Práctica 5: Grupos

Ej. 1. Probar que todo grupo cíclico G es un grupo abeliano.

Ej. 2. Sean $a, b \in G$. Probar que $o(a) = o(a^{-1})$, $o(ab) = o(ba)$ y $o(b^{-1}ab) = o(a)$.

Ej. 3. Sea G un grupo abeliano y sea T el conjunto de los elementos de G de orden finito. Probar que T es un subgrupo de G. Mostrar con un ejemplo que esto es falso si G no es abeliano.

Ej. 4. 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, computar g^{ab}); proponer un protocolo que les permita a Alice y Bob establecer una clave en común y secreta.

Ej. 5. Probar que $\mathbb{Z} \times \mathbb{Z}$ no es un grupo cíclico, pero que puede ser generado por un subconjunto finito.

Ej. 6. Dar un ejemplo (cuando sea posible) de

a) Un conjunto finito que genere un grupo finito.

b) Un conjunto finito que genere un grupo infinito.

c) Un conjunto infinito que genere un grupo finito.

d) Un conjunto infinito que genere un grupo infinito (y no pueda ser generado por un conjunto finito).

Ej. 7. 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:

$$H \vee K = \langle H \cup K \rangle.$$
$$H \wedge K = H \cap K.$$

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

Ej. 8. Sea S_3 el grupo de biyecciones de $\{1, 2, 3\}$ en sí mismo.

a) Sea H el grupo cíclico de S_3 generado por $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Probar que ninguna clase a derecha (excepto el mismo H que es la clase de la identidad) es también una clase a izquierda múdulo H.

b) Probar que existe $a \in S_3$ tal que $aH \cap Ha = \{a\}$.

c) Sea K el grupo cíclico de S_3 generado por $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Probar K es normal en S_3.

d) Probar que S_n no es cíclico para $n \geq 3$.

Ej. 9. Sean K y N subgrupos de G, con N normal en G. Probar que:

a) $N \cap K$ es un subgrupo normal de K.

b) $\langle N \cup K \rangle = NK = KN$, donde $NK = \{nk : n \in N,\, k \in K\}$ y lo mismo para KN.

c) Si K es un subgrupo normal de G y $K \cap N = \{e\}$, entonces $kn = nk$ para cada $k \in K$ y cada $n \in N$.

Ej. 10. Sea H un subgrupo normal de G tales que H y G/H son grupos finitamente generados (es decir, en ambos casos son el grupo generado por una cantidad finita de elementos). Probar que G es finitamente generado.

Ej. 11. El *centro* de un grupo G se define como $Z(G) = \{g \in G : gx = xg\ \forall x \in G\}$. Mostrar que:

a) El centro de $GL(n, \mathbb{R})$ es el grupo de matrices que son múltiplos no nulos de la identidad.

b) El centro de S_n con $n \geq 2$ es $\{1\}$.

c) G es abeliano si y solo si $Z(G) = G$.

d) $Z(G) \triangleleft G$ para todo grupo G.

e) $Z\left(G/Z(G)\right)$ es trivial.

Ej. 12. 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.

d) $G/N \simeq (\mathbb{R} - \{0\}, *)$.

Ej. 13. Sean A, B grupos y consideremos el grupo producto $A \times B$. Sean $\pi_A : A \times B \to A$ y $\pi_B : A \times B \to B$ las proyecciones sobre cada factor. Probar que

a) $A \times \{e_B\} \triangleleft A \times B$ y $\{e_A\} \times B \triangleleft A \times B$

b) π_A y π_B son epimorfismos.

c) $\ker(\pi_A) = \{e_A\} \times B$ y $\ker(\pi_B) = A \times \{e_B\}$.

d) $(A \times B)/(A \times \{e_B\}) \simeq B$

e) Si $N \triangleleft A$ y $M \triangleleft B$ entonces $N \times M \triangleleft A \times B$ y $(A \times B)/(N \times M) \simeq (A/N) \times (B/M)$.

Ej. 14. Probar que si un grupo tiene una cantidad finita de subgrupos, debe ser un grupo finito.

Ej. 15. Probar que si G es un grupo infinito, entonces G tiene al menos un subgrupo propio.

Ej. 16. Probar que existen sólo dos grupos distintos de orden 4 (salvo isomorfismo): $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ej. 17. Hallar todos los subgrupos de $\mathbb{Z}_6$, $\mathbb{Z}_8$ y $\mathbb{Z}_9$.

Ej. 18. Sea G el grupo multiplicativo de matrices no singulares 2×2 a coeficientes racionales. Sean $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Probar que $o(A) = 4$, $o(B) = 3$ pero AB tiene orden infinito.

Ej. 19. Sea G grupo y H subgrupo de G, demostrar que $H \lhd G$ si se cumple al menos una de las siguientes condiciones:

a) G es abeliano.

b) $[G : H] = 2$.

c) $\varphi : G \to G'$ es un morfismo de grupos, G' es abeliano y H es un subgrupo de G tal que $\ker(\varphi) \subseteq H$.

Ej. 20. Sea p un número primo y $a \in \mathbb{Z}$ tal que $p \nmid a$. Probar que:

a) Si $n \equiv r\ (p-1)$, entonces $a^n \equiv a^r\ (p)$.

b) Concluir en particular que $a^n \equiv a^{r_{p-1}(n)}\ (p)$.

Ej. 21. Probar que para todo $a \in \mathbb{Z}$, $7 \mid a^{362} - a^{62}$.

Ej. 22. Resolver los siguientes sistemas en congruencia:

a) $S)$ $\begin{cases} x \equiv 3\,(10) \\ x \equiv 1\,(11) \\ x \equiv 2\,(7) \end{cases}$ **b)** $S)$ $\begin{cases} x \equiv 3\,(22) \\ x \equiv 5\,(8) \\ x \equiv 17\,(20) \end{cases}$ **c)** $S)$ $\begin{cases} 3x \equiv 2\,(7) \\ 7x \equiv 5\,(8) \\ 6x \equiv 8\,(10) \end{cases}$

Ej. 23. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz dijo que eso era imposible. ¿Quién tiene razón?

Ej. 24. Una banda de 13 piratas asaltó un barco mercantil y se hizo con una gran cantidad de monedas de oro, todas idénticas entre sí. Cuando trataron de distribuirlas equitativamente entre ellos, les sobraron 8 monedas. Por lo tanto, decidieron no repartirlas. Imprevistamente, dos de ellos contrajeron sarampión y murieron. Al volver a intentar repartir las monedas, les sobraron 3, y por lo tanto volvieron a cancelar la distribución. Posteriormente murieron otros 3 piratas ahogados. Los restantes volvieron a intentar distribuir las monedas, pero les sobraron 5. Cansados de tanto intentar distribuir sin poder ser equitativos, optaron por guardar las monedas hasta que se les ocurriese una solución. Tiempo después, los piratas se arrepintieron de todas sus fechorías y decidieron hacer un acto caritativo a modo de redención. Se dirijeron a un pueblo muy pobre en el que había exactamente 1136 personas viviendo, y decidieron integrarse al pueblo para iniciar una nueva vida. Más aún, decidieron que repartirían equitativamente todas las monedas entre todos los habitantes del pueblo, incluyéndose a ellos. Pero, para su sorpresa, volvieron a sobrar monedas. ¿Cuántas monedas sobraron?