

Grupos, anillos y cuerpos

1 Operaciones binarias

Definición 1 *Dados los conjuntos A , B y C , llamamos operación binaria interna sobre A a cualquier función $*$ cuyo dominio es el producto cartesiano $A \times A$ y codominio A , esto es:*

$$\begin{aligned} *: A \times A &\longrightarrow A \\ (a_1, a_2) &\longmapsto a_1 * a_2 \end{aligned}$$

Ejemplo 1 *La suma y el producto en los enteros modulares son operaciones internas.*

$$+: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \qquad \cdot: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

Definición 2 *Dados los conjuntos A , B y C , una operación binaria externa es una función cuyo dominio es el producto cartesiano $A \times B$ y codominio C , esto es:*

$$\begin{aligned} *: A \times B &\longrightarrow C \\ (a, b) &\longmapsto a * b \end{aligned}$$

Ejemplo 2 *La función $*: \mathbb{N} \times \mathcal{P}(\mathbb{R}) \longrightarrow \mathcal{P}(\mathbb{R})$, definida para cada $n \in \mathbb{N}$ y $p(x) \in \mathcal{P}(\mathbb{R})$ como $*(n, p(x)) = n p(x)$ es una operación externa, donde $\mathcal{P}(\mathbb{R})$ es el conjunto de polinomios con coeficientes reales.*

Ejemplo 3 *De forma similar se puede observar que la función*

$$\begin{aligned} *: \mathbb{Z} \times \mathcal{M}_{m \times n}(\mathbb{Z}) &\longrightarrow \mathcal{M}_{m \times n}(\mathbb{Z}) \\ (\lambda, M) &\longmapsto *(\lambda, M) = \lambda M \end{aligned}$$

es una operación externa.

⁰EAC, Dept. Mat. Aplicada

1.1 Propiedades

En este apartado vamos a centrarnos en el estudio de las propiedades de las operaciones binarias. En primer lugar, vamos a estudiar algunas de las propiedades más interesantes de las operaciones internas.

Propiedad asociativa: Si para cada $a, b, c \in A$ se verifica que

$$(a * b) * c = a * (b * c)$$

Propiedad conmutativa: Si para cada $a, b \in A$ se verifica que

$$a * b = b * a$$

Leyes de cancelación: Cancelación a la izquierda si para cada $a, b, c \in A$ se verifica que

$$\text{si } a * b = a * c \quad \text{entonces } b = c$$

Si tenemos una segunda operación \star

Propiedad distributiva: Si para cada $a, b, c \in A$ se verifica que

$$a \star (b * c) = (a \star b) * (a \star c)$$

Por otro lado, algunos elementos del conjunto A se pueden comportar de forma notable con respecto a una operación $*$.

Elemento neutro $e \in A$: Si para cada $a \in A$ se verifica que

$$a * e = e * a = a$$

Elemento absorbente $z \in A$: Si para cada $a \in A$ se verifica que

$$a * z = z * a = z$$

Elemento idempotente $a \in A$: Si se verifica que

$$a * a = a$$

Elemento simétrico $a \in A$: Si existe un elemento $a' \in A$ tal que

$$a * a' = a' * a = e$$

Ejemplo 4 *Comprobar qué propiedades cumplen las operaciones siguientes.*

- $*$: $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ definida como $p * q = p$, para todo $p, q \in \mathbb{Q}$.

- $\star: (\mathbb{Z}_n \times \mathbb{Z}_n) \times (\mathbb{Z}_n \times \mathbb{Z}_n) \rightarrow \mathbb{Z}_n$ definida como

$$(n, m) \star (s, t) = (n + s, m + t)$$

para todo $(n, m), (s, t) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Ejercicio 1 Dado un conjunto A , sobre el que definimos la operación:

$$\Delta: A \times A \longrightarrow A; \quad x \Delta y = y$$

Argumentar por qué es una operación interna y estudiar qué propiedades, de las anteriores, cumple. ¿Y si $A = \mathbb{Z}_7$?

1.2 Estructuras algebraicas

Cuando tenemos uno o más conjuntos con una o varias operaciones binarias, con unas determinadas propiedades y unos determinados elementos notables, estamos ante una estructura algebraica.

