Estructuras Algebraicas

1. Sea $(A, \star)$ un magma. Demuestra:

a) Si $(A, \star)$ es un monoide, el elemento neutro de A es único.

b) Si $(A, \star)$ es un grupo, para todo $a \in A$ el elemento inverso de a es único.

2. Decide de manera razonada si los siguientes magmas son semigrupos, monoides o 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) $(D = \{M \in \mathbb{M}_2(\mathbb{Q}) : M \text{ es triangular superior}\}, \cdot)$.

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

3. 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.

4. Sea $(G, *)$ un grupo. Demostrar que si $a, b, c \in G$ se tiene:

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

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

5. 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?

6. Encuentra todas las tablas de multiplicar distintas que puede tener algún grupo con 1, 2, 3 o 4 elementos. Decide cuales son abelianos.

7. 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

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

8. Demuestra que si un anillo A cumple que el elemento neutro de la suma y de la multiplicación son el mismo, entonces $|A| = 1$. Recuerda que este anillo no es un cuerpo, pues en un cuerpo, por definición, $0 \neq 1$.

9. 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.

10. Sea d es un entero libre de cuadrados. En $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ 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.

11. 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 las matrices 2×2 con coeficientes en $\mathbb{C}$ de la forma

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\}.$$

Recuerda que $\overline{z}$ es el conjugado de z, es decir, $\overline{a+bi} = a - bi$ si $a, b \in \mathbb{R}$.

a) Si para $a \in \mathbb{R}$, llamamos

$$a = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Demuestra que $(a, b, c, d) \mapsto a + bI + cJ + dK$ es una biyección entre $\mathbb{R}^4$ y $\mathbb{H}$.

b) Demuestra que $I^2 = J^2 = K^2 = IJK = -1$. En resumen,

$$\mathbb{H} = \{a + bI + cJ + dK \, : \, a, b, c, d \in \mathbb{R}\} \text{ tal que } I^2 = J^2 = K^2 = IJK = -1.$$

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

12. Sea $(K, +, \cdot)$ un cuerpo.

a) Demuestra que si $a, b \in K$ y $a \cdot b = 0$, entonces $a = 0$ o $b = 0$.

b) En K, denotamos 1 al elemento neutro del producto, $2 = 1 + 1$, etc. Demuestra que si $|K|$ es finito, $n = \overbrace{1 + \cdots + 1}^{n \text{ veces}} = 0$ para algún $n \in \mathbb{N}$.

c) Demuestra que si $a \in K$ y $n = 0$ en K, entonces $\overbrace{a + \cdots + a}^{n \text{ veces}} = 0$.

d) Demuestra que el menor n que cumple que $n = 0$ en K es primo.

e) Si hay un cuerpo con 4 elementos, escribe su tabla de sumar.

f) Demuestra que si $a \in K$ y $a^2 \in \{0, 1, a\}$, entonces $a \in \{0, \pm 1\}$.

g) Encuentra un cuerpo con 4 elementos.

13. Para cada $n \in \mathbb{N}$, definimos $\mathbb{Z}/n\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}/n\mathbb{Z}\}$ con la suma y producto definidas por

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i. \end{aligned}$$

a) Demuestra que $\mathbb{Z}/2\mathbb{Z}[i], \mathbb{Z}/4\mathbb{Z}[i], \mathbb{Z}/5\mathbb{Z}[i]$ no son cuerpos, pero $\mathbb{Z}/3\mathbb{Z}[i]$ sí lo es.

b) Demuestra que si p es un primo de la forma $a^2 + b^2$, entonces $\mathbb{Z}/p\mathbb{Z}[i]$ no es un cuerpo.

14. Se define en $\mathbb{N} \times \mathbb{N}$ la relación

$$(n, m) \sim (r, s) \Longleftrightarrow n + s = m + r.$$

a) Demuestra que es una relación de equivalencia.

El conjunto cociente $\mathbb{N} \times \mathbb{N}/\!\sim$ lo denotamos por $\mathbb{Z}$, en el definimos las operaciones:

$$\begin{aligned} [(n, m)] + [(r, s)] &= [(n + r, m + s)], \\ [(n, m)] \cdot [(r, s)] &= [(nr + ms, ns + mr)]. \end{aligned}$$

b) Demuestra que las anteriores operaciones están bien definidas.

c) Demuestra que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.

15. En $\mathbb{Z} \times \mathbb{N}$ se define la relación

$$(a,b) \sim (c,d) \iff ad = bc.$$

a) Demuestra que es una relación de equivalencia.

El conjunto cociente $\mathbb{Z} \times \mathbb{N}/\sim$ lo denotamos por $\mathbb{Q}$, en el definimos las operaciones:

$$\begin{aligned}[(a,b)] + [(c,d)] &= [(ad+bc, bd)],\\ [(a,b)] \cdot [(c,d)] &= [(ac, bd)].\end{aligned}$$

b) Demuestra que las anteriores operaciones están bien definidas.

c) Demuestra que $(\mathbb{Q}, +, \cdot)$ es un cuerpo.

16. 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 $\mathbb{F}_p$.

17. En $\mathbb{R}^2$ definimos las operaciones

$$\begin{aligned}(a,b) + (c,d) &= (a+c, b+d),\\ (a,b) \cdot (c,d) &= (ac-bd, ad+bc).\end{aligned}$$

a) Demuestra que $(\mathbb{R}^2, +, \cdot)$ es un cuerpo.

b) Calcula (x,y) satisfaciendo cada una de las siguiente ecuaciones:

$$\begin{aligned}(x,y)^2 + (-1,0) &= (0,0),\\ (x,y)^2 + (5,0) &= (0,0),\\ (x,y)^2 + (-5,0) &= (0,0),\\ (x,y)^2 + (x,y) + (-1,0) &= (0,0),\\ (x,y)^3 + (-1,0) &= (0,0).\end{aligned}$$