Capítulo 4

Operaciones internas y estructuras algebraicas

El lector seguramente ya conoce y maneja muchas operaciones internas: suma y producto de números (enteros, racionales o reales), suma y producto de matrices cuadradas, suma de vectores del plano o del espacio, composición de aplicaciones de un conjunto en si mismo, suma y producto de funciones reales, unión e intersección de subconjuntos de un conjunto dado, etc. Cuando el conjunto y las operaciones internas que se consideren cumplen determinadas propiedades nos encontramos frente a una estructura algebraica.

Estas estructuras son importantes por su sencillez y por los resultados y propiedades que de ellas se deducen, resultados que serán válidos cada vez que se maneje el mismo tipo de estructura. Identidades en los números reales del tipo $a^2 - b^2 = (a+b)(a-b)$, $(a+b)^2 = a^2 + b^2 + 2ab$, el binomio de Newton o deducciones del tipo si $ax = ay$ y $a \neq 0$ entonces $x = y$, no son válidas, por ejemplo, para el producto de matrices cuadradas. Basta observar el siguiente contraejemplo:

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}\begin{pmatrix} 5 & 3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$$

y sin embargo $\begin{pmatrix} 5 & 3 \\ -1 & 1 \end{pmatrix} \neq \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$. Hay por tanto propiedades que satisfacen las operaciones en $\mathbb{R}$ que no satisfacen las operaciones con matrices cuadradas. Identificaremos qué estructura permite operar como en $\mathbb{R}$ o en qué estructura hay que operar con más cautela. Es decir, despojamos de todo significado a los elementos del conjunto y a la operación para quedarnos con las reglas del juego y sus consecuencias.

Definiremos las estructuras básicas para operaciones internas: grupos, anillos y cuerpos. De estas estructuras, el lector ya conoce un buen número de ejemplos. A lo largo de estudios posteriores, tanto en Físicas como en Matemáticas, se encontrará muy a menudo con este tipo de estructuras. Por ello, el estudio de este capítulo supone una economía importante de medios intelectuales.

4.1. Operaciones internas

Sea E un conjunto. Una **operación interna**, o **ley de composición interna**, en E es una aplicación de $E \times E$ en E. Es decir, es una ley que asocia a todo par (a, b) de elementos de E un elemento único de E, que notaremos, $a \star b$.

Ejemplo 4.1 Son operaciones internas conocidas:

$\cap$ Intersección en el conjunto $\mathcal{P}(\Omega)$ de las partes de un conjunto Ω.

$\cup$ Unión en el conjunto $\mathcal{P}(\Omega)$ de las partes de un conjunto Ω.

$\circ$ Composición en el conjunto $\mathcal{F}(\Omega)$ de las aplicaciones de un conjunto Ω en sí mismo.

$+$ Suma en los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$.

$-$ Resta en los conjuntos $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$.

$\cdot$ (también denotado $\times$, o sin signo) Producto en los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$.

$/$ División en los conjuntos $\mathbb{Q}^*$ o $\mathbb{R}^*$.

$+$, $\times$ Suma y producto en el conjunto de matrices cuadradas de orden n.

$\wedge$, $\vee$ Conjunción y disyunción en el conjunto de proposiciones lógicas.

$\wedge$, $\vee$ Máximo común divisor y mínimo común múltiplo en $\mathbb{N}^*$.

$\wedge$ Producto vectorial en el espacio euclideo tridimensional.

La resta en $\mathbb{N}$ o el producto escalar en el espacio euclideo tridimensional no son operaciones internas.

Propiedades

Sea E un conjunto y $\star$ una operación interna definida en E.

- La operación $\star$ es **asociativa** si para todo $a, b, c \in E$

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

Una de las ventajas de la propiedad asociativa es que se pueden eliminar los paréntesis, siendo válida la notación $a \star b \star c$.
Otra ventaja es que permite definir por recurrencia como se operan $n+1$ elementos, $a_1 \star a_2 \star \cdots \star a_n \star a_{n+1} = (a_1 \star a_2 \star \cdots \star a_n) \star a_{n+1}$.

Ejemplo 4.2 De las operaciones del ejemplo 4.1 hemos visto en capítulos anteriores que son asociativas las leyes $\wedge$ y $\vee$ en el conjunto de proposiciones lógicas, $\cap$ y $\cup$ en $\mathcal{P}(\Omega)$ y la composición de aplicaciones en $\mathcal{F}(\Omega)$. Veremos en los capítulos 5 y 6 que las operaciones $+$ y $\cdot$ son asociativas en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$. También son asociativas las operaciones $\wedge$ y $\vee$, máximo común divisor y mínimo común múltiplo en $\mathbb{N}^*$, o $+$ y $\times$, suma y producto en el conjunto de matrices cuadradas de orden n. No es asociativa la resta o la división. Observe que $(9-5)-1 \neq 9-(5-1)$ o $(16/4)/2 \neq 16/(4/2)$.

- La operación $\star$ es **conmutativa** si para todo $a, b \in E$

$$a \star b = b \star a$$

Una ventaja de la propiedad conmutativa es que el orden en que se colocan los elementos a la hora de operar es indiferente. Si la operación $\star$ es asociativa y conmutativa entonces $a_1 \star a_2 \star \cdots \star a_n$ permanece invariable cuando se permutan o se reagrupan de manera arbitraria los elementos. Tiene sentido hablar por tanto de

$$\bigstar_{i=1}^{n} a_i$$

por $a_1 \star a_2 \star \cdots \star a_n$ siendo el orden de los mismos indiferente.
En particular, cuando se utiliza la notación aditiva o la notación multiplicativa para operaciones que sean asociativas y conmutativas, se usan los símbolos siguientes:

$\sum_{i=1}^{n} a_i$, o $\sum_{i=1}^{n} a_i$, para indicar la suma de los elementos $a_1, a_2, \ldots, a_n$. En el caso en que todos los a_i sean iguales a a, la suma se indica por **na**.

$\prod_{i=1}^{n} a_i$, o $\prod_{i=1}^{n} a_i$, para el producto de los elementos $a_1, a_2, \ldots, a_n$. En el caso en que todos los a_i sean iguales a a, el producto se indica por $\mathbf{a^n}$.

También se utilizan para la intersección y unión de conjuntos las notaciones siguientes:

$\bigcap_{i=1}^{n} A_i$, o $\bigcap_{i=1}^{n} A_i$, para indicar la intersección de los conjuntos $A_1, A_2, \ldots, A_n$.

$\bigcup_{i=1}^{n} A_i$, o $\bigcup_{i=1}^{n} A_i$, para indicar la unión de los conjuntos $A_1, A_2, \ldots, A_n$.

Ejemplo 4.3 De las operaciones del ejemplo 4.1, no son conmutativas la composición de aplicaciones o el producto de matrices. Esto conlleva que cuando

se manejen igualdades, por ejemplo de matrices, hay que proceder con cautela a la hora de multiplicar los dos miembros de la igualdad, multiplicando ambos miembros a la izquierda, o ambos a la derecha. Es decir, de $A = B$ se deduce que $AC = BC$ o $CA = CB$ pero no se deduce que que $AC = CB$. Tampoco son conmutativas la resta o la división.

- Se denomina **elemento neutro** de la operación interna $\star$ en E, a un elemento $e \in E$ que cumple para todo $a \in E$

$$a \star e = e \star a = a$$

Ejemplo 4.4 Los elementos neutros de $+$ y $\cdot$ en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ son respectivamente 0 y 1. Los de $\cap$ y $\cup$ en $\mathcal{P}(\Omega)$ son respectivamente Ω y $\emptyset$. El elemento neutro de la composición en $\mathcal{F}(\Omega)$ es la aplicación identidad I_Ω. El elemento neutro en el producto de matrices cuadradas de orden 2 es la matriz identidad de orden 2, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. No existe elemento neutro en la resta o división en $\mathbb{R}^*$ o $\wedge$, máximo común divisor en $\mathbb{N}^*$.

Proposición 4.5 Sea $\star$ una operación interna en E. Si existe elemento neutro de $\star$ en E, éste es único.

Demostración: Basta observar que si e y e' son ambos elementos neutros entonces

$$\begin{aligned} e \star e' &= e \text{ pues } e' \text{ es elemento neutro y} \\ e \star e' &= e' \text{ pues } e \text{ es elemento neutro.} \end{aligned}$$

En consecuencia, $e = e'$.

□

Supongamos que en E tenemos definido una operación interna $\star$ con elemento neutro $e \in E$.

- Se denomina **elemento simétrico** del elemento $a \in E$ a un elemento $a' \in E$ tal que

$$a \star a' = a' \star a = e$$

Observación: De la propia definición del elemento simétrico se deduce que si a' es elemento simétrico de a, entonces a es elemento simétrico de a'.

Ejemplo 4.6

En $\mathbb{N}$, ningún elemento tiene simétrico respecto de la suma (salvo $a = 0$) o el producto (salvo $a = 1$).

En $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ el simétrico de a para la suma es $-a$.

En $\mathbb{Z}$, no existe el simétrico de a para el producto salvo si $a = -1$ o $a = 1$.

En $\mathbb{Q}^*$ y $\mathbb{R}^*$ el simétrico de a para el producto es $\frac{1}{a}$.

Según vimos en el capítulo anterior, en el conjunto $\mathcal{F}(\Omega)$ de las aplicaciones de un conjunto dado en sí mismo, sólo tienen simétrico respecto de la composición las aplicaciones biyectivas. El simétrico de la biyección f es la biyección inversa f^{-1}.

En el conjunto de matrices cuadradas de orden n sólo tienen simétrico respecto del producto, las matrices cuyo determinante es distinto de 0.

Proposición 4.7 Sea $\star$ una operación interna asociativa en E con elemento neutro $e \in E$. Si $a \in E$ tiene elemento simétrico, éste es único.

Demostración: Supongamos que a' y a'' son ambos elementos simétricos de a. Utilizamos la propiedad asociativa para calcular de dos maneras distintas $a' \star a \star a''$

$$\begin{aligned} a' \star a \star a'' &= (a' \star a) \star a'' = e \star a'' = a'' \text{ y} \\ a' \star a \star a'' &= a' \star (a \star a'') = a' \star e = a' . \end{aligned}$$

En consecuencia, $a' = a''$. □

4.2. Grupos

Definición 4.8 Sean G un conjunto no vacío y $\star$ una operación interna en G. Se dice que el par $(G, \star)$ tiene estructura de grupo, o que $(G, \star)$ es un **grupo** , si se satisfacen las siguientes propiedades:

1. La operación $\star$ es asociativa.
2. Existe elemento neutro de $\star$ en G.
3. Para todo elemento $a \in G$, existe en G el elemento simétrico de a respecto de $\star$.