A veces, si el conjunto sobre el que actúa una operación es finito $A = \{a_1, a_2, \dots, a_n\}$ es posible representar dicha operación mediante una tabla de la forma

$*$	a_1	\dots	a_j	\dots	a_n
a_1			\vdots		
\vdots			\vdots		
a_i	\dots	\dots	$a_i * a_j$	\dots	\dots
\vdots			\vdots		
a_n			\vdots		

Las estructuras se presentan agrupando bajo un paréntesis el conjunto y las operaciones que actúan sobre él, como por ejemplo $(A, *)$, $(A, *, \star)$ y $(A, B, *, \star)$.

Ejemplo 5 Enteros modulares

El conjunto \mathbb{Z}_n se define mediante una relación de equivalencia en \mathbb{Z} llamada de congruencia módulo n :

Se dice que $a \equiv b \pmod{n}$ si y solo si $b - a$ es múltiplo entero de n

Una de las operaciones internas que se pueden definir sobre este conjunto, se representa por $+$, y viene dada por

$$[a] + [b] = [a + b]$$

Obteniendo que $(\mathbb{Z}_n, +)$ es una estructura algebraica. Dado que \mathbb{Z}_n es finito, se puede representar dicha operación mediante una tabla. Por ejemplo podemos observar las dadas para \mathbb{Z}_2 y \mathbb{Z}_5 :

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

Escribe las tablas para \mathbb{Z}_4 y \mathbb{Z}_5 , y analiza las diferencias.

Ejercicio 2 Estudiar las propiedades de $(\mathbb{Z}_n, +)$.

1.3 Morfismos

Definición 3 Dadas dos estructuras algebraicas similares (con las mismas propiedades) se llama homomorfismo entre las estructuras a una función entre los conjuntos que respeta la estructura. Por ejemplo, si $(A, *)$ y (B, \star) son dos estructuras algebraicas, un homomorfismo entre ambas es una función $f: A \rightarrow B$ que verifica

$$f(a * b) = f(a) \star f(b)$$

para cada par de elementos a, b de A .

Cuando los homomorfismos son inyectivos o sobreyectivos reciben nombres especiales, estos son los siguientes:

Monomorfismo: si es inyectivo.

Epimorfismo: si es sobreyectivo.

Isomorfismo: si es biyectivo.

Definición 4 Decimos que dos estructuras algebraicas son isomorfas si existe un isomorfismo entre ambas.

Ejemplo 6 Dados los conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3\}$ con operaciones definidas mediante las tablas

$*$	a	b	c
a	a	b	c
b	b	b	b
c	c	b	b

\star	1	2	3
1	1	1	1
2	1	2	3
3	1	3	1

se observa que son estructuras isomorfas, puesto que la función $f: A \rightarrow B$ definida como $f(a) = 2$, $f(b) = 1$ y $f(c) = 3$ es un isomorfismo.

2 Teoría de Grupos

2.1 Semigrupos

Definición 5 Una estructura $(S, *)$ es un semigrupo si S es no vacío y $*$ es una operación binaria interna que verifica la propiedad asociativa.

Si además verifica la propiedad conmutativa decimos que es un semigrupo conmutativo.

Ejemplo 7 Tenemos que

- $(\mathbb{N}, +)$ es un semigrupo conmutativo.
- (\mathbb{Z}, \cdot) es un semigrupo conmutativo.
- $(\mathcal{P}(A), \cup)$ y $(\mathcal{P}(A), \cap)$ son semigrupos conmutativos.
- $(\mathbb{N}, *)$, siendo $a * b = a^b$, no es un semigrupo.
- $(\mathbb{Z}, -)$ no es un semigrupo.
- (A^A, \circ) , donde $A^A = \{f \mid f: A \rightarrow A\}$ y \circ es la operación composición, es un semigrupo no conmutativo.
- (\mathcal{M}_n, \cdot) es un semigrupo no conmutativo.

2.2 Subsemigrupos

Definición 6 Dado un semigrupo $(S, *)$ y un subconjunto $A \subseteq S$ decimos que es un subsemigrupo si restringiendo la operación $*$ a los elementos de A se sigue teniendo estructura de semigrupo, es decir, $(A, *)$ es también semigrupo.

La única condición para que $(A, *)$ sea subsemigrupo de $(S, *)$ es que la restricción de la operación $*$ al subconjunto A sea cerrada en A . Cuando A cumple esta condición se suele decir que A es cerrado para la operación $*$.

