

Tema 3

Grupos

1. Leyes de composición interna

(1.1) Sea A un conjunto. Una *ley de composición interna* en A es una aplicación del producto cartesiano $A \times A$ en A . Las leyes de composición internas se suelen denotar con símbolos no alfanuméricos, como por ejemplo $+$, \cdot , $*$, \times , \otimes , \oplus , etc.

(1.2) Ejemplos.

- Las aplicaciones

$$\begin{array}{ll} + : \mathbb{Z} \times \mathbb{Z} & \longrightarrow \mathbb{Z} \\ (a, b) & \longmapsto a + b \end{array} \qquad \begin{array}{ll} \cdot : \mathbb{Z} \times \mathbb{Z} & \longrightarrow \mathbb{Z} \\ (a, b) & \longmapsto a \cdot b \end{array}$$

son leyes de composición interna en \mathbb{Z} .

- Sea A un conjunto, y sea E el conjunto de las aplicaciones de A en A . Entonces

$$\begin{array}{ll} \circ : E \times E & \longrightarrow E \\ (f, g) & \longmapsto g \circ f \end{array}$$

es una ley de composición interna en E .

- Sea m un entero positivo. Como consecuencia de la compatibilidad que existe entre la relación de congruencia módulo m y la suma y el producto de números enteros (ver (4.6) del tema anterior), tenemos que

$$\begin{array}{ll} + : \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow \mathbb{Z}_m \\ (\bar{a}, \bar{b}) & \longmapsto \overline{a + b} \end{array} \qquad \begin{array}{ll} \cdot : \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow \mathbb{Z}_m \\ (\bar{a}, \bar{b}) & \longmapsto \overline{a \cdot b} \end{array}$$

son leyes de composición interna en \mathbb{Z}_m .

2. Grupos

(2.1) Un *grupo* es una terna $(G, *, e)$, donde G es un conjunto, $*$ es una ley de composición interna en G y e es un elemento de G de manera que se satisfacen:

(2.1.1) (propiedad asociativa) para cualesquiera elementos g, g' y g'' de G ,

$$g * (g' * g'') = (g * g') * g'';$$

(2.1.2) (propiedad del elemento neutro) para todo elemento g de G ,

$$g * e = e * g = g;$$

(2.1.3) (propiedad del elemento inverso) para todo elemento g de G , existe un elemento g^{-1} de G tal que

$$g * g^{-1} = g^{-1} * g = e;$$

Si además se satisface que

(2.1.4) (propiedad conmutativa) para cualesquiera elementos g y g' de G ,

$$g * g' = g' * g$$

entonces se dice que $(G, *, e)$ es un grupo abeliano.

(2.2) Ejemplos.

- $(\mathbb{Z}, +, 0)$ es un grupo abeliano, pero $(\mathbb{N}, +, 0)$ no es un grupo porque, salvo 0, ningún elemento de \mathbb{N} tiene inverso en \mathbb{N} .
- $(\mathbb{Q} - \{0\}, \cdot, 1)$ es un grupo abeliano, pero $(\mathbb{Z} - \{0\}, \cdot, 1)$ no lo es porque, salvo 1 y -1 , ningún elemento de $\mathbb{Z} - \{0\}$ tiene inverso en $\mathbb{Z} - \{0\}$.
- $(\mathbb{R}, +, 0)$ y $(\mathbb{R} - \{0\}, \cdot, 1)$ son grupos abelianos. También son grupos abelianos $(\mathbb{C}, +, 0)$ y $(\mathbb{C} - \{0\}, \cdot, 1)$.
- Si m es un entero positivo, entonces $(\mathbb{Z}_m, +, \bar{0})$ es un grupo abeliano.
- Pongamos $m = 5$. Entonces $(\mathbb{Z}_5 - \{\bar{0}\}, \cdot, \bar{1})$ es un grupo abeliano. La tabla de la multiplicación en $\mathbb{Z}_5 - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ es

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(2.3) Cuando no hay posibilidad de confusión sobre la ley de composición interna o sobre el elemento neutro, solamente se menciona el conjunto, y se dice, por ejemplo, que G es un grupo.

La ley de composición interna de un grupo abeliano se denotan normalmente usando el símbolo “+”.

3. Subgrupos y homomorfismos de grupos

(3.1) Sea $(G, *, e)$ un grupo. Un *subgrupo* de G es un subconjunto H de G tal que $(H, *, e)$ también es un grupo, o equivalentemente, tal que

(3.1.1) $H \neq \emptyset$;

(3.1.2) para cualesquiera elementos g y h de H ,

$$g * h^{-1} \in H.$$

(3.2) Sean $(G, *, e)$ y (G', \times, e') dos grupos. Un *homomorfismo de grupos* es una aplicación $f : G \rightarrow G'$ tal que $f(g * h) = f(g) \times f(h)$ para cualesquiera $g, h \in G$.

