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

Soluciones

a) No es ninguno de ellos pues $\oplus$ no es asociativa.

b) No es un grupo pues no existen inversos. Es un monoide (y semigrupo) donde el elemento neutro es 1.

c) No es grupo ni monoide pues no existe elemento neutro (el polinomio nulo no tiene grado). Es un semigrupo pues la suma de polinomios es asociativa.

d) Es un grupo (y también monoide y semigrupo) donde el elemento neutro es el polinomio nulo y el elemento inverso de $P(x)$ es $-P(x)$.

e) No es grupo ni monoide pues no existe elemento neutro (el polinomio nulo no tiene grado). Es un semigrupo pues la suma de polinomios es asociativa.

f) Es un grupo (y también monoide y semigrupo) donde el elemento neutro es la matriz nula y el inverso de M es $-M$.

g) No es un grupo pues en general no todas las matrices son invertibles. Es un monoide (y semigrupo) donde el elemento neutro es la matriz identidad.

h) Es un grupo (y también monoide y semigrupo) donde el elemento neutro es la identidad y el inverso de una matriz con entradas a_{ij} es una matriz con entradas $\frac{1}{a_{ij}}$.

i) No es grupo ni monoide pues no existe elemento neutro. Supongamos que exista, luego $\forall x : \gcd(e, x) = x$; es decir que e es múltiplo de cualquier número. Absurdo. Es un semigrupo pues es una operación asociativa.

j) No es grupo ni monoide pues no existe elemento neutro. Supongamos que exista, luego $\forall x : \operatorname{lcm}(e, x) = x$; es decir que todos los números son multiplos de e. Absurdo. Es un semigrupo pues es una operación asociativa.

k) Es un grupo (y también monoide y semigrupo) donde el elemento neutro es la función nula y el inverso de f es $-f$.

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

- Clausura: Sean $f, g \in G$, luego $x \in dom(f \circ g) \Rightarrow x \in X$. Ademas $f(g(x)) \in X$ luego $cod(f \circ g) = X$, es decir $f \circ g \in X \to X$.
- Asociatividad:

$$(f \circ (g \circ h))(x) = f(g \circ h(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$$

- Elemento neutro:

$$f \circ id(x) = f(id(x)) = f(x)$$

$$id \circ f(x) = id(f(x)) = f(x)$$

3. Sea X un conjunto cualquiera. Probar que $(X \Rightarrow X, \circ, id_X)$ 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

   - Clausura: Trivial pues la composición de biyecciones también es biyectiva.
   - Asociatividad: Análogo al grupo $X \to X$.
   - Elemento neutro: Análogo al grupo $X \to X$.
   - Elemento inverso: Para $f \in X \Rightarrow X$ resulta $f \circ f^{-1} = id$.

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

   Solución Como $(b^{-1}a^{-1})(ab) = b(aa^{-1})b^{-1} = bb^{-1} = 1$ entonces ab es inverso a derecha de $(b^{-1}a^{-1})$ luego:

   $$\left(b^{-1}a^{-1}\right) = \left(b^{-1}a^{-1}\right)e = \left(b^{-1}a^{-1}\right)\underbrace{(ab)(ab)^{-1}}_{e} = e(ab)^{-1} = (ab)^{-1}$$

   Análogamente para la izquierda.

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

   Solución Lo demostraremos por inducción en $a \in \mathbb{N}_0$.

   - Caso base $a = 0$: $g^{a+b} = g^{0+b} = g^b = eg^b = g^0 g^b = g^a g^b$.
   - Caso inductivo: Supongamos que $g^{a+b} = g^a g^b$

     $$g^{(a+1)+b} = g^{(a+b)+1} = g^{a+b}g = g^a g^b g = g^a g^{b+1} = g^a\left(gg^b\right) = (g^a g)\, g^b = g^{a+1}g^b$$

   Resta ver que sucede si $a < 0$. Sea $a = -k$ con $k \in \mathbb{N}$, luego

   $$g^a g^b = g^{a+b} \iff \left(g^a g^b\right)^{-1} = \left(g^{-k+b}\right)^{-1} \iff \left(g^a g^b\right)^{-1} = \left(g^{-k} g^b\right)^{-1} = \left(g^a g^b\right)^{-1}$$

   lo cual vale.

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

- Caso base $n = 0$: $(a \cdot b)^n = e = e \cdot e = a^n \cdot b^n$.
- Caso inductivo: Supongamos que $(a \cdot b)^n = a^n \cdot b^n$.
  - $(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b) = a^n \cdot b^n \cdot a \cdot b = a^n \cdot a \cdot b^n \cdot b = a^{n+1} b^{n+1}$.
  - $(a \cdot b)^{n-1} = (a \cdot b)^n \cdot (a \cdot b)^{-1} = a^n \cdot b^n \cdot b^{-1} \cdot a^{-1} = a^n \cdot a^{-1} \cdot b^n \cdot b^{-1} = a^{n-1} b^{n-1}$.

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 embargo, 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

$$(ab)^2 = a^2 b^2 \iff (ab)^2 (ab)^{-1} = a^2 b^2 (ab)^{-1} \iff$$

$$\iff ab = a^2 b^2 b^{-1} a^{-1} = a^2 b a^{-1} \iff b = aba^{-1} \iff ba = ab$$

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 Para $m \in M$ definimos $f_m : G \to G$ como $f_m(x) = x \oplus m$. Veamos que f es biyectiva:

- Inyectividad: Sean $f(x_1) = f(x_2)$, luego por definición de f resulta $x_1 \oplus m = x_2 \oplus m$ y por ley cancelativa $x_1 = x_2$.
- Sobreyectividad: Resulta ser consecuencia de que f es inyectiva y G es finito.