Si además la operación $\star$ es conmutativa se dice que el grupo es **conmutativo o abeliano**.

También se dice que G es un grupo respecto de $\star$, o incluso, si el contexto es suficientemente claro respecto de la operación considerada, que G es un grupo, para indicar que $(G, \star)$ es un grupo.
Es conveniente señalar, según la definición anterior, una diferencia importante entre el elemento neutro y el elemento simétrico: mientras que el elemento neutro debe satisfacer la propiedad de dejar invariantes a todos los elementos del grupo (es decir, es el mismo para todos), cada elemento de G tiene su propio elemento simétrico. Escrito en términos de cuantificadores sería:

Elemento neutro: $\exists e \in G$ tal que $\forall a \in G, a \star e = e \star a = a$

Elemento simétrico: $\forall a \in G\ \exists a' \in G$ tal que $a \star a' = a' \star a = e$

Notación aditiva: Cuando la operación de un grupo se representa con el símbolo $+$, el grupo se llama aditivo.
El elemento neutro se llama elemento nulo, o cero, y se denota por 0.
El elemento simétrico de a se denota por $-a$ y se denomina elemento **opuesto**.
La notación $a - b$ se usa para indicar al elemento $a + (-b)$.
Si $n \in \mathbb{N}^*$, na indica la suma de n veces a. La propiedad asociativa de la operación $+$ hace que $a + a + \cdots + a$ permanezca invariable cuando se reagrupan de manera arbitraria los factores y se escribe:

$$na = \overbrace{a + a + \cdots + a}^{n\text{veces}}$$

Notación multiplicativa: Cuando la operación se representa con el símbolo $\cdot$, el grupo se dice multiplicativo.
El elemento neutro se denota por 1 y se llama unidad.
El elemento simétrico de a, que se denota por a^{-1}, se llama elemento **inverso** de a.
Análogamente al caso aditivo, si $n \in \mathbb{N}^*$, a^n indica el producto de n veces a y $a \cdot a \cdot \cdots \cdot a$ permanece invariable cuando se reagrupan de manera arbitraria los factores y se escribe:

$$a^n = \overbrace{a \cdot a \cdot \cdots \cdot a}^{n\text{veces}}$$

Las notaciones $\frac{1}{a}$ o $1/a$ por a^{-1} se utilizan exclusivamente para los números. De hecho, la notación $\frac{b}{a}$ sería confusa si la operación no es conmutativa, ya que a priori $\frac{1}{a}b$ y $b\frac{1}{a}$ pueden ser distintos. Así por ejemplo, si A es una matriz cuadrada inversible de orden 2, su inversa se denota por A^{-1} y nunca se utiliza la notación $\frac{1}{A}$.

Ejemplo 4.9 Ejemplos de grupos conocidos.

1. Veremos en capítulos posteriores que los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son grupos conmutativos respecto de la suma.

2. Los conjuntos $\mathbb{Q}^*, \mathbb{R}^*$ y $\mathbb{C}^*$ son grupos conmutativos respecto del producto.
3. El conjunto de matrices de orden $n \times m$ respecto de la suma de matrices es un grupo conmutativo.
4. El conjunto de matrices cuadradas inversibles de orden n es un grupo no conmutativo respecto del producto.
5. El conjunto $\mathcal{B}(\Omega)$ de las aplicaciones biyectivas de un conjunto Ω en sí mismo es un grupo no conmutativo respecto de la composición de aplicaciones.

Ejercicio 4.10 Demuestre que $(\mathcal{P}(\Omega), \triangle)$ es un grupo conmutativo, siendo $\triangle$ la diferencia simétrica.

Solución: Recordemos que si $X, Y \in \mathcal{P}(\Omega)$, entonces $X \triangle Y = (X \setminus Y) \cup (Y \setminus X) = (X \cap \overline{Y}) \cup (\overline{X} \cap Y)$. La operación $\triangle$ es claramente interna y conmutativa en $\mathcal{P}(\Omega)$. Veamos que es asociativa. Sean $A, B, C \in \mathcal{P}(\Omega)$. Se verifica:

$$\begin{aligned}(A \triangle B) \triangle C &= [(A \cap \overline{B}) \cup (\overline{A} \cap B)] \triangle C \\ &= [(A \cap \overline{B}) \cup (\overline{A} \cap B) \cap \overline{C}] \cup \overline{[(A \cap \overline{B}) \cup (\overline{A} \cap B) \cap C]} \\ &= [(A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C})] \cup [[(\overline{A} \cup B) \cap (A \cup \overline{B})] \cap C]\end{aligned}$$

Pero,

$$\begin{aligned}[(\overline{A} \cup B) \cap (A \cup \overline{B})] \cap C &= [(\overline{A} \cap A) \cup (\overline{A} \cap \overline{B}) \cup (A \cap B) \cup (B \cap \overline{B})] \cap C \\ &= [(\overline{A} \cap \overline{B}) \cup (A \cap B)] \cap C \\ &= (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)\end{aligned}$$

y en consecuencia,

$$(A \triangle B) \triangle C = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)$$

Utilizando la propiedad conmutativa de $\triangle$, la fórmula anterior, y las propiedades conmutativa y asociativa de la unión y la intersección, se deduce que

$$\begin{aligned}A \triangle (B \triangle C) &= (B \triangle C) \triangle A \\ &= (B \cap \overline{C} \cap \overline{A}) \cup (\overline{B} \cap C \cap \overline{A}) \cup (\overline{B} \cap \overline{C} \cap A) \cup (B \cap C \cap A) \\ &= (A \triangle B) \triangle C\end{aligned}$$

El elemento neutro es el conjunto vacío pues $A \triangle \emptyset = \emptyset \triangle A = A$ para todo A, y el elemento simétrico de $A \in \mathcal{P}(\Omega)$ es el propio A pues $A \triangle A = \emptyset$. □

Ejemplo 4.11 Los pares siguientes no son un grupo:

1. $(\mathbb{N},+)$ y $(\mathbb{R},\cdot)$. Sólo el 0 tiene elemento opuesto en el primer caso, mientras que en el segundo caso, el 0 no tiene inverso.

2. $(\mathcal{P}(\Omega),\cap)$ y $(\mathcal{P}(\Omega),\cup)$. En ambos casos, ningún elemento, salvo el elemento neutro, tiene elemento simétrico, pues si $A\cap B=\Omega$ necesariamente $A=B=\Omega$. Análogamente, si $A\cup B=\emptyset$ entonces $A=B=\emptyset$.

3. El conjunto de matrices cuadradas de orden n con la multiplicación de matrices no es un grupo pues todas las matrices cuyo determinante es cero no tienen inversa.

Proposición 4.12 Propiedades en un grupo
Sea $(G,\star)$ un grupo. Se tiene:

1. Para todo $a,b,c\in G$, $a\star b=a\star c\Rightarrow b=c$. (Propiedad cancelativa)
2. Para todo $a,b\in G$, existe un único $x\in G$ tal que $a\star x=b$.
3. Si a^{-1} y b^{-1} son los simétricos de a y b, entonces $(a\star b)^{-1}=b^{-1}\star\ a^{-1}$

Demostración: 1. Basta componer a la izquierda con el elemento simétrico de a:

$$\begin{aligned} \text{De } a\star b &= a\star c \quad \text{se pasa a,}\\ a^{-1}\star(a\star b) &= a^{-1}\star(a\star c) \quad \text{y en consecuencia,}\\ (a^{-1}\star a)\star b &= (a^{-1}\star a)\star c\\ e\star b &= e\star c \quad \text{es decir, } b=c. \end{aligned}$$

2. Como en 1,

$$\begin{aligned} \text{de } a\star x &= b \quad \text{se pasa a,}\\ a^{-1}\star(a\star x) &= a^{-1}\star b \quad \text{y en consecuencia,}\\ (a^{-1}\star a)\star x &= a^{-1}\star b \quad \text{es decir,}\\ e\star x=x &= a^{-1}\star b \end{aligned}$$

3. Basta observar que
$\left(b^{-1}\star\ a^{-1}\right)\star(a\star b)=b^{-1}\star\left(a^{-1}\star a\right)\star b=b^{-1}\star e\star b=b^{-1}\star b=e$
y análogamente también se cumple $(a\star b)\star\left(b^{-1}\star\ a^{-1}\right)=e$.

□

Observaciones: La propiedad cancelativa indica que en un grupo $(G,\star)$, la aplicación $f_a\colon G\longrightarrow G$, con $a\in G$, tal que $f_a(x)=a\star x$ para todo $x\in G$, es una aplicación inyectiva.

En las tres propiedades ha de observarse que el orden en el que se disponen los elementos es importante cuando el grupo no es conmutativo. El inverso de $a \star b$ es $b^{-1} \star a^{-1}$ que no tiene porque coincidir con $a^{-1} \star b^{-1}$. También, cuando hemos hallado en 2, el elemento $x = a^{-1} \star b$ tal que $a \star x = b$, que puede ser diferente de $b \star a^{-1}$.

Ejemplo 4.13 Las siguientes tablas representan operaciones internas. Las dos primeras tablas representan dos operaciones, $\circledast$ y $\star$, en el conjunto $G = \{e, a\}$ mientras que la tercera tabla representa la operación $*$ en el conjunto $G' = \{e, a, b, c\}$.