Si $f : G \rightarrow G'$ es un homomorfismo de grupos, entonces

(3.2.1) $f(e) = e'$, porque $f(e) \times f(e) = f(e * e) = f(e)$, y operando con el inverso $(f(e))^{-1}$ de $f(e)$,

$$f(e) = (f(e))^{-1} \times f(e) \times f(e) = (f(e))^{-1} \times f(e) = e';$$

(3.2.2) si $g \in G$ y g^{-1} es su inverso, entonces $f(g^{-1})$ es el inverso de $f(g)$, porque

$$f(g) \times f(g^{-1}) = f(g * g^{-1}) = f(e) = e',$$

y de manera similar, $f(g^{-1}) \times f(g) = e'$.

(3.3) Sean $(G, *, e)$ y (G', \times, e') dos grupos y sea $f : G \rightarrow G'$ un homomorfismo de grupos. Se llama *núcleo de f* al conjunto

$$\text{Ker } f = \{g : g \in G, f(g) = e'\},$$

y se llama *imagen de f* al conjunto

$$\text{Im } f = \{g' : g' \in G', \exists g \in G, f(g) = g'\}.$$

El núcleo de f es un subgrupo de G , y la imagen de f es un subgrupo de G' .

(3.4) Sea $f : G \rightarrow G'$ un homomorfismo de grupos. Se dice que:

(3.4.1) f es un *monomorfismo* si f es inyectiva;

(3.4.2) f es un *epimorfismo* si f es sobreyectiva;

(3.4.3) f es un *isomorfismo* si f es biyectiva.

(3.5) Sea $f : G \rightarrow G'$ un homomorfismo de grupos. Entonces:

(3.5.1) f es un epimorfismo si, y sólo si, $\text{Im } f = G'$;

(3.5.2) f es un monomorfismo si, y sólo si, $\text{Ker } f = \{e\}$.

En efecto, si f es un monomorfismo y $g \in \text{Ker } f$ (o sea, $f(g) = e'$), entonces, dado que también $f(e) = e'$, se tiene que $g = e$.

Recíprocamente, si $\text{Ker } f = \{e\}$ y $g, h \in G$ son elementos tales que $f(g) = f(h)$, entonces $g * h^{-1} \in \text{Ker } f$, puesto que

$$f(g * h^{-1}) = f(g) \times f(h^{-1}) = f(h) \times f(h)^{-1} = e'.$$

Luego $g * h^{-1} = e$, y por lo tanto

$$g = g * h^{-1} * h = e * h = h.$$

4. Anillos y cuerpos

(4.1) Un anillo (asociativo y unitario) es una quintupla $(A, +, 0, \cdot, 1)$ donde A es un conjunto, “+”, “ \cdot ” son leyes de composición interna en A y $0, 1 \in A$ son tales que

(4.1.1) $(A, +, 0)$ es un grupo abeliano;

(4.1.2) La ley “ \cdot ” es asociativa, esto es, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para cualesquiera $a, b, c \in A$;

(4.1.3) La ley “ \cdot ” tiene como elemento neutro a 1, esto es, $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$;

(4.1.4) (propiedad distributiva) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ para cualesquiera $a, b, c \in A$.

Si además la ley “ \cdot ” tiene la propiedad conmutativa, esto es, si $a \cdot b = b \cdot a$ para cualesquiera $a, b \in A$, entonces se dice que A es un anillo conmutativo.

(4.2) Un cuerpo es un anillo $(K, +, 0, \cdot, 1)$ de manera que $(K - \{0\}, \cdot, 1)$ es un grupo abeliano.

(4.3) Ejemplos.

(4.3.1) $(\mathbb{Q}, +, 0, \cdot, 1)$ es un cuerpo.

(4.3.2) $(\mathbb{R}, +, 0, \cdot, 1)$ y $(\mathbb{C}, +, 0, \cdot, 1)$ son cuerpos.

(4.4) Ejemplo. Sea m un entero positivo. La quintupla $(\mathbb{Z}_m, +, \bar{0}, \cdot, \bar{1})$ (donde “+” y “ \cdot ” son la suma y el producto de clases de congruencia módulo m respectivamente) es un cuerpo si, y sólo si, m es primo.

En efecto, sabemos que $(\mathbb{Z}_m, +, \bar{0})$ es un grupo abeliano, y que $(H_m, \cdot, \bar{1})$, donde $H_m = \{\bar{a} \in \mathbb{Z}_m : \text{m.c.d.}(a, m) = 1\}$, también lo es. Además,

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \overline{a \cdot (b + c)} = \overline{ab + ac} = (\bar{a} \cdot \bar{b}) + (\bar{a} \cdot \bar{c})$$

para cualesquiera $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$.

Si m es primo, entonces $\mathbb{Z}_m - \{\bar{0}\} = H_m$ es un grupo abeliano, y por lo tanto \mathbb{Z}_m es un cuerpo.

Recíprocamente, si \mathbb{Z}_m es un cuerpo, entonces $(\mathbb{Z}_m - \{\bar{0}\}, \cdot, \bar{1})$ es un grupo abeliano. Supongamos, en ese caso, que m no es primo, y sean $1 < p < m$ un factor primo de m y $k = m/p$. Entonces $\bar{p}, \bar{k} \in \mathbb{Z}_m - \{\bar{0}\}$, pero $\bar{p} \cdot \bar{k} = \bar{0} \notin \mathbb{Z}_m - \{\bar{0}\}$ — una contradicción. Luego m tiene que ser primo.