Práctica 3: Semigrupos, Monoides y Grupos

Semigrupos, Monoides y Grupos

1. Analizar en cada caso si es un grupo, un monoide, un semigrupo o ninguno de ellos:

a) $(\mathbb{Z}, -)$.

b) $(\mathbb{N}, \times)$.

c) $(\mathbb{R}^{>0}, \times)$.

d) $(M(n, \mathbb{R}), +)$, donde $M(n, \mathbb{R})$ es el conjunto de matrices $n \times n$ con coeficientes en $\mathbb{R}$.

e) $(M(n, \mathbb{R}), \times)$.

f) $(GL(n, \mathbb{R}), +)$, donde $GL(n, \mathbb{R})$ es el conjunto de matrices de $M(n, \mathbb{R})$ con determinante no nulo.

g) $(GL(n, \mathbb{R}), \times)$.

h) $(\Sigma^*, \circ)$, donde Σ^* es el conjunto cadenas sobre el alfabeto Σ bajo la operación de concatenación.

i) $(\mathbb{N}, \text{mcd})$.

j) $(\mathbb{N}, \text{mcm})$.

k) $(X \to X, \circ)$, donde $X \to X$ es el conjunto de funciones de X en X bajo la operación de composición de funciones.

l) $(X \Rightarrow X, \circ)$, donde $X \Rightarrow X$ es el conjunto de funciones biyectivas de X en X bajo la operación de composición de funciones.

2. Mostrar que en un grupo el elemento neutro y los inversos sos únicos.

3. Sea G un grupo, entonces para todo $a, b, c \in G$:

a) **Ley de cancelación a izquierda:** $ab = ac \Rightarrow b = c$.

b) **Ley de cancelación a derecha:** $ba = ca \Rightarrow b = c$.

c) $(ab)^{-1} = b^{-1}a^{-1}$.

d) $(a^{-1})^{-1} = a$.

4. Sea G un grupo. Entonces para todo $g \in G$ y $n, m \in \mathbb{Z}$:

a) $g^n g^m = g^{n+m}$.

b) $(g^n)^m = g^{nm}$.

5. Si G es un grupo abeliano entonces para todo $a, b \in G$ y $n \in \mathbb{Z}$ se tiene $(ab)^n = a^n b^n$.

6. Sea $n \in \mathbb{Z}$. Considerar la relación de congruencia módulo n en $\mathbb{Z}$, es decir:

$$a \sim b \Leftrightarrow n \mid (a - b)$$

Sea $\mathbb{Z}_n := \{\overline{x} : x \in \mathbb{Z}\}$ el conjunto de clases de equivalencia. Definimos la operación

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

a) Verificar que la operación está bien definida.

b) Mostrar que $\mathbb{Z}_n$ admite estructura de grupo con dicha operación.

7. Sean G y H grupos, entonces $G \times H$ es un grupo bajo la operación:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

8. Sea M un monoide finito. Probar que si vale la ley de cancelación a derecha, entonces M es en realidad un grupo.

9. Probar:

a) $G \simeq G^{op}$ para todo grupo G.

b) $D_3 \simeq S_3$, donde D_3 es el grupo de simetrías del triángulo equilátero y S_3 es el grupo de permutaciones de 3 elementos.

c) $D_4 \not\simeq S_4$ pero existe un monomorfismo $D_4 \to S_4$, donde D_4 es el grupo de simetrías del cuadrado y S_4 es el grupo de permutaciones de 4 elementos.

d) $len : (\Sigma^*, \circ) \to (\mathbb{N}_0, +)$ es un morfismo de monoides.

e) $exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \times)$ es un isomorfismo de grupos.

10. Sea $\varphi : G \to H$ un morfismo de grupos. Entonces:

a) $\varphi(e_G) = e_H$.

b) $\varphi(g^{-1}) = \varphi(g)^{-1}$ para todo $g \in G$.

11. Probar que para todo monoide $(M, \oplus)$ existe un monomorfismo de monoides $emb : (M, \oplus) \to (M \to M, \circ)$.

12. Sea G un grupo y $H \subseteq G$ un subconjunto. Entonces son equivalentes:

a) H es subgrupo de G.

b) $H \neq \emptyset$ y $h_1^{-1} \in H$ y $h_1 h_2 \in H$ para todo $h_1, h_2 \in H$.

c) H es un grupo y la inclusión $i : H \hookrightarrow G$, $i(h) = h$ es un morfismo de grupos.

13. Probar que todo subgrupo de $\mathbb{Z}$ es de la forma $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ para algún $n \in \mathbb{N}_0$.

14. **Teorema de Cayley.** Probar que todo grupo $(G, \oplus)$ es isomorfo a un subgrupo de $(G \Rightarrow G, \circ)$.