$\circledast$	e	a
e	e	a
a	a	a

$\star$	e	a
e	e	a
a	a	e

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

Así el elemento que, por ejemplo, está situado en la intersección de la linea de b con la columna de c en la tercera tabla, es $b*c$ y en este caso, $b*c = a$. Veamos si definen estructura de grupo conmutativo o no.
En los tres casos e es el elemento neutro pues la fila y columna de e dejan invariante la primera fila y la primera columna respectivamente.
También se observa a primera vista que las tres operaciones son conmutativas pues las tablas son simétricas respecto de la diagonal principal (la que baja de izquierda a derecha).
En el primer caso, el elemento a no tiene simétrico, pues no existe ningún elemento a' tal que $a \circledast a' = e$. Luego $(G, \circledast)$ no es un grupo.
En el segundo caso, el simétrico de a es a.
En el tercer ejemplo los elementos simétricos de a, b y c son respectivamente los propios a, b y c.
La propiedad asociativa en el segundo caso se verifica comprobando que $x \star (y \star z) = (x \star y) \star z$ en todos los casos posibles de $x, y, z \in G$. Claramente se cumple si uno de los tres elementos es el elemento neutro e por tanto sólo hay que comprobar que $a \star (a \star a) = (a \star a) \star a$ que se cumple pues la operación es conmutativa.
La propiedad asociativa en el tercer cuadro es un poco más tediosa. Hay que comprobar que $a*(b*c) = (a*b)*c$, $a*(c*b) = (a*c)*b$, $a*(a*c) = (a*a)*c$, $a*(c*a) = (a*c)*a$, $a*(a*b) = (a*a)*b$, $a*(b*a) = (a*b)*a$, $b*(b*c) = (b*b)*c$, $b*(c*b) = (b*c)*b$, $b*(b*a) = (b*b)*a$, $b*(a*b) = (b*a)*b$, $c*(c*a) = (c*c)*a$, $c*(a*c) = (c*a)*c$, $c*(c*b) = (c*c)*b$ y $c*(b*c) = (c*b)*c$. Todos los demás casos se deducirían de los casos anteriores, la propiedad conmutativa y la del elemento neutro.
Este grupo se denomina grupo de Klein y tiene una representación geométrica en el que e es la identidad en el espacio tridimensional y a, b y c representan las simetrías axiales de eje Ox, Oy y Oz. La operación $*$ es la composición de movimientos.

Subgrupos

Dados el grupo $(G, \star)$ y el subconjunto no vacío H de G, consideramos la operación $\star$, restringida a los elementos del subconjunto H. Se dice que H es un **subgrupo** de G si $(H, \star)$ es a su vez un grupo. En particular, el subconjunto unitario $H = \{e\}$ siendo e el elemento neutro de G y el propio G son subgrupos de G.
Observemos que si para todos los elementos de G se cumple la propiedad asociativa, en particular se cumple para los elementos de H. Luego para verificar que H es un subgrupo de G hay que comprobar únicamente que:

i) Si $a, b \in H$ entonces $a \star b \in H$ (i.e., $\star$ es operación interna en H).

ii) $e \in H$, siendo e el elemento neutro de $\star$ en G.

iii) Si $a \in H$ entonces el elemento simétrico de a, a^{-1}, pertenece a H.

Estas condiciones se condensan en una en la siguiente proposición de caracterización de subgrupos.

Proposición 4.14 Sean un grupo $(G, \star)$ y H un subconjunto no vacío de G. H es un subgrupo de G si y sólo si para todo $a, b \in H$, $a \star b^{-1} \in H$.

Demostración: Es evidente que la condición es necesaria para que H sea un subgrupo. Veamos que es suficiente.
Supongamos que para todo $a, b \in H$, $a \star b^{-1} \in H$. Como $H \neq \emptyset$, existe $a \in H$,y en consecuencia $e = a \star a^{-1} \in H$. Luego el elemento neutro es un elemento de H y se cumple ii). En consecuencia, para todo $b \in H$ se tiene que $e \star b^{-1} = b^{-1} \in H$ y se cumple iii). Finalmente , la operación $\star$ es interna en H pues si $a, b \in H$, acabamos de ver que $b^{-1} \in H$ y por tanto $a \star (b^{-1})^{-1} = a \star b \in H$.

□

La ventaja de esta caracterización es que muchas veces se puede demostrar que $(H, \star)$ es un grupo demostrando que es un subgrupo de un grupo conocido. No hay entonces que demostrar la propiedad asociativa, ni la propiedad conmutativa si el grupo es conmutativo. Simplemente hay que ver que se satisface la propiedad de la proposición anterior.

Ejercicio 4.15 Sea $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
Demuestre que $(\mathbb{Z}[\sqrt{2}], +)$ es un grupo siendo $+$ la suma habitual de números reales restringida a $\mathbb{Z}[\sqrt{2}]$.
Solución: Basta ver que $\mathbb{Z}[\sqrt{2}]$ es un subgrupo de $(\mathbb{R}, +)$. Utilizamos la caracterización anterior. En efecto:
$\mathbb{Z}[\sqrt{2}] \neq \emptyset$ pues $0 = 0 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
Sean $z, z' \in \mathbb{Z}[\sqrt{2}]$. Comprobemos que $z - z' \in \mathbb{Z}[\sqrt{2}]$. Sean $a, a', b, b' \in \mathbb{Z}$ tales que $z = a + b\sqrt{2}$ y $z' = a' + b'\sqrt{2}$. Como $z - z' = a + b\sqrt{2} - (a' + b'\sqrt{2}) = a - a' + (b - b')\sqrt{2}$

y teniendo en cuenta que $a - a', b - b' \in \mathbb{Z}$ pues $(Z, +)$ es un grupo, se tiene que $z - z' \in \mathbb{Z}[\sqrt{2}]$. □

Ejercicio 4.16 Sean $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$, con $n \in \mathbb{N}^*$, y $2\pi\mathbb{Z} = \{2k\pi \mid k \in \mathbb{Z}\}$. Demuestre que ambos son grupos respecto de la suma de números reales restringida a cada uno de ellos.

Solución: El conjunto $n\mathbb{Z}$ es el conjunto de múltiplos de n. Veamos que $n\mathbb{Z}$ es subgrupo de $(\mathbb{Z}, +)$.

$n\mathbb{Z} \neq \emptyset$ pues $n \in n\mathbb{Z}$.

Sean $a, b \in n\mathbb{Z}$. Comprobemos que $a - b \in n\mathbb{Z}$. Sean k y $h \in \mathbb{Z}$ tales que $a = kn$ y $b = hn$. Como $a - b = kn - hn = (k - h)n$, teniendo en cuenta que $k - h \in \mathbb{Z}$ pues $(Z, +)$ es un grupo, se tiene que $a - b \in n\mathbb{Z}$.

De forma análoga se demuestra que $2\pi\mathbb{Z}$ es un subgrupo de $(\mathbb{R}, +)$. □

Congruencia módulo un subgrupo

Sea $(G, \star)$ un grupo conmutativo y sea H un subgrupo. La relación $\mathcal{R}_H$ en G definida para todo $a, b \in G$ por,

$$a \,\mathcal{R}_H\, b \quad \text{si y sólo si} \quad a \star b^{-1} \in H$$

es una relación de equivalencia, que se denomina **congruencia módulo H.**

Es *reflexiva*, pues para todo $a \in G$, $a \star a^{-1} = e \in H$ y en consecuencia $a \,\mathcal{R}_H\, a$.

Es *simétrica*, pues si $a \,\mathcal{R}_H\, b$ entonces $a \star b^{-1} \in H$. En consecuencia, $\left(a \star b^{-1}\right)^{-1} = b \star a^{-1} \in H$. Por tanto $b \,\mathcal{R}_H\, a$.

Es *transitiva*, pues si $a \,\mathcal{R}_H\, b$ y $b \,\mathcal{R}_H\, c$ entonces $a \star b^{-1} \in H$ y $b \star c^{-1} \in H$ y como la operación $\star$ es interna en H resulta que $(a \star b^{-1}) \star (b \star c^{-1}) = a \star c^{-1} \in H$, es decir, $a \,\mathcal{R}_H\, c$.

Estudiemos cómo son las clases de equivalencia. Sea $a \in G$ y $[a]$ la clase de a. Se tiene:

$$[a] = a \star H = \{a \star h \mid h \in H\}$$

En efecto, si $b \in [a]$ entonces el elemento $h = b \star a^{-1} \in H$ y resulta que $b = h \star a = a \star h$. Recíprocamente si $b = a \star h$ con $h \in H$, entonces $b \star a^{-1} = h \in H$. La expresión de las clases de equivalencia permite deducir las siguientes propiedades:

- Toda clase de equivalencia de la relación $\mathcal{R}_H$ es equipotente a H.

En efecto, sea $a \in G$ y $[a]$ la clase de a. Sea la aplicación ϕ: $H \longrightarrow [a]$ definida por, $\phi(h) = a \star h$ para todo $h \in H$. De la expresión de $[a]$, se deduce que ϕ es sobreyectiva. La inyectividad de ϕ resulta de la propiedad cancelativa que se satisface en todo grupo.

- Si card(G) es finito, entonces cualquier subgrupo H cumple que card(H) es un divisor de card(G).

Supongamos que G tiene n elementos y sea k el número de elementos de H. Por la propiedad anterior, todas las clases de equivalencia tienen k elementos. Denotaremos al conjunto cociente $G/\mathcal{R}_H$ por G/H. Como

$$G = \bigcup_{[a]\in G/H} [a] \quad \text{y si } [a],[b] \in G/H, \quad [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$$

resulta que $n = ck$, siendo c el número de clases distintas. En consecuencia, k es un divisor de n.

En un grupo con un número finito de elementos, a card(G) se le denomina **orden del grupo** G.

Ejemplo 4.17 Entre los conjuntos cocientes que hemos estudiado, ya nos hemos encontrado algunos que pueden ser considerados como conjuntos cocientes asociados a un subgrupo dado. En concreto, si tomamos $n\mathbb{Z}$ como subgrupo de $\mathbb{Z}$, o $2\pi\mathbb{Z}$ como subgrupo de $\mathbb{R}$, véase el ejercicio 4.16, obtenemos precisamente los conjuntos cocientes de los ejemplos 3.10 y 3.11, los enteros módulo n, $\mathbb{Z}/n\mathbb{Z}$ y los números reales módulo 2π, $\mathbb{R}/2\pi\mathbb{Z}$.

4.3. Anillos

Consideramos ahora conjuntos donde están definidas dos operaciones internas.
Por analogía con las operaciones internas de números y por comodidad, denotaremos la primera operación como suma, $+$, mientras que a la segunda la llamaremos producto, $\cdot$, e igual que en los números omitiremos a menudo el símbolo. Es decir, escribiremos ab por $a\cdot b$. El utilizar otros signos, por ejemplo, $\oplus$ y $\odot$, para representar las operaciones sería quizás más correcto pero muy engorroso y no lo haremos en general. Sólo utilizaremos otros símbolos en algún ejemplo donde las operaciones, ya conocidas, tienen su propio símbolo.

