1. Analizar en cada caso si $(G, \oplus)$ es un grupo, un monoide, un semigrupo o ninguno de ellos:

   a) $G = \mathbb{Z}$, $a \oplus b = a - b$.

   b) $G = \mathbb{N}_0$, $a \oplus b = a \cdot b$.

   c) G es el conjunto de polinomios de grado menor o igual que n, $n \in \mathbb{N}$, con la suma usual.

   d) G es el conjunto de polinomios de grado menor o igual que n y el polinomio nulo, $n \in \mathbb{N}$, con la suma usual.

   e) G es el conjunto de polinomios de grado igual a n, $n \in \mathbb{N}$, con la suma usual.

   f) $G = \mathbb{R}^{n \times n}$ con la suma usual.

   g) $G = \mathbb{R}^{n \times n}$ con el producto usual.

   h) $G = \mathbb{R}^{n \times n}$ con el producto definido por $(A \circ B)_{ij} = a_{ij} \cdot b_{ij}$.

   i) $G = \mathbb{Z}^+$ con el producto definido por $n \oplus k = \gcd(n, k)$.

   j) $G = \mathbb{Z}^+$ con el producto definido por $n \oplus k = \operatorname{lcm}(n, k)$.

   k) $G = \{f \in [0, 1] \to \mathbb{R} | f$ es funcion continua$\}$ con el producto definido por $f \oplus g = f + g$.

Soluciones

a) COMPLETAR.

b) COMPLETAR.

c) COMPLETAR.

d) COMPLETAR.

e) COMPLETAR.

f) COMPLETAR.

g) COMPLETAR.

h) COMPLETAR.

i) COMPLETAR.

j) COMPLETAR.

k) COMPLETAR.

2. Sea X un conjunto cualquiera. Probar que $(X \to X, \circ, id_X)$ es un monoide, donde $X \to X$ representa el conjunto de funciones de X en X.

   Solución COMPLETAR.

3. Sea X un conjunto cualquiera. Probar que $(X \to X, \Rightarrow, id_X)$ es un grupo, donde $X \Rightarrow X$ representa el conjunto de funciones biyectivas de X en X. A esta clase de grupo le llamaremos grupo de biyecciones.

   Solución COMPLETAR.

4. Probar que si G es un grupo y $a, b \in G$ entonces $(ab)^{-1} = b^{-1}a^{-1}$.

   Solución COMPLETAR.

5. Probar que si G es un grupo, $a, b \in \mathbb{Z}$ y $g \in G$ entonces $g^a g^b = g^{(a+b)}$.

   Solución COMPLETAR.

6. Probar que si G es un grupo abeliano entonces $\forall a, b \in G$ y $\forall n \in \mathbb{Z}$ es $(a \cdot b)^n = a^n \cdot b^n$.

   Solución COMPLETAR.

7. Probar que si G es un grupo y $g \in G$, entonces $(g^a)^b = g^{ab}$ para todos los enteros a, b.

   Solución COMPLETAR.

8. Diffie-Hellman. Alice y Bob desean ponerse de acuerdo en un número secreto. Sin em bargo, saben que sus comunicaciones son monitoreadas por Eve, lo cual parece imposibilitar esta tarea.

Utilizando el resultado del ejercicio anterior, y sabiendo que existe un grupo cíclico finito G y su generador g para los cuales resulta computacionalmente costoso resolver el problema de Diffie-Hellman (dados g^a y g^b, encontrar g^{ab}); proponer un protocolo que les permita a Alice y Bob establecer una clave en común y secreta.

Solución COMPLETAR.

9. Si G es un grupo tal que $(a \cdot b)^2 = a^2 \cdot b^2$ para todo par $a, b \in G$, probar que G es abeliano.

Solución COMPLETAR.

10. Sea $(M, \oplus, e)$ un monoide finito. Probar que si vale la ley de cancelación a derecha ($a \oplus c = b \oplus c \Rightarrow a = b$), entonces $(M, \oplus, e)$ es en realidad un grupo.

Solución COMPLETAR.