Ejemplo 8 Algunos ejemplos son:

- Dado el semigrupo $(\mathbb{Z}, +)$, el subconjunto $(2\mathbb{Z}, +)$ es un subsemigrupo, en cambio el conjunto de los impares no lo es.

- En el semigrupo (A^A, \circ) el subconjunto de las funciones biyectivas $S(A)$ es un subsemigrupo.

2.3 Monoides

Definición 7 Dado un semigrupo $(S, *)$ decimos que tiene elemento neutro si existe un elemento $e \in S$ que verifica

$$e * a = a * e = a \quad \text{para todo } a \in S$$

Teorema 1 En todo semigrupo, el elemento neutro, si existe, es único.

Definición 8 A un semigrupo con elemento neutro se le llama monoide. Si además el semigrupo es conmutativo se le llama monoide conmutativo.

Ejemplo 9 Algunos ejemplos son:

- $(\mathbb{Z}^+, +)$ no es monoide porque $0 \notin \mathbb{Z}^+$.
- $(\mathcal{M}_{m \times n}, +)$ es un monoide conmutativo.
- $(\mathcal{M}_{n \times n}, \cdot)$ es un monoide no conmutativo.

Ejercicio 3 Probar que las estructuras $(\mathcal{M}_n(\{0,1\}), \vee)$, $(\mathcal{M}_n(\{0,1\}), \wedge)$ y $(\mathcal{M}_n(\{0,1\}), \odot)$, son monoides, donde \vee , \wedge y \odot son las operaciones booleanas usuales.

¿Cuáles de los ejemplos de semigrupos anteriores son monoides?

2.3.1 El semigrupo libre de las cadenas

Definición 9 Llamamos alfabeto a un conjunto Σ al que se le exige que ningún elemento pueda ser formado por yuxtaposición de elementos del propio Σ . A los elementos de Σ se les llama también cadenas de longitud uno.

Yuxtaponiendo dos elementos de Σ se obtiene un nuevo elemento de un conjunto de cadenas de longitud 2. Este proceso se puede extender recursivamente para formar cadenas de longitud n . Si denominamos $\Sigma^1 = \Sigma$, cada Σ^n , con $n \geq 2$, se construye como

$$\Sigma^n = \{xy \mid x \in \Sigma, y \in \Sigma^{n-1}\}$$

El conjunto de todas las cadenas, de longitud mayor o igual que uno, se representa por

$$\Sigma^+ = \bigcup_{n=1}^{\infty} \Sigma^n$$

Consideremos de forma axiomática la existencia de una cadena ϵ que no pertenece a ningún Σ^n y que llamamos cadena de longitud 0, o bien, cadena nula. Esta cadena tiene la propiedad de dejar invariante a cualquier cadena por yuxtaposición, es decir

$$x\epsilon = \epsilon x = x \quad \text{para todo } x \in \Sigma^n$$

Por último, llamamos Σ^* al conjunto formado por las cadenas de cualquier longitud, incluida la cadena nula.

$$\Sigma^* = \Sigma^+ \cup \{\epsilon\}$$

Este conjunto, dotado con la operación binaria de *concatenación*, que consiste en yuxtaponer dos cadenas de Σ^* , verifica la propiedad asociativa, y además tiene elemento neutro ϵ . Se le conoce con el nombre de *Semi-grupo libre de las cadenas* (aunque en realidad es un monoide) y juega un importante papel en la teoría de lenguajes formales.

2.4 Submonoides

Dado un monoide $(S, *)$, un subconjunto $A \subseteq S$ es *submonoide*, si además de ser subsemigrupo, contiene al elemento neutro. Por lo tanto:

Teorema 2 Sea $(S, *)$ un monoide y $A \subseteq S$. Las condiciones necesarias y suficientes para que el subconjunto A sea submonoide son:

1. Que sea cerrado para la operación: si $a, b \in A$ entonces $a * b \in A$
2. El elemento neutro pertenece al subconjunto: $e \in A$

Ejemplo 10 Llamamos $n\mathbb{Z}$ al conjunto de los productos de un entero n por todos los elementos de \mathbb{Z} . Si $n > 1$ obtenemos que $(n\mathbb{Z}, +)$ son submonoides de $(\mathbb{Z}, +)$, en cambio $(n\mathbb{Z}, \cdot)$ son subsemigrupos (y no submonoides) de (\mathbb{Z}, \cdot) (que sí es monoide).