Definición 4.18 Sea A un conjunto y sean $+$ y $\cdot$ dos operaciones internas definidas en A. Diremos que $(A, +, \cdot)$ es un **anillo** si se satisfacen

1. $(A, +)$ es un grupo conmutativo.
2. La operación $\cdot$ es asociativa.
3. La operación $\cdot$ es **distributiva** respecto de la operación $+$, esto es,

$$a(b+c) = ab + ac \quad \text{y} \quad (b+c)a = ba + ca$$

Si, además, la operación $\cdot$ es conmutativa, se dice que $(A, +, \cdot)$ es un **anillo conmutativo**.
Si $(A, +, \cdot)$ es un anillo con elemento neutro para el producto, siendo éste distinto del elemento neutro de la suma, se dice que $(A, +, \cdot)$ es un **anillo unitario**.

Seguiremos la mismas notaciones aditiva y multiplicativa que utilizamos en los grupos. En concreto:
El elemento neutro de la suma se llama **elemento nulo** y se designa por 0.
El simétrico de a para $+$ se denomina **elemento opuesto** y se designa por $-a$.
El elemento neutro del producto, si existe, se denomina **elemento unidad** y se designa por 1. Además se cumple que $1 \neq 0$.
El simétrico de a para $\cdot$, si existe, se denomina **elemento inverso** de a y se designa por a^{-1}. En este caso se dice que a es un elemento **inversible**.
En las expresiones $ab+ac$ y $ba+ca$ de la propiedad distributiva, debería en realidad poner $(ab) + (ac)$ y $(ba) + (ca)$. Por convenio, se suprimen los paréntesis, porque al igual que en las operaciones entre números se atribuye prioridad al producto sobre la suma.
Si $n \in \mathbb{N}^*$, las notaciones na y a^n se escriben para indicar:

$$na = \overbrace{a + a + \cdots + a}^{n\text{veces}} \quad y \quad a^n = \overbrace{a \cdot a \cdot \cdots \cdot a}^{n\text{veces}}$$

Ejemplo 4.19 Ejemplos de anillos conocidos.

1. Veremos en capítulos posteriores que los conjuntos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son anillos conmutativos unitarios respecto de la suma y el producto habituales.

2. El conjunto de matrices cuadradas de orden n respecto de la suma y del producto de matrices es un anillo unitario no conmutativo.

Ejercicio 4.20 Demuestre que el conjunto $\mathcal{P}(\Omega)$ es un anillo conmutativo y unitario respecto de la diferencia simétrica $\triangle$ como "suma" y la intersección $\cap$ como "producto".

Solución: Vimos en el ejercicio 4.10 que $(\mathcal{P}(\Omega), \triangle)$ era un grupo conmutativo. Vimos en el capítulo 2 que la intersección es asociativa, conmutativa y con elemento unidad, Ω. Veamos la propiedad distributiva de $\cap$ respecto de $\triangle$. En efecto, para todo $A, B, C \in \mathcal{P}(\Omega)$ se tiene:

$$\begin{aligned} A \cap (B \triangle C) &= A \cap [(B \cap \overline{C}) \cup (\overline{B} \cap C)] \\ &= (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C) \\ &= \big((A \cap B) \cap (\overline{A} \cup \overline{C})\big) \cup \big((\overline{A} \cup \overline{B}) \cap (A \cap C)\big) \\ &= ((A \cap B) \cap \overline{(A \cap C)}) \cup (\overline{(A \cap B)} \cap (A \cap C)) \\ &= (A \cap B) \triangle (A \cap C) \end{aligned}$$

□

Proposición 4.21 Propiedades en un anillo
Sea $(A, +, \cdot)$ un anillo. Se tiene:

1. Para todo $a \in A$, $a \cdot 0 = 0 \cdot a = 0$. (Se dice que 0 es **absorbente** para el producto).
2. Para todo $a, b \in A$, $(-a)b = a(-b) = -(ab)$ y $(-a)(-b) = ab$.
3. Si además el anillo A es CONMUTATIVO se satisfacen las igualdades:
   $(a+b)^2 = a^2 + b^2 + 2ab$
   $(a+b)(a-b) = a^2 - b^2$
   $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$
   $= \sum_{p=0}^{n} \binom{n}{p} a^{n-p}b^p$ para todo $n \in \mathbb{N}^*$.
   (Binomio de Newton)

Demostración: 1. Usando la propiedad distributiva del producto respecto de la suma, $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$ y por la propiedad cancelativa de todo grupo, véase la proposición 4.12, se deduce que $a \cdot 0 = 0$. La otra igualdad se hace de manera análoga.

2. De $(ab) + [(-a)b] = (a + (-a))b = 0 \cdot b = 0$, se deduce que ab y $(-a)b$ son opuestos, es decir, $(-a)b = -(ab)$. Las otras igualdades son análogas.

3. Las dos primeras igualdades se obtienen teniendo en cuenta que $ab = ba$ Finalmente demostremos la fórmula del binomio de Newton por inducción sobre el exponente n.
i) Para $n = 1$ el resultado es trivial.
ii) Supongamos que la fórmula es cierta para n, esto es, $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$ y demostremos que $(a+b)^{n+1} = \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1}$. En efecto,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) \\
&= \left[\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n\right](a+b) \\
&= \binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{n-1}a^2b^{n-1} + \binom{n}{n}ab^n + \\
&\quad \binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n-1}ab^n + \binom{n}{n}b^{n+1} \\
&= \binom{n}{0}a^{n+1} + \left[\binom{n}{1} + \binom{n}{0}\right]a^n b + \left[\binom{n}{2} + \binom{n}{1}\right]a^{n-1}b^2 + \cdots \\
&\quad + \left[\binom{n}{n} + \binom{n}{n-1}\right]ab^n + \binom{n}{n}b^{n+1}
\end{aligned}$$

Teniendo en cuenta que $1 = \binom{n}{0} = \binom{n+1}{0} = \binom{n}{n} = \binom{n+1}{n+1}$ y que, compruébese,

$$\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}$$

se obtiene

$$(a+b)^{n+1} = \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \binom{n+1}{2}a^{n-1}b^2 + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1}.$$

□

Divisores de cero

En un anillo $(A, +, \cdot)$, se dice que el elemento $a \in A$, $a \neq 0$, es un **divisor de cero** si existe $b \in A$, $b \neq 0$, tal que $ab = 0$.

Ejemplo 4.22 En los anillos $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ no existen divisores de cero.
Sí existen divisores de cero en el anillo $(\mathcal{P}(\Omega), \triangle, \cap)$ pues todo subconjunto A de Ω tal que $A \neq \emptyset$, y $A \neq \Omega$ es un divisor de cero ya que $A \cap \overline{A} = \emptyset$.
También hay divisores de cero en el anillo de las matrices cuadradas de orden 2.

Por ejemplo, se tiene que $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$ es un divisor de cero pues tomando $B = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ se tiene que:

$$AB = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Ejercicio 4.23 Sea $(A, +, \cdot)$ un anillo unitario. Demuestre que si a es un divisor de cero entonces a no es inversible. En consecuencia, un elemento inversible no puede ser un divisor de cero.

Solución: Por reducción al absurdo, suponemos que a es un divisor de cero inversible. En consecuencia, existe el inverso de a, a^{-1}, y existe $b \neq 0$ tal que $ab = 0$. Multiplicando ambos miembros a la izquierda por a^{-1} se obtiene $a^{-1}(ab) = a^{-1}0 = 0$, esto es $(a^{-1}a)b = 1 \cdot b = b = 0$ que es una contradicción con la elección de b. □

Un anillo sin divisores de cero se denomina **anillo íntegro**.

Subanillos. Ideales

Sea $(A, +, \cdot)$ un anillo y sea H un subconjunto no vacío de A donde consideramos las restricciones de las operaciones de A. Se dice que H es un **subanillo** de A si $(H, +, \cdot)$ es a su vez un anillo. Cuando el anillo A es unitario entonces también se exige a todo subanillo que contenga al elemento unidad de A.

Observación: Si A es un anillo y consideramos $H = \{0\}$, con las operaciones restringidas, resulta que $H = \{0\}$ es un subanillo de A si A no es unitario mientras que $H = \{0\}$ no es un subanillo de A si A es unitario. Esta aparente anomalía se debe al hecho de que muchos autores bajo el término "anillo" engloban a lo que nosotros hemos llamado anillo unitario. En ese caso un subanillo es un anillo en su terminología, que en la nuestra se corresponde con la de anillo unitario. En resumen, todo subanillo de un anillo no unitario es por definición un anillo, mientras que un subanillo de un anillo unitario es un anillo unitario.

Igual que ocurría en los grupos, algunas propiedades del anillo A se satisfacen automáticamente en H, como la propiedad asociativa del producto o la propiedad distributiva del producto respecto de la suma. Es muy fácil demostrar la siguiente proposición que caracteriza a los subanillos de un anillo dado.

Proposición 4.24 Sean $(A, +, \cdot)$ un anillo y H un subconjunto no vacío de A. H es un subanillo de A si y sólo si para todo $a, b \in H$ se cumple:

i) $a - b \in H$

ii) $ab \in H$

iii) Si el anillo $(A, +, \cdot)$ es unitario entonces $1 \in H$.

Se observa que la condición i) asegura que $(H, +)$ es un subgrupo de $(A, +)$ (véase la proposición 4.14), mientras que la condición ii) significa que el producto es una operación interna en H. Por tanto, si se satisfacen las condiciones i) y ii) se puede asegurar que $(H, +, \cdot)$ es un anillo.

Como en los grupos, a veces es más rápido demostrar que $(A, +, \cdot)$ es un anillo, demostrando que es un subanillo de un anillo conocido. Así nos evitamos las propiedades asociativa y conmutativa de la suma, la propiedad asociativa del producto y la propiedad distributiva del producto sobre la suma. Todas estas propiedades si se satisfacen para los elementos en A, se satisfacen en particular para los elementos de H.

Ejercicio 4.25 Demuestre que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, con la suma y producto usuales, es un subanillo de $\mathbb{R}$.

Solución: Como ya vimos en el ejercicio 4.15, $(\mathbb{Z}[\sqrt{2}], +)$ era un subgrupo de $(\mathbb{R}, +)$. Sólo tenemos que demostrar que el producto es interno en $\mathbb{Z}[\sqrt{2}]$ y que $1 \in \mathbb{Z}[\sqrt{2}]$. De

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + a'b)\sqrt{2}$$

se deduce que el producto es interno en $\mathbb{Z}[\sqrt{2}]$. Además, $1 = 1 + 0\sqrt{2}$ y por tanto $1 \in \mathbb{Z}[\sqrt{2}]$. □

Ejercicio 4.26 ¿Por qué $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ no es un subanillo de $\mathbb{Z}$ para $n \geqslant 2$?