Ahora consideremos $m' \in G$ tal que $f_m(m') = e$, entones $m' \oplus m = e$ por lo que m' es inverso a izquierda de m.

Ademas $m \oplus \underbrace{m' \oplus m}_{e} = e \oplus m \iff m \oplus m' = e$, por lo que m' también es inverso a derecha de m.

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

   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)

- Reflexividad: Trivial.
- Transitividad: Sean $x, y, z \in \mathbb{Z}$ tales que $x \sim y$ y $y \sim z$, luego tenemos $x = an + r$, $y = bn + r$ y $z = cn + r$ (con $r < n$) por lo que $x \sim z$.
- Simetría: Sean $x, y \in \mathbb{Z}$ tales que $x \sim y$, luego tenemos $x = an + r$ e $y = bn + r$ por lo que $y \sim x$.

b)

1) COMPLETAR.
2)
   - Asociatividad:

     $$\overline{x}+(\overline{y}+\overline{z}) = \overline{x}+\overline{y+z} = \overline{x+(y+z)} = \overline{(x+y)+z} = (\overline{x}+\overline{y})+\overline{z}$$

   - Elemento neutro: $\overline{0}+\overline{x} = \overline{0+x} = \overline{x}$ y $\overline{x}+\overline{0} = \overline{x+0} = \overline{x}$.
   - Elemento inverso: $\overline{x}+\overline{(-x)} = \overline{x+(-x)} = \overline{0}$ y $\overline{(-x)}+\overline{x} = \overline{(-x)+x} = \overline{0}$.

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

- $\boxed{\Rightarrow}$:
  - Sean $a, b \in H$, luego por ser subgrupo $a \oplus b^{-1} \in H$ y nuevamente por la misma razón $a \oplus b \oplus a^{-1} \in H$. Como $a \oplus b = (a \oplus b \oplus a^{-1}) \oplus a^{-1}$ y H es grupo, entonces $a \oplus b \in H$.
  - Observemos que $e \in H$ pues para $x = y$ resulta $x \oplus y^{-1} \in H$ por ser grupo. Sea $a \in H$, luego $a^{-1} = e \oplus a^{-1}$ y como H es grupo, $a^{-1} \in H$.
- $\boxed{\Leftarrow}$: Sean $a, b \in H$ luego $b^{-1} \in H$, luego también $a \oplus b^{-1} \in H$.

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 algún 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. Sean $(G, \oplus)$ y $(H, \ominus)$ grupos y $h : (G, \oplus) \to (H, \ominus)$ un homomorfismo. Probar que:

    a) $h(e_G) = e_H$, donde e_G es el neutro de G y e_H el neutro de H.

    b) Si $a \in G$ es $h(a^{-1}) = h(a)^{-1}$.

    c) Si h es sobreyectiva y G es abeliano, entonces H es abeliano.

Soluciones

a) COMPLETAR.

b) COMPLETAR.

c) COMPLETAR.

21. Sean $f : G \to G'$ un homomorfismo de grupos, G' abeliano. Probar que si H es un subgrupo de G que contiene a $ker\,(f)$ entonces $H \lhd G$.

Solución COMPLETAR.

22. Sean $(G, \cdot)$ y $(H, \cdot')$ grupos, entonces definiendo $(g_1, h_1) \oplus (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot' h_2)$ resulta $(G \times H, \oplus)$ un grupo.

Solución COMPLETAR.

23. Sea G un grupo y M, N subgrupos normales de G tales que $G = M \cdot N$. Probar $G/\,(M \cap N) \cong G/M \times G/N$.

Solución COMPLETAR.

24. Sea G un grupo. Si definimos L como el conjunto de los subgrupos normales de G, entonces $(L, \cdot, \cap)$ es un retículo modular.

Solución COMPLETAR.

25. Hacer un diagrama de Hasse de los subgrupos normales del grupo de Klein ($V = \mathbb{Z}_2 \times \mathbb{Z}_2$). ¿El retículo L del apartado anterior es distributivo?

Solución COMPLETAR.

26. Sean G, H grupos. Si $A \lhd G$ y $B \lhd H$, entonces $(G \times H)\,/\,(A \times B) \cong (G/A) \times (H/B)$.

Solución COMPLETAR.

27. Probar que existen sólo dos grupos distintos de orden 4 (salvo isomorfismo). Ayuda: utilizar el teorema de Lagrange para probar que un grupo de orden 4 que no es cíclico debe consistir de la identidad y tres elementos de orden 2

Solución COMPLETAR.

28. Probar que todo subgrupo de $\mathbb{Z}$ es de la forma $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$ para algún $n \in \mathbb{N}$. Mostrar que $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Solución COMPLETAR.

29. Probar que si N es un subgrupo de índice 2 en un grupo G, entonces N es normal en G.

Solución COMPLETAR.

30. En la práctica de relaciones se definió al kernel de una función $f : A \to B$ como la relación:

$$ker\,(f) = \{(a, a')\,|a, a' \in A, f\,(a) = f\,(a')\}$$

Explicar la relación entre el kernel de un homomorfismo definido para grupos, y el kernel de la función que plantea el homomorfismo.

Solución COMPLETAR.