Estructuras Algebraicas

Llamaremos **grupo** al par $(A, *)$ constituido por un conjunto, A, no vacío y una operación, $*$, sobre él que verifica las siguientes propiedades:

1. es *cerrada* en A: $a * b \in A \quad \forall\, a, b \in A$
2. *asociativa*: $(a * b) * c = a * (b * c), \quad \forall\, a, b, c \in A$
3. existencia de *elemento neutro*: $e \in A$ tal que $a * e = e * a = a, \quad \forall\, a \in A$
4. existencia de *elemento inverso/opuesto*: $\forall\, a \in G \quad \exists\, b \in A$ tal que $a * b = b * a = e$

Si todos los elementos del grupo $(A, *)$ verifican la propiedad *conmutativa*: $a * b = b * a, \quad \forall\, a, b \in A$; diremos que el grupo es conmutativo o abeliano.

Sea A un conjunto dotado de dos operaciones cerradas (leyes de composición), la suma y el producto, que denotaremos por $+$ y $\cdot$ respectivamente. Diremos que $(A, +, \cdot)$ es un **anillo** si se cumplen los siguientes axiomas:

1. $(A, +)$ es un grupo abeliano
2. el producto, $\cdot$, es *asociativo*: $(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall\, a, b, c \in A$
3. propiedades *distributivas*: $a + (b \cdot c) = a \cdot b + a \cdot c, \quad \forall\, a, b, c \in A$ y $(a + b) \cdot c = a \cdot c + b \cdot c, \quad \forall\, a, b, c \in A$

Si el producto es conmutativo decimos que el anillo es conmutativo. Si existe elemento neutro (unidad) para el producto se dice que el anillo es unitario (o con unidad).

Llamaremos **cuerpo** a todo anillo $(A, +, \cdot)$ unitario, conmutativo y tal que todo elemento distinto del cero posea inverso. Es decir, que verifique:

1. $(A, +)$ es grupo abeliano
2. $(A, \cdot)$ es grupo abeliano
3. propiedad distributiva: : $a + (b \cdot c) = a \cdot b + a \cdot c, \quad \forall\, a, b, c \in A$

1. Decide de manera razonada si los conjuntos son grupos con las operaciones indicadas:

a) Dado un conjunto no vacío X, el conjunto G de las biyecciones de X con la composición, $(G, \circ)$.

Calcula el cardinal de G si X es un conjunto finito.

b) $(\mathbb{Z}, *)$ donde para $n, m \in \mathbb{Z}, n * m = \min(n, m)$.

c) $(\mathbb{N}, *)$ donde para $n, m \in \mathbb{N}, n * m = n$.

d) $(A = \{M \in \mathbb{M}_2(\mathbb{Z}) : \det M = -1\}, \cdot)$.

e) $(B = \{M \in \mathbb{M}_2(\mathbb{Z}) : \det M = 1\}, \cdot)$.

f) $(C = \{M \in \mathbb{M}_2(\mathbb{Z}) : \det M = +1, -1\}, \cdot)$.

g) $(D = \{M \in \mathbb{M}_2(\mathbb{Q}) : M \text{ es trigular superior}\}, \cdot)$.

h) $(G = \{1, -1, i, -i\}, \cdot)$, donde $i^2 = -1$.

2. Demuestra que el conjunto $E = \{\overline{5}, \overline{15}, \overline{25}, \overline{35}\} \subset \mathbb{Z}/40\mathbb{Z}$ es un grupo con el producto módulo 40. Identifica el elemento neutro, y el opuesto de cada elemento.

3. Considera el conjunto $F = \{\overline{1}, \overline{9}, \overline{16}, \overline{22}, \overline{53}, \overline{74}, \overline{79}, \overline{81}, \lambda\} \subset \mathbb{Z}/91\mathbb{Z}$. Se sabe que F es un grupo con el producto módulo 91. ¿Cuál es el valor de λ?

4. Sea $(G = \{a, b, c\}, *)$ un grupo, donde a es el elemento neutro. Escribe su tabla. Deduce que el grupo es abeliano.

5. Sea $(A, +, \cdot)$ un anillo. Demuestra:

a) Si 0 denota el elemento neutro de $(A, +)$, entonces $a \cdot 0 = 0 \cdot a = 0$, para todo $a \in A$.

b) Si $-a$ denota el elemento opuesto de a en $(A, +)$, entonces

$$(-a) \cdot b = -(a \cdot b), \qquad a \cdot (-b) = -(a \cdot b), \qquad (-a) \cdot (-b) = (a \cdot b).$$

6. Sea $n \in \mathbb{N}$. Demuestra que las operaciones suma y producto en $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} [a] + [b] &= [a + b], \\ [a] \cdot [b] &= [a \cdot b]. \end{aligned}$$

están bien definidas (i.e. no dependen de los representantes elegidos).

a) Demuestra que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un anillo.

b) Demuestra que si $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un cuerpo entonces $n = p$ primo. A ese cuerpo se le denota por $\mathbb{F}_p$.

7. Sea d es un entero libre de cuadrados. En $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \,|\, a, b \in \mathbb{Z}\}$ se definen las operaciones:

$$\begin{aligned} (a + b\sqrt{d}) \;+\; (a' + b'\sqrt{d}) &= (a + a') + (b + b')\sqrt{d}, \\ (a + b\sqrt{d}) \;\cdot\; (a' + b'\sqrt{d}) &= (aa' + bb'd) + (ab' + ba')\sqrt{d}. \end{aligned}$$

Decidir si $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ es un anillo conmutativo con unidad.

8. Sea $(A, +, \cdot)$ un anillo con unidad. Se dice que $a \in A$ es invertible si existe $\widehat{a} \in G$ tal que $a \cdot \widehat{a} = 1 = \widehat{a} \cdot a$. Sea $\mathcal{U}(A)$ el conjunto de elementos invertibles de A. Demuestra que $(\mathcal{U}(A), \cdot)$ es un grupo.

9. Un anillo con unidad $(A, +, \cdot)$ se llama *anillo de división* si $\mathcal{U}(A) = A \setminus \{0\}$. Obsérvese que todo cuerpo es un anillo de división conmutativo. Se definen los cuaterniones (de Hamilton) como

$$\mathbb{H} = \{a + bi + cj + dk \,:\, a, b, c, d \in \mathbb{R}\} \text{ tal que } i^2 = j^2 = k^2 = ijk = -1.$$

Demuestra que $(\mathbb{H}, +, \cdot)$ es un anillo de división no conmutativo.