2.5 Grupos

Definición 10 Dado un conjunto G y una operación interna $*$: $G \times G \rightarrow G$ que verifica las propiedades:

1. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$;
2. Existencia de elemento neutro: existe un elemento $e \in G$ que cumple que $a * e = e * a = a$ para cualquier $a \in G$, que llamamos elemento neutro;
3. Existencia de elemento simétrico: para cada $a \in G$, existe un elemento $a' \in G$ tal que $a * a' = a' * a = e$, que llamamos elemento simétrico de a ;

se dice que el par $(G, *)$ forma un grupo.

Además, si la operación interna cumple la propiedad conmutativa ($a * b = b * a$ para cada $a, b \in G$), se dice que el grupo es conmutativo, aunque se emplea también el término de grupo abeliano en honor al matemático noruego Niels Henrik Abel (1802–1829).

Ejemplo 11 Podemos comprobar que:

- Los pares $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$ son grupos abelianos (aditivos), mientras que el par $(\mathbb{N}, +)$ no lo es. Esto último debido a que no se cumple la propiedad de elemento simétrico.
- Ninguno de los pares (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) y (\mathbb{R}, \cdot) es grupo. Todos fallan, al menos, en que el simétrico de 0 no es un elemento del conjunto considerado. Sin embargo, los conjuntos (\mathbb{Q}^*, \cdot) y (\mathbb{R}^*, \cdot) , donde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ y $\mathbb{R}^* = \mathbb{R} - \{0\}$, son grupos abelianos (multiplicativos).
- Si p es primo, (\mathbb{Z}_p^*, \cdot) , es un grupo abeliano.
- Si consideramos un conjunto A , el formado por todas las aplicaciones biyectivas de A en A , denotado por $S(A)$, junto con la operación composición de funciones forman un grupo.

Ejercicio 4 Estudiar las propiedades que cumplen las estructuras $(\mathcal{P}(A), \cup)$ y $(\mathcal{P}(A), \cap)$.

2.5.1 Notación

Para la operación de un grupo, la notación habitual es la *multiplicativa*, pero en los casos de grupos conmutativos se suele usar la *notación aditiva*.

Dado un grupo $(G, *)$, si la notación es multiplicativa, éste se representa por (G, \cdot) , y se adoptan los siguientes convenios, donde $a \in G$.

- El elemento neutro se representa por 1.
- El elemento simétrico de a se representa por a^{-1} y se llama *inverso de a*

- – Si $n \in \mathbb{Z}^+$, se define $a^n = \overbrace{a \cdot a \cdots a}^{n \text{ veces}}$;
 – si $n = 0$, se define $a^0 = 1$
 – si $n \in \mathbb{Z}^+$, se define $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

- Para cualesquiera $n, m \in \mathbb{Z}$ se tiene que

$$\begin{aligned} a^{m+n} &= a^m \cdot a^n \\ a^{m-n} &= a^m \cdot a^{-n} \\ a^{mn} &= (a^m)^n \end{aligned}$$

De forma análoga, dado un grupo $(G, *)$, si la notación es aditiva, éste se representa por $(G, +)$, y se adoptan los siguientes convenios, donde $a \in G$.

- El elemento neutro se representa por 0.
- El elemento simétrico de a se representa por $-a$ y se llama *opuesto de a*

- – Si $n \in \mathbb{Z}^+$, se define $n.a = \overbrace{a + a + \cdots + a}^{n \text{ veces}}$;
 – si $n = 0$, se define $0a = 0$
 – si $n \in \mathbb{Z}^+$, se define $(-n)a = n(-a) = -(na)$

- Para cualesquiera $n, m \in \mathbb{Z}$ se tiene que

$$\begin{aligned} (m+n)a &= ma + na \\ (m-n)a &= ma + (-na) \text{ (que se podrá denotar por } ma - na) \\ (mn)a &= m(na) \end{aligned}$$

Debemos observar que como todo grupo es un monoide, el elemento neutro del grupo debe ser único. Además, se tienen los siguientes resultados:

Teorema 3 *En un grupo $(G, *)$, el elemento simétrico de cualquier $a \in G$ es único.*

Teorema 4 *En un grupo $(G, *)$, se cumplen las leyes de cancelación. Esto es, para cualesquiera $a, b, c \in G$ se tiene que:*

- Si $a * b = a * c$, entonces $b = c$.
- Si $b * a = c * a$, entonces $b = c$.