Solución: Aunque en el ejercicio 4.16 demostramos que $n\mathbb{Z}$ era un subgrupo de $(\mathbb{Z}, +)$, y claramente si $a, b \in n\mathbb{Z}$ entonces $ab \in n\mathbb{Z}$, sin embargo, $1 \notin n\mathbb{Z}$. En este caso $(n\mathbb{Z}, +, \cdot)$ no es un subanillo del anillo unitario $(\mathbb{Z}, +, \cdot)$, pero sí que es un anillo con las operaciones de $\mathbb{Z}$ restringidas a $n\mathbb{Z}$. □

De entre los subconjuntos de un anillo, además de los subanillos, los ideales juegan un papel muy relevante, véase por ejemplo, el ejercicio 9. Para simplificar la introducción del concepto, nos limitaremos al caso de anillos conmutativos.

Definición 4.27 Sean $(A,+,\cdot)$ un anillo conmutativo e I un subconjunto no vacío de A. Se dice que I es un **ideal** de A si se cumple:

i) $a-b\in I$ para todo $a,b\in I$.

ii) $ac\in I$ para todo $a\in I$ y para todo $c\in A$.

Se observa que la condición i) asegura que $(I,+)$ es un subgrupo de $(A,+)$, mientras que de la condición ii) se deduce que el producto es, en particular, una operación interna en I. Por tanto, todo ideal $(I,+,\cdot)$ es un anillo.

Ejemplo 4.28

1. $n\mathbb{Z}=\{kn \mid k\in\mathbb{Z}\}$, $n\in\mathbb{N}$ es un ideal de $\mathbb{Z}$ pues si $a\in n\mathbb{Z}$ y $c\in\mathbb{Z}$, existe $k\in\mathbb{Z}$ tal que $a=kn$ y en consecuencia, $ac=(kn)c=(kc)n\in n\mathbb{Z}$.
   Para $n=0$, se obtiene $I=\{0\}$, mientras que para $n=1$ se obtiene $I=\mathbb{Z}$. De hecho:

2. $\{0\}$ y A son siempre ideales del anillo A.

3. $\mathbb{Z}[\sqrt{2}]$ no es un ideal de $\mathbb{R}$ pues tomando $a=1\in\mathbb{Z}[\sqrt{2}]$ y $c\in\mathbb{R}\setminus\mathbb{Z}[\sqrt{2}]$, resulta que $ac=c\notin\mathbb{Z}[\sqrt{2}]$.

Definición 4.29 Si $(A,+,\cdot)$ es un anillo conmutativo y $a\in A$ es un elemento fijo, el conjunto

$$aA=\{ak \mid k\in A\}$$

también denotado por (a), es un ideal de A que se denomina **ideal principal** generado por a.

Veremos en el capítulo 5 que todos los ideales de $\mathbb{Z}$ son principales.

4.4. Cuerpos

Un **cuerpo** es un anillo conmutativo unitario en el que todo elemento no nulo es inversible respecto del producto.

Recordemos todas sus propiedades.

Definición 4.30 Sea $\mathbb{K}$ un conjunto y sean $+$ y $\cdot$ dos operaciones internas definidas en $\mathbb{K}$.
$(\mathbb{K}, +, \cdot)$ es un **cuerpo** si se satisfacen las siguientes propiedades:

1. Las operaciones $+$ y $\cdot$ son asociativas en $\mathbb{K}$.
2. Las operaciones $+$ y $\cdot$ son conmutativas en $\mathbb{K}$.
3. La operación $\cdot$ es distributiva respecto de la operación $+$ en $\mathbb{K}$.
4. Existen dos elementos distintos en $\mathbb{K}$ que se designan por $0, 1$ que son elementos neutros de la suma y del producto respectivamente.
5. Existencia de opuestos: para todo elemento a de $\mathbb{K}$ existe el simétrico de a respecto de la suma que se designa por $-a$.
6. Existencia de inversos: para todo elemento $a \neq 0$ de $\mathbb{K}$ existe el simétrico de a para el producto que se designa por a^{-1}.

Observación: En la literatura matemática, la definición de cuerpo no siempre incluye la conmutatividad del producto. En ese caso, cuando el producto es conmutativo lo indican denominándolo cuerpo conmutativo. Nosotros entenderemos que en un cuerpo el producto es conmutativo. Seguimos en este sentido la terminología inglesa que denomina *field* a lo que hemos denominado cuerpo mientras que si el producto no es conmutativo se denomina anillo de división (*division ring*).
Si $(\mathbb{K}, +, \cdot)$ es un cuerpo y H es un subconjunto de $\mathbb{K}$, consideramos las restricciones a H de las operaciones en $\mathbb{K}$. Se dice que H es un **subcuerpo** de K si $(H, +, \cdot)$ es a su vez un cuerpo.

Ejemplo 4.31 Veremos en los capítulos siguientes que $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son cuerpos. Sin embargo, $(\mathbb{Z}, +, \cdot)$ o $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ no son cuerpos pues no todos los elementos no nulos son inversibles, por ejemplo, $x = 2$ no es inversible ni en $\mathbb{Z}$, ni en $\mathbb{Z}[\sqrt{2}]$.

Ejemplo 4.32 Consideramos el conjunto cociente de los enteros módulo 3, $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, de los ejemplos 3.10 y 4.17 y definimos las operaciones $+$ y $\cdot$ tomando representantes en cada clase de equivalencia, esto es:

$$[a] + [b] = [a + b] \text{ y } [a] \cdot [b] = [a \cdot b]$$

Se comprueba que las operaciones no dependen de los representantes escogidos (véase

el ejercicio 9) y se obtienen las tablas siguientes:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Las propiedades asociativa y conmutativa de ambas operaciones se deducen de las propiedades conmutativa y asociativa de la suma y del producto en $\mathbb{Z}$.
Es fácil comprobar que $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ es un cuerpo.

Consideremos ahora el conjunto cociente de los enteros módulo 4, $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, y definiendo de nuevo las operaciones $+$ y $\cdot$ mediante

$$[a] + [b] = [a + b] \text{ y } [a] \cdot [b] = [a \cdot b]$$

se obtiene:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

En este caso $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ es un anillo conmutativo unitario pero no es un cuerpo pues 2 no es inversible: basta recorrer la fila o columna del 2 para observar que no existe ningún elemento x tal que $2x = 1$. □

Del ejercicio 4.23 se deduce que un cuerpo no puede tener divisores de cero. Por tanto si $\mathbb{K}$ es un cuerpo, entonces el producto es una operación interna en $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Recordando parte de lo estudiado en este tema se tiene:

Proposición 4.33 Sea $\mathbb{K}$ un conjunto y sean $+$ y $\cdot$ dos operaciones internas definidas en K.
$(\mathbb{K}, +, \cdot)$ es un cuerpo si y sólo si se cumplen las siguientes propiedades:

1. $(\mathbb{K}, +)$ es un grupo conmutativo.
2. $(\mathbb{K}^*, \cdot)$ es un grupo conmutativo.
3. La operación $\cdot$ es distributiva respecto de la operación $+$ en $\mathbb{K}$.

Como todo cuerpo $(\mathbb{K}, +, \cdot)$ es un anillo conmutativo, se satisfacen en particular todas las propiedades, válidas para anillos, de la proposición 4.21. Asimismo, $(\mathbb{K}^*, \cdot)$ satisface todas las propiedades, válidas para grupos, de la proposición 4.12. En particular, en un cuerpo $(\mathbb{K}, +, \cdot)$ se obtiene:

- $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in \mathbb{K}$.
- Si $a \cdot b = 0$ entonces $a = 0$ o $b = 0$. (No hay divisores de 0)
- Si $ab = ac$ y $a \neq 0$ entonces $b = c$. (Propiedad cancelativa en $(\mathbb{K}^*, \cdot)$)
- Si $a \neq 0$ y $b \in \mathbb{K}$, la ecuación $ax + b = 0$ tiene solución única en $\mathbb{K}$, $x = -ba^{-1}$.

Igual que para los anillos se introdujo el concepto de subanillo, el concepto de subcuerpo es análogo. Sea $(\mathbb{K}, +, \cdot)$ un cuerpo y sea H un subconjunto no vacío de $\mathbb{K}$ donde consideramos las restricciones de las operaciones de $\mathbb{K}$. Se dice que H es un **subcuerpo** de $\mathbb{K}$ si $(H, +, \cdot)$ es a su vez un cuerpo.

Teniendo en cuenta las proposiciones 4.14 y 4.33 resulta inmediata la siguiente proposición.

Proposición 4.34 Sean $(\mathbb{K}, +, \cdot)$ un cuerpo y H un subconjunto no vacío de $\mathbb{K}$. H es un subcuerpo de $\mathbb{K}$ si y sólo si se verifica:
i) $a - b \in H$ para todo $a, b \in H$.
ii) $ab^{-1} \in H$ para todo $a, b \in H^* = H \setminus \{0\}$.

4.5. Orden y operaciones

Si en un conjunto tenemos definidas una relación de orden y una operación interna, el hecho de que se cumplan ciertas propiedades de compatibilidad entre la operación y la relación de orden permite trabajar con "desigualdades"de manera similar a como se trabaja con desigualdades con números. Por simplificar, en este apartado supondremos que todas las operaciones son conmutativas.

Supongamos que tenemos un grupo conmutativo G donde por comodidad denotamos por $+$ la operación interna de G, siendo 0 el elemento neutro de $(G, +)$ y $-a$ el elemento simétrico de a. Sea una relación de orden $\preceq$ definida sobre G. Se dice que $(G, +, \preceq)$ es un **grupo ordenado** si la relación de orden es compatible con la suma, esto es:

$$\text{para todo } a, b \text{ y } c \in G \qquad a \preceq b \implies a + c \preceq b + c$$

Observemos que en este caso si $m, n \in G$ son tales que $0 \preceq m$ y $0 \preceq n$ entonces $0 \preceq m+n$ pues sumando n en los dos términos de $0 \preceq m$, se obtiene $n \preceq m+n$ y por la propiedad transitiva se obtiene $0 \preceq m+n$. Por analogía con los números se dice que el elemento $a \in G$ es **positivo** si se cumple $0 \preceq a$ y el conjunto de los elementos positivos de G se denota por G_+. Se dice que el elemento $a \in G$ es **negativo** si $a \preceq 0$.
Indistintamente se escribe $b \succeq a$ para indicar $a \preceq b$ que se lee como b "sucede", "es posterior" o "es mayor o igual" a a. La notación $a \prec b$ o $b \succ a$ indica $a \preceq b$ y $a \neq b$.