15. Verificar las siguientes afirmaciones sobre grupos cíclicos:

a) Si G es un grupo cíclico, entonces G es abeliano.

b) $\mathbb{Z}$ es cíclico.

c) $\mathbb{Z}_n$ es cíclico.

d) S_n no es cíclico para $n \geq 3$.

e) Si G es un grupo cíclico, entonces $G \simeq \mathbb{Z}$ o $G \simeq \mathbb{Z}_n$.

16. 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. Sabiendo que existe un grupo cíclico finito G con generador g para el cual 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.

17. Sea G un grupo. Definimos

$$\mathcal{L}(G) := \{H \subseteq G : H \text{ es un subgrupo de } G\}.$$

a) Mostrar que $\mathcal{L}(G)$ admite estructura de retículo con las siguientes operaciones:

$$H \vee K = HK.$$
$$H \wedge K = H \cap K.$$

b) Identificar qué retículo determina $\mathcal{L}(\mathbb{Z})$.

Coclase, subgrupo normal y grupo cociente

18. El kernel de un morfismo de grupos $\varphi : G \to H$ se define como el conjunto:

$$\ker(\varphi) = \{g \in G : \varphi(g) = e_H\}.$$

Sin embargo, 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 ambas definiciones al aplicarse al morfismo φ.

19. Sea G un grupo y H un subgrupo G. Se definen las relaciones de congruencia módulo H a izquierda y a derecha como:

$$g_1 \equiv_l g_2 \bmod H \iff g_1 g_2^{-1} \in H.$$
$$g_1 \equiv_r g_2 \bmod H \iff g_1^{-1} g_2 \in H.$$

Probar las siguientes proposiciones:

a) $- \equiv_l - \bmod H$ es una relación de equivalencia en G y para todo $g \in G$ su coclase (clase de equivalencia) a izquierda es $\overline{g}^l = Hg := \{hg : h \in H\}$.

b) $- \equiv_r - \bmod H$ es una relación de equivalencia en G y para todo $g \in G$ su coclase (clase de equivalencia) a derecha es $\overline{g}^r = gH := \{gh : h \in H\}$.

c) Todas las coclases (a izquierda o derecha) tienen la misma cardinalidad. Es decir, tienen la cardinalidad de H.

20. Probar que existen sólo dos grupos distintos de orden 4 (salvo isomorfismo): $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

21. Sea G un grupo y H un subgrupo de G, entonces son equivalentes:

a) $H \triangleleft G$ (H es un subgrupo normal de G).

b) $gHg^{-1} = H$ para todo $g \in G$.

c) $gH = Hg$ para todo $g \in G$.

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

$$\tau_{a,b} : \mathbb{R} \to \mathbb{R},\ \tau_{a,b}(x) = ax + b$$

Probar que

a) $G = \{\tau_{a,b} : a \in \mathbb{R} - \{0\}, b \in \mathbb{R}\}$ es un grupo bajo la operación de composición.

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

c) $N = \{\tau_{1,b} \in G\}$ es un subgrupo normal de G.

23. Sea $\varphi : G \to G'$ un morfismo de grupos. Entonces:

a) $\ker(\varphi) \triangleleft G$.

b) Si G' es abeliano y H es un subgrupo de G tal que $\ker(\varphi) \subseteq H$, entonces $H \triangleleft G$.

24. Si G es un grupo abeliano y H es un subgrupo de G, entonces $H \triangleleft G$.

25. Si G es un grupo y H es un subgrupo de G de índice 2, entonces $H \triangleleft G$.

26. Si $H \triangleleft G$, entonces la operación

$$(g_1H)(g_2H) = (g_1g_2)H$$

define una estructura de grupo en G/H tal que la proyección al cociente $\pi : G \to G/H$ es un epimorfismo de grupos.

27. Considerar el grupo D_4.

a) Calcular el orden de sus elementos.

b) Identificar todos sus subgrupos.

c) Determinar cuáles de los subgrupos son normales.

d) Para cada subgrupo normal $H \triangleleft D_4$, ¿qué grupo determina D_4/H?

Teoremas de isomorfismo

28. Probar los siguientes isomorfismos:

a) $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

b) $\mathbb{Z}_{mn}/\mathbb{Z}_m \simeq \mathbb{Z}_n$.

29. Sean G, H grupos. Si $A \triangleleft G$ y $B \triangleleft H$, entonces $(G \times H)/(A \times B) \simeq (G/A) \times (H/B)$.

30. Sea G un grupo y M, N subgrupos normales de G tales que $G = MN$. Probar que $G/(M \cap N) \simeq G/M \times G/N$.

Grupo Libre

31. Mostrar que:

a) $\langle a \mid a^n = e \rangle \simeq \mathbb{Z}_n$.

b) $\langle a, b \mid a^3 = b^2 = (ab)^2 = e \rangle \simeq D_3$.