Teorema 5 *Dado un grupo $(G, *)$ y elementos $a, b \in G$, se tiene que:*

1. *El elemento simétrico del neutro es él mismo: $e' = e$.*
2. *El simétrico del simétrico de un elemento a es el propio a : $(a')' = a$.*
3. *$(a * b)' = b' * a'$*
4. *Las ecuaciones del tipo: $a * x = b$ y $x * a = b$, tienen solución única.*

De forma usual, se representará la operación de un grupo abeliano cualquiera por $+$ (*notación aditiva*). Para el resto de grupos, se denotará la operación interna por \cdot (*notación multiplicativa*).¹

Ejercicio 5 *Sobre el conjunto \mathbb{Z}_n , se define la operación interna dada por $[a] \cdot [b] = [ab]$. ¿Es (\mathbb{Z}_n, \cdot) un grupo? ¿Qué ocurre con (\mathbb{Z}_n^*, \cdot) ?*

2.6 Grupos Simétricos

Ya hemos visto que dado A , el conjunto $S(A)$ de las aplicaciones biyectivas es un grupo. Si A es finito entonces a las aplicaciones biyectivas, de A en A , se les llama permutaciones y al grupo de las permutaciones $S(A)$ se le suele representar como S_n (donde n es el cardinal de A) y se le conoce como el *grupo simétrico* en n letras o n símbolos.

Se puede considerar que los elementos de A son de la forma $1, 2, \dots$ y n , en lugar de a_1, a_2, \dots y a_n ; por tanto, tenemos que $A = \{1, 2, \dots, n\}$.

Si $\sigma \in S_n$ y $\sigma(i) = s_i$, se acostumbra a usar la siguiente notación para representarla:

¹Para los casos en los que no se cree confusión, este símbolo se podrá omitir.

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}$$

Llamamos *producto de permutaciones* a la composición como funciones, es decir $\sigma\tau = \tau \circ \sigma$.

Ejemplo 12 En el grupo simétrico S_4 si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad y \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Bajo esta notación el elemento neutro será la permutación identidad

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Teorema 6 El grupo simétrico S_n tiene $n!$ elementos.

Ejemplo 13 El grupo simétrico S_3 tiene $3! = 6$ elementos que son:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \end{pmatrix} \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

donde e actúa como elemento neutro y la tabla para este grupo queda de la forma:

	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_2	μ_3	μ_1
ρ_2	ρ_2	e	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	e	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	e	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	e

2.7 Subgrupos

Definición 11 Decimos que un subconjunto H de un grupo (G, \cdot) es un subgrupo si es grupo con la restricción de la operación G en H , y se representa por $H \leq G$.

Por tanto, que H es subgrupo si verifica:

1. Contiene al elemento neutro: $e \in H$.
2. Es cerrado para la operación: si $a, b \in H$, entonces $a \cdot b \in H$.
3. Es cerrado para el inverso: si $a \in H$, entonces $a^{-1} \in H$.²

Ejemplo 14 Dado cualquier grupo (G, \cdot) , los subconjuntos $\{e\}$ y el propio G son subgrupos de (G, \cdot) , y reciben el nombre de subgrupos triviales. Los subgrupos que no son triviales se denominan subgrupos propios.

Ejemplo 15 El par (\mathbb{R}^+, \cdot) forma un subgrupo de (\mathbb{R}^*, \cdot) , mientras que (\mathbb{R}^-, \cdot) no lo es.

Ejercicio 6 Buscar un subgrupo de $(\mathbb{Z}_4, +)$.

El siguiente teorema, proporciona una caracterización del concepto de subgrupo.

Teorema 7 Dado un grupo (G, \cdot) , una condición necesaria y suficiente para que un subconjunto $H \subseteq G, H \neq \emptyset$ sea subgrupo es que

$$\text{para todo } a, b \in H, \text{ se tiene que } ab^{-1} \in H$$

Ejemplo 16 Los subgrupos del grupo $(\mathbb{Z}, +)$ son los subconjuntos de la forma $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ siendo $n \in \mathbb{N}$.

Ejercicio 7 Probar que para el grupo multiplicativo (Q^*, \cdot) , el conjunto $\{1, 2, 1/2, 2^2, 1/2^2, \dots, 2^n, 1/2^n, \dots\}$ es un subgrupo.

