene dos generadores, 1 y -1. En efecto, se cumple que $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Proposición 1.6. Si G es un grupo cíclico, cualquier subgrupo $H \leq G$ también es cíclico.

Demostración. Supongamos que $H \neq \{e\}$ y $H \neq G$, puesto que estos casos son triviales. Sea $k \in \mathbb{N}$ el más pequeño tal que $a^k \in H$. Podemos observar que dado que $H \leq G$, tenemos que $a^{-k} \in H$. Vamos a ver que $H = \left\langle a^k \right\rangle$.

(i) Si $x \in H$, tenemos que existe $l \in \mathbb{Z}$ tal que $x = a^l$. Por el algoritmo de la división, tenemos que existen $q, r \in \mathbb{Z}$ tales que

$$l = qk + r, \quad 0 \leq r < k.$$

Entonces, tenemos que

$$a^l = a^{qk+r} = \left(a^k\right)^q a^r.$$

Dado que $a^l, \left(a^k\right)^q \in H$, debe ser que $a^r \in H$. Como $k \in \mathbb{N}$ era el menor tal que $a^k \in H$ y $r < k$, debe ser que $r = 0$, por lo que $x = a^l = \left(a^k\right)^q \in H$. Así, hemos visto que $H \leq \left\langle a^k \right\rangle$.

(ii) Por otro lado, si $x \in \left\langle a^k \right\rangle$, tenemos que existe $n \in \mathbb{Z}$ tal que $x = \left(a^k\right)^l \in H$. Así, tenemos que $\left\langle a^k \right\rangle \subset H$.

Así, hemos visto que $H = \left\langle a^k \right\rangle$, por lo que es cíclico. □

Corolario 1.1. Todo $H \leq \mathbb{Z}$ es un subgrupo cíclico, es decir, existe $m \in \mathbb{Z}$ tal que $H = \langle m \rangle$.

Demostración. Se deduce fácilmente a partir de la proposición y de la observación anterior. □

Ejemplo. 1. El conjunto $U_n = \left\{z \in \mathbb{C} \,:\, z^2 = 1\right\}$, de las raíces n-ésimas de la unidad, es un grupo cíclico con la multiplicación. Recordamos que $w_k = e^{i\frac{2\pi k}{n}}$, para $k = 0, \ldots, n-1$. Es sencillo ver que $(U_n, \cdot, 1) \leq (\mathbb{C}/\left\{0\right\}, 1)$. En efecto,

$$e^{i\frac{2\pi \cdot 0}{n}} = e^0 = 1.$$

Ahora, si $w_1, w_2 \in U_n$, tenemos que si $k_1 > k_2$:

$$w_1 w_2^{-1} = e^{i\frac{2\pi k_1}{n}} e^{i\frac{2\pi(-k_2)}{n}} = e^{i\frac{e\pi(k_1-k_2)}{n}} \in U_n.$$

Así, está claro que $(U_n, \cdot, 1) \leq (\mathbb{C}/\left\{0\right\} \;\cdot, 1)$. Para ver que es cíclico basta con ver que $U_n = \left\langle e^{i\frac{2\pi}{n}} \right\rangle$.

2. En $\mathbb{Z}$, tenemos que $\forall m \in \mathbb{Z}$, $m\mathbb{Z} \leq \mathbb{Z}$. Sabemos que $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. Podemos definir la operación:

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ ([a]_m, [b]_m) &\to [a+b]_m. \end{aligned}$$

Vamos a ver que está operación está bien definida. Si $x \in [a]_m$ e $y \in [b]_m$, tenemos que

$$m|x-a \quad \text{y} \quad m|y-b.$$

Así, existen $\lambda, \mu \in \mathbb{Z}$ tales que $x = a + \lambda m$ e $y = b + \mu m$. Por tanto, obtenemos que

$$x+y = a+\lambda m+b+\mu m = (a+b)+(\lambda+\mu)\, m \iff x+y \equiv a+b \mod m \iff [x+y]_m = [a+b]_m.$$

Queremos ver ahora que $(Z_m, +, [0]_m)$ es un grupo. Está claro que $\mathbb{Z}_m \neq \emptyset$ y que el elemento neutro es $[0]_m$. Ahora comprobamos que hay inversos. Si $[a]_m \in \mathbb{Z}_m$, tenemos que $[-a]_m \in \mathbb{Z}_m$ y, por definición, $[a]_m + [-a]_m = [0]_m$. También se puede ver que $\mathbb{Z}_m$ es cíclico, es decir, que $\mathbb{Z}_m = \langle [1]_m \rangle$.

Lema 1.2. Sea G un grupo cíclico, por lo que $G = \langle a \rangle$. Entonces si $a^k \neq e$, $\forall k \in \mathbb{N}$, tenemos que G tiene orden infinito. En caso contrario, si $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$ tenemos que $G = \langle a \rangle = \left\{e, a, \dots, a^{m-1}\right\}$. Además, $a^k = e$ si y solo si $m|k$.

Demostración. **(i)** Sea $a^k \neq e$, $\forall k \in \mathbb{N}$. Entonces, $a^k \neq e$, $\forall \mathbb{Z}/\left\{0\right\}$, por lo que el orden de G es infinito. En efecto, si existieran $i, j \in \mathbb{Z}$ distintos tales que $a^i = a^j$, tendríamos que $a^{i-j} = e$, lo que es una contradicción.

(ii) Por otro lado, sea $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$. Vamos a ver que $G = \langle a \rangle = \left\{e, a, \dots, a^{m-1}\right\}$. Es trivial que $\left\{e, a, \dots, a^{m-1}\right\} \subset G$. Recíprocamente, si $g \in G$, tenemos que existe $l \in \mathbb{Z}/\left\{0\right\}$ tal que $g = a^l$. Por el algoritmo de la división, tenemos que existen $q, r \in \mathbb{Z}$ tales que

$$l = mq + r,\ 0 \leq r < m.$$

Así, tenemos que

$$a^l = a^{mq+r} = \left(a^m\right)^q a^r = a^r.$$

Así, como $0 \leq r < m$, debe ser que $g \in \left\{e, a, \dots, a^{m-1}\right\}$, por lo que $G \subset \left\{e, a, \dots, m-1\right\}$. Consecuentemente, $G = \left\{e, a, \dots, a^{m-1}\right\}$.
Finalmente, como $l = qm + r$, es trivial que $a^l = e \iff r = 0$.

$\square$

Observación. En el lema podemos ver que $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$ es también el orden de G.

Proposición 1.7. Dos grupos G y H cícliclos del mismo orden son isomorfos.

Demostración. Sea $G = \langle a \rangle$ y $H = \langle b \rangle$. Consideremos la aplicación

$$\begin{aligned} f : G &\to H \\ a^k &\to b^k. \end{aligned}$$

Vamos a ver que se trata de un homomorfismo de grupos:

$$f\left(a^k\right) f\left(a^t\right) = b^k b^t = b^{k+t} = f\left(a^{k+t}\right) = f\left(a^k a^t\right).$$

Ahora vamos a ver que es biyectiva.

Inyectiva. Si $|G| > k \geq t$ y $f\left(a^k\right) = f\left(a^t\right)$, tenemos que $f\left(a^{k-t}\right) = b^{k-t} = e$. Como $|G| > k - t \geq 0$, debe ser que $k - t = 0$, por lo que $a^k = a^t$.

Sobreyectiva. Si $c \in H$ con $c = b^k$ para algún $k = 0, \dots, |H| - 1$, tenemos que $f\left(a^k\right) = b^k = c$.

Así, está claro que f es un isomorfismo. $\square$