11. Sea $n \in \mathbb{Z}$. Definamos la relación $a \sim b$ si y solo si el resto de dividr a por n coincide con el resto de dividir b por b.

    a) Probar que $\sim$ es una relación de equivalencia en $\mathbb{Z}$.

    b) Consideremos ahora el conjunto de las clases de equivalencia definidas por $\sim$ en $\mathbb{Z}$, que notaremos $\mathbb{Z}_n$, es decir

    $$\mathbb{Z}_n = \{\overline{x} / x \in \mathbb{Z}\}$$

    donde

    $$\overline{x} = \{y \in \mathbb{Z} / x \sim y\}$$

    y definamos en $\mathbb{Z}_n$ la operación

    $$\overline{x} + \overline{y} = \overline{x + y}$$

    1) Verificar que esta operación esta bien definida. *Sugerencia*: probar que $a \sim b \iff \exists k \in \mathbb{Z} / a - b = nk$.
    2) Probar que $\mathbb{Z}_n$ es un grupo con dicha operación.

Soluciones

a) COMPLETAR.

b)

1) COMPLETAR.
2) COMPLETAR.

12. Sean $(G, \oplus)$ un grupo y $H \subseteq G$ con $H \neq \emptyset$. Probar que H es un subgrupo de G si y solo si:

- $a \oplus b \in H$, para todo par $a, b \in H$.
- $a^{-1} \in H$, para todo $a \in H$.

Soluciones COMPLETAR.

13. Probar que si H y K son subgrupos de un grupo G entonces $H \cap K$ es subgrupo de G.

Solución COMPLETAR.

14. Sean $a, b \in \mathbb{R}$, definimos

$$\begin{array}{rccc} \tau_{a,b} & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & \tau_{a,b}(x) = ax + b \end{array}$$

Sea $G = \{\tau_{a,b} / a \in \mathbb{R} - \{0\}, b \in \mathbb{R}\}$

a) Probar que G es un grupo bajo la composición.

b) Probar que $H = \{\tau_{a,b} \in G / a \in \mathbb{Q}\}$ es un subgrupo de G.

c) Sea $N = \{\tau_{1,b} \in G\}$. Probar que N es un subgrupo de G y que $g \in G, n \in N \Rightarrow gng^{-1} \in N$.

Soluciones

a) COMPLETAR.

b) COMPLETAR.

c) COMPLETAR.

15. Sea $(G, \oplus)$ un grupo y $\varphi : G \to G / \varphi(a) = a^{-1}$.

    a) Probar que φ es biyectiva.

    b) ¿Que relación hay entre φ y φ^{-1}?

    Soluciones

    a) COMPLETAR.

    b) COMPLETAR.

16. Probar que para todo monoide $(M, \otimes, e)$ existe un homomorfismo inyectivo emb: $(M, \otimes, e) \to (M \to M, \circ, id_X)$.

    Solución COMPLETAR.

17. Cayley. Probar que todo grupo $(G, \otimes, e)$ es isomorfo a un subgrupo de un grupo de biyecciones.

    Solución COMPLETAR.

18. Sea G un grupo cíclico. Probar que G es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$ para algun n.

    Solución COMPLETAR.

19. Verificar en cada uno de los siguientes casos si $\phi : G \to H$ es un homomorfismo de grupo:

    a) $G = H = \mathbb{R} - \{0\}$ bajo la multiplicación usual, $\phi(x) = x^2$.

    b) $G = H = \mathbb{R} - \{0\}$ bajo la multiplicación usual, $\phi(x) = 2^x$.

    c) $G = H = (\mathbb{R}, +)$, $\phi(x) = x + 1$.

    d) $G = H = (\mathbb{R}, +)$, $\phi(x) = 13x$.

Soluciones

a) COMPLETAR.

b) COMPLETAR.

c) COMPLETAR.

d) COMPLETAR.

20. COMPLETAR.

    a) COMPLETAR.

    b) COMPLETAR.

    c) COMPLETAR.

    Soluciones

    a) COMPLETAR.

    b) COMPLETAR.

    c) COMPLETAR.

21. COMPLETAR.

    Solución COMPLETAR.

22. COMPLETAR.

    Solución COMPLETAR.

23. COMPLETAR.

    Solución COMPLETAR.

24. COMPLETAR.

    Solución COMPLETAR.

25. COMPLETAR.

Solución COMPLETAR.

26. COMPLETAR.

Solución COMPLETAR.

27. COMPLETAR.

Solución COMPLETAR.

28. COMPLETAR.

Solución COMPLETAR.

29. COMPLETAR.

Solución COMPLETAR.

30. COMPLETAR.

Solución COMPLETAR.