Ejercicio 8 Comprobar que (\mathbb{Z}^*, \cdot) no es un subgrupo de (\mathbb{Q}^*, \cdot) , esto es, $(\mathbb{Z}^*, \cdot) \not\leq (\mathbb{Q}^*, \cdot)$.

En el caso de considerar un subconjunto finito, el teorema de caracterización se simplifica del siguiente modo:

Teorema 8 Si $H \neq \emptyset$ es un subconjunto finito de un grupo (G, \cdot) , entonces H es subgrupo si y solo si es cerrado para la operación del grupo.

Si el subgrupo H es finito llamamos *orden del subgrupo* al número de elemento que posee.

²Obsérvese que las propiedades 2) y 3) implican la propiedad 1)

2.8 Morfismos de grupos

Definición 12 Dados los grupos $(G, *)$ y (G', \star) , decimos que una función $f: (G, *) \rightarrow (G', \star)$ es un homomorfismo de grupos si

$$f(a * b) = f(a) \star f(b) \quad \text{para todo } a, b \in G$$

se mantiene la terminología de monomorfismo, epimorfismo e isomorfismo.

Teorema 9 Si $f: (G, *) \rightarrow (G', \star)$ es un homomorfismo de grupos, entonces se verifica:

1. Si e y e' son los elementos neutros de $(G, *)$ y (G', \star) respectivamente, entonces $f(e) = e'$.
2. Para cada $a \in G$ se cumple $f(a^{-1}) = (f(a))^{-1}$.
3. Para cada entero n y cada $a \in G$ se cumple $f(a^n) = (f(a))^n$.
4. $(f(G), \star)$ es un subgrupo, llamado subgrupo imagen y se denota por $\text{Im}(f)$.

Ejemplo 17 Probemos que la función $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$ definida por $f(x) = e^x$ es un isomorfismo.

- Si $f(a) = f(b)$, de modo que $e^a = e^b$, entonces $a = b$. Por lo tanto, f es inyectiva.
- Si $c \in \mathbb{R}^+$, entonces $\ln(c) \in \mathbb{R}$ y $f(\ln(c)) = e^{\ln(c)} = c$, por lo tanto f es sobreyectiva.
- $f(a + b) = e^{a+b} = e^a e^b = f(a)f(b)$, por lo tanto f es un isomorfismo.

Ejercicio 9 Sea $f: (\mathbb{N}, +) \rightarrow (\mathbb{N}, \cdot)$ definida por $f(x) = 2^x$. Demostrar que f es un homomorfismo.

Ejemplo 18 Si consideramos un grupo (G, \cdot) y un elemento $a \in G$, la función $f: (G, \cdot) \rightarrow (G, \cdot)$, definida como $f(x) = a^{-1}xa$, para cada $x \in G$ y donde a^{-1} es el inverso de a , es un isomorfismo de grupos.

Ejercicio 10 Sea $f: (\mathbb{R}^+ - \{0\}, \cdot) \rightarrow (\mathbb{R}, +)$ definida por $f(x) = \log(x)$. Demostrar que f es un isomorfismo.

3 Anillos y Cuerpos

3.1 Anillos

Definición 13 Dado un conjunto A con dos operaciones internas que denotamos por $+$ y \cdot , decimos que $(A, +, \cdot)$ es un anillo si verifica:

1. $(A, +)$ es un grupo abeliano.
2. (A, \cdot) es un semigrupo.
3. Para cualesquiera $a, b, c \in A$ se cumplen:
 - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
 - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Cuando (A, \cdot) es un monoide se dice que A es un anillo unitario o anillo con unidad. Denotaremos al elemento neutro de (A, \cdot) por 1.

Cuando (A, \cdot) es un semigrupo conmutativo, se dice que R es un anillo conmutativo.

Ejemplo 19 Los conjuntos numéricos con las operaciones habituales $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son anillos conmutativos unitarios. $(\mathbb{N}, +, \cdot)$ no es un anillo por no ser $(\mathbb{N}, +)$ un grupo.

Ejemplo 20 Para cada entero positivo n :

- el conjunto \mathbb{Z}_n junto con la suma y el producto usuales es un anillo conmutativo y unitario.
- el conjunto $\mathcal{M}_n(A)$ de matrices cuadradas con coeficientes en un anillo $(A, +, \cdot)$, junto con las operaciones de suma y producto de matrices, forman un anillo.