Proposición 4.35 En un grupo ordenado $(G, +, \preceq)$ se satisfacen las siguientes propiedades:

1. $a \preceq b$ si y sólo si $b + (-a) \in G_+$.
2. Si $a \preceq b$ y $a' \preceq b'$ entonces $a + a' \preceq b + b'$.
3. Si $a \preceq b$ entonces $-b \preceq -a$.

Demostración: 1. De $a \preceq b$ sumando $-a$ en ambos miembros, se obtiene $0 \preceq b + (-a)$, esto es, $b + (-a) \in G_+$. El recíproco se obtiene sumando a en ambos miembros en la expresión $0 \preceq b + (-a)$.
2. De $a \preceq b$ y $a' \preceq b'$ se deduce que $a + a' \preceq b + a'$ y $b + a' \preceq b + b'$. De la propiedad transitiva de la relación de orden se deduce que $a + a' \preceq b + b'$.
3. De $a \preceq b$ se deduce sumando $-a$, que $0 \preceq b + (-a)$. Sumando $-b$, se obtiene $-b \preceq (-b) + b + (-a)$, es decir, $-b \preceq -a$.

□

Observación: La notación numérica de $b - a$ por $b + (-a)$ se extiende a todos los grupos con notación aditiva. De esta manera el punto 1 de la proposición anterior se escribe:

$$a \preceq b \quad \text{si y sólo si} \quad b - a \in G_+$$

Si la relación de orden es total, se dice que el grupo es un **grupo totalmente ordenado**.

Ejemplo 4.36

1. Veremos en los capítulos 5 y 6 que $(\mathbb{Z}, +, \leqslant)$, $(\mathbb{Q}, +, \leqslant)$ y $(\mathbb{R}, +, \leqslant)$ son grupos totalmente ordenados.

2. $(\mathbb{Q}^*, \cdot, \leqslant)$ no es un grupo ordenado pues el orden no es compatible con el producto, ya que $1 \leqslant 2$ y sin embargo para $c = -1$ no se cumple que $1(-1) \leqslant 2(-1)$. En cambio, sí es un grupo totalmente ordenado el conjunto de los

números racionales estrictamente positivos $(\mathbb{Q}_+^*, \cdot, \leqslant)$ pues veremos que si a, b y $c \in \mathbb{Q}_+^*$ si $a \leqslant b$ entonces $ac \leqslant bc$.

3. Consideramos en $\mathbb{R}^2$ la suma definida componente a componente, es decir, $(a,b) + (c,d) = (a+c, b+d)$ y el orden producto definido en el ejemplo 3.23,

$$(a,b) \leqslant_P (c,d) \qquad \text{si y sólo si} \qquad a \leqslant c \quad \text{y} \quad b \leqslant d$$

entonces $(\mathbb{R}^2, +, \leqslant_P)$ es un grupo parcialmente ordenado pues si $(a,b) \leqslant_P (c,d)$ y $(e,f) \in \mathbb{R}^2$ entonces $(a,b) + (e,f) \leqslant_P (c,d) + (e,f)$ puesto que de $a \leqslant c$ y $b \leqslant d$, se deduce que $a + e \leqslant c + e$ y $b + f \leqslant d + f$.

4. Sea $\mathcal{F}([0,1], \mathbb{R})$ el conjunto de funciones reales de variable en $[0,1] \subset \mathbb{R}$ donde, como es habitual, se define la suma de funciones y el orden, para todo $f, g \in \mathcal{F}([0,1], \mathbb{R})$, mediante:

   - $(f+g)(x) = f(x) + g(x)$ para todo $x \in [0,1]$.
   - $f \preceq g$ si y sólo si $f(x) \leqslant g(x)$ para todo $x \in [0,1]$.

   Se comprueba fácilmente que $(\mathcal{F}([0,1], \mathbb{R}), +, \preceq)$ es un grupo parcialmente ordenado.

Supongamos ahora que la relación de orden está definida sobre un conjunto A donde tenemos definida una estructura de anillo conmutativo $(A, +, \cdot)$. Ya vimos como en $\mathbb{Q}$ el orden $\leqslant$ no es en general compatible con el producto de números racionales aunque sin embargo, sí es compatible cuando nos restringimos a números positivos. Ésta será la condición que se pide a la segunda operación en un anillo ordenado.
Se dice que $(A, +, \cdot, \preceq)$ es un **anillo ordenado** si se cumple lo siguiente:

> i) Para todo a, b y $c \in A$ si $a \preceq b$ entonces $a + c \preceq b + c$.
> ii) Para todo $a, b \in A$ si $0 \preceq a$ y $0 \preceq b$ entonces $0 \preceq ab$.

Todo anillo ordenado, $(A, +, \cdot, \preceq)$, es en particular un grupo ordenado, $(A, +, \preceq)$. En consecuencia, en un anillo ordenado se satisfacen todas las propiedades de la proposición 4.35. De nuevo se designa por A_+ al conjunto de elementos positivos de A, $A_+ = \{a \in A \mid 0 \preceq a\}$.
Si la relación de orden es total, se dice que el anillo es un **anillo totalmente ordenado**. Si además, el anillo es un cuerpo hablaremos de un **cuerpo ordenado**.
En un anillo totalmente ordenado se define el **valor absoluto** de $a \in A$ mediante

$$|a| = \begin{cases} a & \text{si} \quad 0 \preceq a \\ -a & \text{si} \quad a \prec 0 \end{cases}$$

Proposición 4.37 En un anillo totalmente ordenado $(A, +, \cdot, \preceq)$ se satisfacen las siguientes propiedades:

1. $a \preceq b$ si y sólo si $b - a \in A_+$.
2. Si $a \preceq b$ y $a' \preceq b'$ entonces $a + a' \preceq b + b'$.
3. Si $a \preceq b$ entonces $-b \preceq -a$.
4. Si $a \preceq b$ y $0 \preceq c$ entonces $ac \preceq bc$.
5. Si $a \preceq b$ y $c \preceq 0$ entonces $bc \preceq ac$.
6. Para todo $a \in A$, $a^2 \succeq 0$.
7. Si A es un anillo unitario entonces $0 \prec 1$.
8. $|a| \succeq 0$ para todo $a \in A$ y $|a| = 0$ si y sólo si $a = 0$.
9. $|ab| = |a|\,|b|$ para todo $a, b \in A$.
10. $|a + b| \preceq |a| + |b|$ para todo $a, b \in A$.

Si además $(A, +, \cdot)$ es un CUERPO también se cumple:

11. Si $a \succ 0$ entonces $a^{-1} \succ 0$.
12. Si $0 \prec a \preceq b$ entonces $b^{-1} \preceq a^{-1}$.
13. Si $a \preceq b \prec 0$ entonces $b^{-1} \preceq a^{-1}$.

Demostración: Las propiedades 1, 2 y 3 se deducen de la proposición 4.35. La propiedad 8 se deduce sin ninguna dificultad.

4. Si $a \preceq b$ y $0 \preceq c$ entonces, $0 \preceq b-a$ y $0 \preceq c$. En consecuencia $0 \preceq (b-a)c = bc-ac$ y por tanto $ac \preceq bc$.

5. Si $a \preceq b$ y $c \preceq 0$ entonces $0 \preceq b - a$ y $0 \preceq -c$. En consecuencia $0 \preceq (b-a)(-c) = -bc + ac$ y por tanto $bc \preceq ac$.

6. Si $0 \preceq a$ de la propiedad ii) de la definición de anillo ordenado se deduce que $0 \preceq a \cdot a = a^2$. Si $a \preceq 0$, multiplicando ambos miembros por a y aplicando la propiedad 5 se deduce que $0 \cdot a \preceq a \cdot a$.

7. Basta tener en cuenta que $1 = 1 \cdot 1 = 1^2$ y por tanto $1 \succeq 0$. Teniendo en cuenta que $1 \neq 0$ se obtiene que $0 \prec 1$.

9. Se comprueba sin dificultad en los cuatro casos posibles: i) $0 \preceq a$ y $0 \preceq b$, ii) $a \prec 0$ y $0 \preceq b$, iii) $0 \preceq a$ y $b \prec 0$ y iv) $a \prec 0$ y $b \prec 0$.

10. Observemos, en primer lugar, que para todo $a \in A$ se cumple trivialmente que $a \preceq |a|$ y $-a \preceq |a|$.

i) Si $0 \preceq a + b$, entonces $|a + b| = a + b \preceq |a| + |b|$.

ii) En caso contrario, $a + b \prec 0$ y en consecuencia, $|a + b| = -a - b \preceq |a| + |b|$.

11. Supongamos $a \succ 0$. Si fuera $a^{-1} \preceq 0$, multiplicando por a ambos términos se deduce que $1 = aa^{-1} \preceq a \cdot 0 = 0$, que contradice la propiedad 7.

12 y 13. En ambos casos se obtiene que $ab \succ 0$. Por la propiedad anterior se deduce que $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \succ 0$. Entonces, si $a \preceq b$, multiplicando ambos miembros por $a^{-1}b^{-1}$, se obtiene $aa^{-1}b^{-1} \preceq ba^{-1}b^{-1}$, esto es, $b^{-1} \preceq a^{-1}$.

□

En los capítulos 5 y 6, veremos que el anillo $(\mathbb{Z}, +, \cdot, \leqslant)$ y los cuerpos $(\mathbb{Q}, +, \cdot, \leqslant)$ y $(\mathbb{R}, +, \cdot, \leqslant)$ son ordenados. También veremos en el capítulo 7, como la propiedad 6 de la proposición anterior, nos permite afirmar que no existe en el conjunto de los números complejos ninguna relación de orden total compatible con la estructura de cuerpo.

4.6. Homomorfismos

Vimos en el ejemplo 3.65 como la existencia de una biyección entre dos conjuntos puede dar lugar a un cierto tipo de identificación entre ambos conjuntos. Cuando estemos trabajando con conjuntos donde se tenga alguna estructura algebraica o de orden hablaremos de identificación cuando la biyección además conserve la estructura.