Teorema 10 Si A es un anillo, con elemento neutro aditivo 0, entonces para cualesquiera elementos $a, b \in A$ se tiene:

1. $0 \cdot a = a \cdot 0 = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Muchas de las propiedades de los anillos son reformulaciones de las propiedades correspondientes a los grupos, por ejemplo:

- Si $m, n \in \mathbb{Z}, a \in \mathbb{R}$ $\begin{cases} ma + na = (m + n)a \\ m(na) = (mn)a \end{cases}$
- Si $m, n \in \mathbb{N}, a \in \mathbb{R}$ $\begin{cases} a^m a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{cases}$

Al ser una estructura más rica que la de grupo, se tienen expresiones completamente nuevas basadas en la propiedad distributiva.

3.2 Subanillos

Definición 14 Dado un anillo $(A, +, \cdot)$, $S \subseteq A$ es un subanillo de $(A, +, \cdot)$ si forma un anillo junto con las operaciones definidas en A , es decir:

$$\text{Dados } x, y \in S \Rightarrow x - y \in S \text{ y } x \cdot y \in S$$

3.3 Morfismos de anillos

Definición 15 Dados los anillos $(A, +, \cdot)$ y (A', \oplus, \odot) , la función $f: (A, +, \cdot) \longrightarrow (A', \oplus, \odot)$ es un homomorfismo de anillos si:

1. $f(a + b) = f(a) \oplus f(b)$
2. $f(a \cdot b) = f(a) \odot f(b)$

Teorema 11 Para cualquier morfismo de anillos $f: (A, +, \cdot) \longrightarrow (A', \oplus, \odot)$, se tiene:

1. $f(0) = 0'$, donde 0 es el elemento neutro de $(A, +)$ y $0'$ el de (A', \oplus) .
2. $f(na) = nf(a)$, $n \in \mathbb{Z}$.
3. $f(A)$ es un subanillo de (A', \oplus, \odot) .
4. Si $(A, +, \cdot)$ es un anillo unitario y $f(1) \neq 0$, entonces $f(1)$ es un elemento neutro para el producto en el anillo $(f(A), \oplus, \odot)$.

4 Dominios de integridad

Definición 16 Si a y b son elementos distintos de cero de un anillo $(A, +, \cdot)$ tal que $a \cdot b = 0$, entonces se dice que a y b son divisores de cero.

Ejemplo 21

- Los elementos $[2]$ y $[3]$ de \mathbb{Z}_6 son dos divisores de cero.
- Los divisores de cero del anillo $(\mathbb{Z}_n, +, \cdot)$ son aquellas clases cuyos elementos no son primos relativos con n .

Teorema 12 Si $(A, +, \cdot)$ es un anillo, entonces son válidas las leyes de cancelación para (A, \cdot) si y solo si no tiene divisores de cero.

Definición 17 Llamamos dominio de integridad a un anillo conmutativo unitario que no contiene divisores de cero.

Ejemplo 22

- Los anillos numéricos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son dominios de integridad.
- El anillo $(\mathcal{M}_n, +, \cdot)$ de matrices cuadradas de orden n , con $n \geq 2$ no son dominios de integridad.

5 Cuerpos

Definición 18 Llamamos cuerpo a un anillo conmutativo unitario $(K, +, \cdot)$ donde cada elemento distinto de cero es inversible, es decir: si $a \in K, a \neq 0$, existe a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Ejemplo 23 \mathbb{Z} , con las operaciones usuales de suma y producto, no es un cuerpo, puesto que los únicos elementos inversibles son 1 y -1 . En cambio sí son cuerpos las estructuras $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$

Teorema 13 Todo cuerpo es un dominio de integridad.

El inverso de este teorema no es cierto, en general, tenemos dominios de integridad que no son cuerpos y $(\mathbb{Z}, +, \cdot)$ es un ejemplo de ello. En cambio si el conjunto considerado es finito.

Teorema 14 Todo dominio de integridad finito es un cuerpo.

Este teorema nos permite identificar los cuerpos finitos.

Corolario 1 *Si p es un entero positivo primo, $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.*

Se puede probar que todo cuerpo finito contiene un subcuerpo que es isomorfo a un cierto $(\mathbb{Z}_p, +, \cdot)$, es más, se prueba también que todos los cuerpos infinitos contienen un subcuerpo isomorfo a $(\mathbb{Q}, +, \cdot)$.