Sean G y G' dos conjuntos donde se tiene respectivamente definida una operación interna y por comodidad denotaremos ambas $+$. Sea $f : G \longrightarrow G'$ una aplicación. Se dice que f es un **homomorfismo** si se cumple que:

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

El homomorfismo se denomina **endomorfismo** cuando $G = G'$ y la operación interna es la misma. Si el homomorfismo es biyectivo hablaremos de **isomorfismo** y finalmente todo endomorfismo biyectivo se denomina **automorfismo**.

Ejemplo 4.38 Ejemplos de homomorfismos.

1. La aplicación f definida por $f(x) = e^x$ es un homomorfismo de $(\mathbb{R}, +)$ en $(\mathbb{R}, \cdot)$ puesto que se cumple que $f(a+b) = f(a)f(b)$ para todo $a, b \in \mathbb{R}$ ya que $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$. En general si $a > 0$, la aplicación $g(x) = a^x$

es un homomorfismo de $(\mathbb{R}, +)$ en $(\mathbb{R}, \cdot)$ que se denomina exponencial de base a.

2. Si $a \in \mathbb{R}$, $a \neq 0$, la aplicación f definida por $f(x) = ax$ es un automorfismo en $(\mathbb{R}, +)$.

3. Sea $(G, +)$ un grupo conmutativo. Las aplicaciones $f, g\colon G \longrightarrow G$ definidas por $f(a) = 3a$ y $g(a) = -a$, donde $3a = a + a + a$ y $-a$ es el elemento simétrico de a, son endomorfismos. En efecto, f es un endomorfismo pues para todo $a, b \in G$ se cumple que $f(a + b) = 3(a + b) = (a + b) + (a + b) + (a + b) = (a + a + a) + (b + b + b) = 3a + 3b = f(a) + f(b)$ donde hemos aplicado las propiedades asociativas y conmutativas de $+$. En general, la aplicación $h\colon G \longrightarrow G$ definida por $h(a) = na$ siendo $n \in \mathbb{N}^*$ es un endomorfismo.
También g es un endomorfismo pues $g(a + b) = -(a + b) = -a + (-b) = g(a) + g(b)$ en virtud del apartado 3 de la proposición 4.12.

Proposición 4.39 Propiedades de un homomorfismo

1. Si $f : G \longrightarrow G'$ es un homomorfismo entonces la operación de G' es una operación interna cuando se restringe al conjunto imagen $f(G)$.

2. Si $f\colon G \longrightarrow G'$ y $g\colon G' \longrightarrow G''$ son homomorfismos entonces la composición $g \circ f\colon G \longrightarrow G''$ es un homomorfismo.

3. Si $f\colon G \longrightarrow G'$ es un isomorfismo entonces la aplicación inversa $f^{-1}\colon G' \longrightarrow G$ es un isomorfismo.

Demostración: 1. Supongamos que a' y $b' \in f(G)$; veamos que $a' + b' \in f(G)$. En efecto, sean a y $b \in G$ tales que $f(a) = a'$ y $f(b) = b'$. En consecuencia, $f(a + b) = f(a) + f(b) = a' + b'$ y como $a + b \in G$ resulta que $a' + b' \in f(G)$.
2. $(g \circ f)(a+b) = g\big(f(a+b)\big) = g\big(f(a)+f(b)\big) = g\big(f(a)\big)+g\big(f(b)\big) = g \circ f(a)+g \circ f(b)$
3. Sabemos que si f es biyectiva, la aplicación inversa f^{-1} es biyectiva. Veamos que f^{-1} es un homomorfismo. Sean a' y $b' \in G'$ y sean $a = f^{-1}(a')$ y $b = f^{-1}(b')$. En consecuencia, $f(a) = a'$ y $f(b) = b'$ y por tanto, $a' + b' = f(a) + f(b) = f(a + b)$ de donde se deduce que $f^{-1}(a' + b') = a + b = f^{-1}(a') + f^{-1}(b')$.

□

Como consecuencia de esta proposición se deduce que la existencia de un isomorfismo entre dos conjuntos dotados de sendas operaciones internas, define una "relación" que satisface las siguientes propiedades:

1. Es reflexiva pues la aplicación identidad I_G es un isomorfismo.

2. Es *simétrica* pues si existe un isomorfismo $f\colon G \longrightarrow G'$, entonces la aplicación inversa $f^{-1} : G' \longrightarrow G$ es un isomorfismo.

3. Es *transitiva* pues si existen dos isomorfismos $f\colon G \longrightarrow G'$ y $g\colon G' \longrightarrow G''$ entonces la composición $g \circ f\colon G \longrightarrow G''$ es un isomorfismo.

Homomorfismos de grupos

En este apartado suponemos además que $(G,+)$ y $(G',+)$ son dos grupos tales que sus elementos neutros son respectivamente 0_G y $0_{G'}$ y $-a$ y $-a'$ denotan los elementos simétricos de $a \in G$ y $a' \in G'$. Sea $f\colon G \longrightarrow G'$ un homomorfismo. Se tiene:

1. $f(0_G) = 0_{G'}$.

2. $f(-a) = -f(a)$ para todo $a \in G$.

3. Si H es un subgrupo de G entonces,

$$f(H) = \{a' \in G' \mid \text{Existe } a \in H,\ f(a) = a'\}$$

es un subgrupo de G'.

4. Si H' es un subgrupo de G' entonces,

$$f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$$

es un subgrupo de G.

Demostración: 1. Basta observar que si $a \in G$ entonces $f(a) = f(0_G + a) = f(0_G) + f(a)$ y sumando $-f(a)$ a la expresión anterior se obtiene,
$0_{G'} = f(a) + (-f(a)) = f(0_G) + f(a) + (-f(a)) = f(0_G)$.
2. En efecto, como

$$\begin{aligned} f(-a) + f(a) &= f(-a + a) = f(0_G) = 0_{G'} \\ f(a) + f(-a) &= f(a + (-a)) = f(0_G) = 0_{G'} \end{aligned}$$

y por tanto $f(-a) = -f(a)$.
3. Supongamos que a' y $b' \in f(H)$; veamos que $a' - b' \in f(H)$. En efecto, sean a y $b \in H$ tales que $f(a) = a'$ y $f(b) = b'$. Aplicando la propiedad anterior se obtiene que $f(a + (-b)) = f(a) + f(-b) = f(a) - f(b) = a' - b'$, y puesto que $a - b \in H$, resulta que $a' - b' \in f(H)$.
4. En primer lugar hacemos constar que el uso de la notación f^{-1} no presupone que f sea una aplicación biyectiva: Se utiliza f^{-1} en el sentido de relación inversa.
Supongamos que a y $b \in f^{-1}(H')$; veamos que $a - b \in f^{-1}(H')$.

Como $f(a-b) = f(a) - f(b)$, $f(a)$ y $f(b) \in H'$ y H' es un subgrupo de G' se obtiene que $f(a) - f(b) \in H'$ y en consecuencia, $a - b \in f^{-1}(H')$. □

De entre los subgrupos que determina un homomorfismo f mediante las propiedades 3 y 4 anteriores, son importantes el conjunto imagen Im $f = f(G)$ y el **núcleo** del homorfismo f que es precisamente $f^{-1}(\{0_{G'}\})$ y se denota por Ker f, es decir,

$$\text{Ker} f = \{a \in G \mid f(a) = 0_{G'}\}$$

Respecto de $f(G)$ y Ker f se tiene:

Teorema 4.40 Sean $(G,+)$ y $(G',+)$ dos grupos y $f: G \longrightarrow G'$ un homomorfismo. Se tiene:

1. Im f es un subgrupo de G'.
2. Ker f es un subgrupo de G.
3. f es inyectivo si y sólo si Ker $f = \{0_G\}$.
4. f es sobreyectivo si y sólo si Im $f = G'$.

Demostración: Sólo tenemos que demostrar el apartado 3 ya que los apartados 1 y 2 son consecuencia de las propiedades 3 y 4 anteriores y el cuarto apartado no es específico de los homomorfismos y sabemos que es válido para cualquier aplicación. Para todo $a, b \in G$ se tiene:

$f(a) = f(b)$ si y sólo si $f(a-b) = f(a) - f(b) = 0_{G'}$, es decir, $a - b \in$ Ker f

En consecuencia si Ker $f = \{0_G\}$ y $f(a) = f(b)$ entonces $a - b = 0_G$, es decir, $a = b$ y por tanto f es inyectiva. Recíprocamente, si f es inyectiva y $c \in$ Ker f entonces $f(c) = 0_{G'} = f(0_G)$ y por tanto, $c = 0_G$.

□

El punto 3 del teorema anterior es muy interesante pues reduce considerablemente el trabajo de comprobar si un determinado homomorfismo es inyectivo.

Ejemplo 4.41

1. Consideremos el grupo $(M, \times)$, siendo M el conjunto de las matrices cuadradas inversibles de orden 2 y $\times$ el producto de matrices, y el grupo multiplicativo $(\mathbb{R}^*, \cdot)$. La aplicación que a toda matriz A le asocia su determinante es un homomorfismo de grupos pues se cumple la regla, *el determinante del producto de dos matrices de M es igual al producto de los determinantes de ambas matrices*. No es un isomorfismo. En efecto, observemos que en este caso, $0_G = 0_M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y $0_{G'} = 0_{\mathbb{R}^*} = 1$. El homomorfismo no es es inyectivo pues $\text{Ker } f \neq \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Basta tomar $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, pues $A \in \text{Ker } f$ ya que $f(A) = \det(A) = 1$.

2. Retomemos el ejemplo 4.38.1 con $f(x) = e^x$ pero restringiendo el conjunto donde f toma valores; $f\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \cdot)$. Además de cumplir las propiedades de la función exponencial, este homorfismo entre grupos es biyectivo; el isomorfismo inverso es la función de $(\mathbb{R}_+^*, \cdot)$ en $(\mathbb{R}, +)$ que se denomina función logaritmo neperiano y se denota $f^{-1}(x) = \log x$.

3. Sea $(G, +)$ un grupo y $a \in G$ fijo . Consideramos la aplicación

$$f : \begin{cases} (\mathbb{Z}, +) & \longrightarrow & (G, +) \\ n & \longmapsto & f(n) = na \end{cases}$$

donde $na = \overbrace{a + a + \cdots + a}^{n\text{veces}}$ si $n \in \mathbb{N}^*$, $0a = 0_G$ y $na = -[(-n)a]$ si $-n \in \mathbb{N}^*$. La aplicación f es un homomorfismo de grupos. El conjunto imagen

$$\text{Im } f = f(\mathbb{Z}) = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$$

es un subgrupo de G que se denomina **subgrupo de G generado por a**. El núcleo

$$\text{Ker } f = \{n \in \mathbb{Z} \mid na = 0\}$$

es un subgrupo de $\mathbb{Z}$.

4. ¿Es $f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definida por $f(x, y) = (x + y, 3x + 5y)$ inyectiva? Una vez que observamos que $f : (\mathbb{R}^2, +) \longrightarrow (\mathbb{R}^2, +)$ es un homomorfismo, basta con hallar el núcleo de f para poder responder. Como $\text{Ker } f = \{(x, y) \in \mathbb{R}^2 \mid (x + y, 3x + 5y) = (0, 0)\} = \{(0, 0)\}$, f es por tanto inyectiva.

Homomorfismos de anillos y cuerpos

Cuando nos encontremos con estructuras definidas con dos operaciones internas, los homomorfismos se definen extendiendo la propiedad a las dos operaciones. Concretamente, si $(A,+,\cdot)$ y $(A',+,\cdot)$ son dos anillos, un **homomorfismo de anillos** de A en A' es una aplicación $f\colon A \longrightarrow A'$ tal que para todo $a,b \in A$ se cumple que:

$$\boxed{\begin{array}{l} \text{i) } f(a+b) = f(a) + f(b) \\ \text{ii) } f(ab) = f(a)f(b) \end{array}}$$

Como todo homomorfismo de anillos es, en particular, un homomorfismo de grupos para la primera operación, se satisfacen todas las propiedades del teorema 4.40 para la primera operación y las propiedades de la proposición 4.39 para la segunda operación. En particular se deduce que Im $f = f(A)$ es a su vez un anillo. También se tiene que si el anillo A es conmutativo entonces Ker f es un ideal de A.
Un **homorfismo de cuerpos** no es más que un homomorfismo de anillos donde además $(A,+,\cdot)$ y $(A',+,\cdot)$ son dos cuerpos.

Homomorfismos de conjuntos ordenados

Cuando queremos hablar de identificaciones de estructuras ordenadas buscaremos biyecciones que conserven el orden. Con más precisión, si tenemos dos conjuntos ordenados $(U,\preceq)$ y $(V,\preccurlyeq)$, una aplicación $f\colon U \longrightarrow V$ se denomina **homomorfismo de estructuras de orden** si es creciente, es decir:

$$\text{para todo } u,u' \in U\,, \qquad \text{si } u \preceq u' \text{ entonces } f(u) \preccurlyeq f(u')$$

Cuando la aplicación f sea además biyectiva hablaremos de un **isomorfismo de estructuras ordenadas**.

En los próximos capítulos iremos introduciendo formalmente los conjuntos numéricos. Es frecuente ver escrito una cadena del tipo:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

En realidad, cuando se escriben estas inclusiones lo que se quiere indicar son identificaciones entre un conjunto y un subconjunto del conjunto siguiente. El tipo de identificación depende de la estructura con que se dota a los conjuntos.
Por ejemplo, la inclusión $\mathbb{Z} \subset \mathbb{Q}$ indica la existencia de un isomorfismo de anillos ordenados: de $(\mathbb{Z},+,\cdot,\leqslant)$ a un subanillo ordenado A de $\mathbb{Q}$, es decir una aplicación biyectiva f de $\mathbb{Z}$ a $A \subset \mathbb{Q}$ que conserva las operaciones y el orden. Estamos ante un isomorfismo de anillos ordenados.
Una vez establecido el isomorfirmo f, se identifica el elemento $z \in \mathbb{Z}$ con el elemento

$f(z) \in \mathbb{Q}$ y se escribe generalmente z en lugar de $f(z)$ y de ahí la escritura $\mathbb{Z} \subset \mathbb{Q}$.

La inclusión $\mathbb{R} \subset \mathbb{C}$ es también una identificación, pero en este caso, veremos en el último capítulo del libro, que no se puede dotar a $\mathbb{C}$ de un orden total compatible con las operaciones. Así, $\mathbb{R} \subset \mathbb{C}$ indica la existencia de una aplicación biyectiva de $\mathbb{R}$ a un subcuerpo $K \subset \mathbb{C}$ que conserva las operaciones. Estamos ante un isomorfismo h de cuerpos. Igualmente, se identifica el elemento $x \in \mathbb{R}$ con el elemento $h(x) \in \mathbb{C}$ y se escribe generalmente x en lugar de $h(x)$.

Comentarios

Aritmética de los números cardinales

Basándonos en conceptos conjuntistas se pueden definir dos operaciones, suma y producto, para números cardinales. Aunque los números cardinales no constituyen un conjunto emplearemos la misma terminología que la de operaciones en conjuntos. Ya hicimos lo mismo en el capítulo anterior al definir el orden de los cardinales.

Sean a y b dos números cardinales y sean A y B dos conjuntos tales que:

$$A \cap B = \emptyset, \quad a = \text{card}(A) \quad \text{y} \quad b = \text{card}(B)$$

Por definición:

$$a + b = \text{card}(A \cup B)$$

Es fácil ver que la definición no depende de la elección de los conjuntos A y B pues si $A \equiv A'$, $B \equiv B'$ y $A' \cap B' = \emptyset$, existen f biyección de A en A' y g biyección de B en B'. Como $A \cap B = \emptyset$ se puede definir la aplicación:

$$\begin{array}{rccl} h: & A \cup B & \longrightarrow & A' \cup B' \\ & x & \longmapsto & h(x) = \begin{cases} f(x) & \text{si } x \in A \\ g(x) & \text{si } x \in B \end{cases} \end{array}$$

Que h es una biyección es consecuencia de serlo f y g y de que $A' \cap B' = \emptyset$.
Para que la definición tenga siempre sentido hay que ver que dados dos números cardinales a y b, siempre existen A y B dos conjuntos tales que $A \cap B = \emptyset$, $a = \text{card}(A)$ y $b = \text{card}(B)$. En efecto, si X e Y son dos conjuntos tales que $a = \text{card}(X)$ y $b = \text{card}(Y)$ entonces los conjuntos $A = \{0\} \times X$ y $B = \{1\} \times Y$ son respectivamente equipotentes con X e Y y además cumplen que $A \cap B = \emptyset$.

Ejercicio 4.42 Justifique que la suma de cardinales satisface las siguientes propiedades:

1. Es conmutativa .
2. Es asociativa.
3. El cardinal 0 es el elemento neutro de la suma.
4. Si $a + b = 0$ entonces $a = 0$ y $b = 0$.

Ejercicio 4.43 Sean a y b dos números cardinales. Demuestre que se satisface la siguiente relación:

$$a \leqslant b \iff \text{Existe un número cardinal } c \text{ tal que } a + c = b$$

Solución: Sean A y B dos conjuntos tales que $a = \text{card}(A)$ y $b = \text{card}(B)$. Si $a \leqslant b$ entonces existe una aplicación inyectiva $i\colon A \to B$. Sean $A' = i(A) \subset B$ y $C = B \setminus A'$. Claramente, $B = A' \cup C$, $A' \cap C = \emptyset$ y $\text{card}(A) = \text{card}(A')$. En consecuencia, tomando $c = \text{card}(C)$ se tiene que $a + c = b$.
Recíprocamente, supongamos que existe un número cardinal c tal que $a + c = b$ y sean A, B y C tres conjuntos tales que $A \cap C = \emptyset$, $a = \text{card}(A)$, $b = \text{card}(B)$ y $c = \text{card}(C)$. En consecuencia, existe una aplicación biyectiva f de $A \cup C$ a B. Por tanto la restricción de f a A es una aplicación inyectiva de A a B. □

Veamos ahora como se define el producto de números cardinales.

Sean a y b dos números cardinales y sean A y B dos conjuntos tales que:

$$a = \text{card}(A) \quad \text{y} \quad b = \text{card}(B)$$

Por definición:

$$a \cdot b = \text{card}(A \times B)$$

Es fácil ver que la definición no depende de la elección de los conjuntos A y B pues si $A \equiv A'$ y $B \equiv B'$, existen f biyección de A en A' y g biyección de B en B'. Se puede definir la aplicación:

$$\begin{aligned} h: \quad A \times B &\longrightarrow A' \times B' \\ (x, y) &\longmapsto h\big((x, y)\big) = \big(f(x), g(y)\big) \end{aligned}$$

Que h es una biyección es consecuencia de serlo f y g, y por tanto $A \times B \equiv A' \times B'$ si $A \equiv A'$ y $B \equiv B'$.

Ejercicio 4.44 Justifique que el producto de cardinales satisface las siguientes propiedades:

1. Es conmutativo.
2. Es asociativo.
3. El número cardinal 1 es el elemento neutro del producto.
4. $a \cdot 0 = 0$ para todo número cardinal a.
5. Si $a \cdot b = 1$ entonces $a = 1$ y $b = 1$.
6. Si $a \cdot b = 0$ entonces $a = 0$ o $b = 0$.
7. Es distributivo respecto de la suma.

Solución: Daremos un esbozo de la demostración de cada propiedad.

1. Se basa en que la aplicación

$$\begin{aligned} f: \quad A \times B &\longrightarrow B \times A \\ (x,y) &\longmapsto f\big((x,y)\big) = (y,x) \end{aligned}$$

es biyectiva.

2. Se basa en que la aplicación

$$\begin{aligned} g: \quad (A \times B) \times C &\longrightarrow A \times (B \times C) \\ \big((x,y),z\big) &\longmapsto g\Big(\big((x,y),z\big)\Big) = \big(x,(y,z)\big) \end{aligned}$$

es biyectiva.

3. Sea $\{m\}$ un conjunto unitario. La propiedad se basa en que la aplicación

$$\begin{aligned} h: \quad A &\longrightarrow A \times \{m\} \\ x &\longmapsto h(x) = (x,m) \end{aligned}$$

es biyectiva.

4. Se basa en que $A \times \emptyset = \emptyset$.
5. Si el conjunto $A \times B$ sólo tiene un elemento entonces los conjuntos A y B sólo tienen un elemento.
6. Si el conjunto $A \times B$ no tiene elementos entonces el conjunto A es vacío o el conjunto B es vacío.
7. Hay que demostrar que

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

cualesquiera que sean los números cardinales a, b y c. Se toman tres conjuntos A, B y C tales que $B \cap C = \emptyset$, $a = \text{card}(A)$, $b = \text{card}(B)$ y $c = \text{card}(C)$. Basta comprobar que:

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \quad \text{y} \quad (A \times B) \cap (A \times C) = \emptyset$$

□