Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2018**
Instituto de Matemática y Estadística

PRÁCTICO 7: Teoría de Grupos - Teorema de Lagrange, órdenes, homomorfismos.

Recordamos el siguiente Teorema, central en la teoría, y útil en varios ejercicios de este Práctico.

Teorema de Lagrange: *Si G es un grupo finito y H un subgrupo de G entonces $|H|$ divide a $|G|$.*

Ejercicio 1. Dados dos grupos $(G, \times, e_G)$ y $(K, *, e_K)$ se define la siguiente operación en el *producto cartesiano* $G \times K$: $(g, k)(g', k') = (g \times g', k * k')$ para todo $g, g' \in G$ y para todo $k, k' \in K$ (operaciones coordenada a coordenada). Probar que $G \times K$ con esta operación es un grupo.

Ejercicio 2.

a. Sean $G = \mathrm{GL}(2, \mathbb{R})$ el grupo multiplicativo de las matrices invertibles 2×2 con coeficientes en $\mathbb{R}$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Probar que $o(A) = 4$, B orden $o(B) = 3$ y que AB tiene orden infinito.

b. Hallar elementos $a, b \in \mathbb{Z}_2 \times \mathbb{Z}$ de orden infinito tales que $a + b$ tiene orden finito (suma coordenada a coordenada).

Ejercicio 3. Escriba la tabla de multiplicación de $U(18)$. Hallar los órdenes de los elementos de $U(18)$. ¿Es $U(18)$ cíclico?

Ejercicio 4.

a. Sea G un grupo. Probar que si $a^n = e_G \Rightarrow o(a)|n$.

b. Sea G un grupo. Probar que si $a^n \neq e_G \Rightarrow o(a) \nmid n$

c. Sea G un grupo. Probar que $o(xy) = o(yx),\ \forall\, x, y \in G$.

d. Probar que si $a \in U(n) \Rightarrow o(a)|\varphi(n)$.

e.
- **i)** Hallar el resto de dividir 2^{20} entre 253.
- **ii)** Sabiendo además que $2^{55} \equiv -45 \pmod{253}$, hallar el orden de 2 en $U(253)$.

Ejercicio 5. Considere un grupo cíclico finito G de orden n, con generador $g \in G$.

a. Probar que $g^k = g^m$ si y solo si $k \equiv m \pmod{n}$

b. Probar que si $mcd(m, n) = d$ y $n = dn'$, entonces el orden de g^m es n'.

c. Probar que g^k es también un generador de G si y solo si $mcd(k, n) = 1$.

d. Usar la parte anterior para probar que G tiene $\varphi(n)$ generadores, donde φ es la función indicatriz de Euler.

Ejercicio 6. Sean H y K subgrupos de un grupo G y e la unidad de G.

a. Probar que si $|H|$ y $|K|$ son coprimos entonces $H \cap K = \{e\}$.

b. Hallar los posibles valores de $|H|$ si $K \subsetneq H \subsetneq G$, $|G| = 660$ y $|K| = 66$.

Ejercicio 7. Sea $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ una función biyectiva. Probar que el inverso de f es:

$$f^{-1} = \underbrace{f \circ f \circ \ldots \circ f}_{n!-1 \text{ veces}}.$$

Ejercicio 8. Sea G un grupo. Probar las siguientes afirmaciones.

a. Si G es cíclico todo subgrupo de G también es cíclico.

b. Si G no tiene subgrupos no triviales entonces G es cíclico, finito y $|G|$ es primo.

Ejercicio 9. Verificar si las siguientes funciones son o no morfismos de grupo.

a. La función traza $tr : (M_{n\times n}(\mathbb{R}), +) \to (\mathbb{R}, +)$

b. La función $f : (M_{n\times n}(\mathbb{R}), +) \to (\mathbb{R}, +)$ dada por $f(A) = tr(A^2)$.

c. La función determinante $det : (\mathsf{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ (recordar que $\mathsf{GL}_n(\mathbb{R})$ es el conjunto de matrices invertibles $n \times n$ con coeficientes en $\mathbb{R}$).

d. La función $f : (\mathsf{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ dada por $f(A) = det(A^2)$.

e. La función $f : (\mathbb{R}^*, \cdot) \to (\mathsf{GL}_n(\mathbb{R}), \cdot)$ dada por $f(\lambda) = \lambda A$ donde $A \in \mathsf{GL}_n(\mathbb{R})$ es una matriz dada (en caso de no serlo siempre, hallar condiciones sobre A para que f sea morfismo).

f. La función trasponer $T : (M_{n\times n}(\mathbb{R}), +) \to (M_{n\times n}(\mathbb{R}), +)$ dada por $T(A) = A^t$.

g. La función trasponer $T : (\mathsf{GL}_n(\mathbb{R}), \cdot) \to (\mathsf{GL}_n(\mathbb{R}), \cdot)$ dada por $T(A) = A^t$.

h. La función $f : (\mathbb{R}^3, +) \to (\mathbb{R}^*, \cdot)$ dada por $f(x, y, z) = e^{x-2y+z}$ (sug. pensarlo como composición de dos morfismos).

Ejercicio 10. Sea $\varphi : G_1 \to G_2$ un morfismo de grupos finitos.

a. Sea $g \in G_1$, probar que $o(\varphi(g))$ divide a $\mathrm{mcd}(|G_1|, |\mathsf{Im}(\varphi)|)$.

b. Probar que si $|G_1|$ y $|G_2|$ son coprimos, entonces φ es trivial.

c. Si φ es un isomorfismo de grupos y $g \in G_1$. Probar que el orden de g en G_1 es igual al orden de $\varphi(g)$ en G_2.

d. Probar que $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ no son isomorfos.

Ejercicio 11. En cada caso verificar si los siguientes grupos son isomorfos o no; en caso que lo sean, encontrar un isomorfismo entre ellos.

a. Los grupos $(\mathbb{Z}_4, +)$ y $(U_{10}, \cdot)$.

b. Los grupos D_3 y S_3 (ambos con la composición).

Ejercicio 12. Sea G un grupo con 4 elementos.

a. Probar que G es abeliano.

b. Probar que o bien $G \simeq \mathbb{Z}_4$ o bien $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ejercicio 13. (Examen Julio 2012)

a. Probar que si $\phi : G_1 \to G_2$ es un homomorfismo de grupos finitos y $g \in G_1$, entonces $o(\phi(g)) \mid mcd(|G_1|, |G_2|)$.

b. Hallar todos los homomorfismos $\phi : \mathbb{Z}_2 \to U(8)$.

c. Hallar p sabiendo que p es primo, y existe un homomorfismo no trivial $\phi : \mathbb{Z}_{51} \to \mathbb{Z}_p$ tal que $\phi(\overline{17}) = \overline{0}$.

Ejercicio 14. En cada parte, ver si existe un morfismo no trivial (es decir, que no mande todos los elementos al neutro) entre los siguientes pares de grupos $G \to K$. En caso de que existan construir dicho morfismo, y si no existe explicar por qué.

a. $G = S_6$ con la composición y $K = \mathbb{Z}_3$ con la suma.

b. $G = \mathbb{Z}_7$ con la suma y $K = S_6$ con la composición.

c. $G = \mathbb{Z}_8$, $K = U(24)$. Sugerencia: construir la tabla de Cayley de K y hallar el orden de todos sus elementos.

d. $G = U(9)$, $K = \mathbb{Z}_{12}$. Sugerencia: G es cíclico.

e. $G = U(15)$, $K = \mathbb{Z}_6$. Sugerencia: construir la tabla de Cayley de G y hallar el orden de todos sus elementos.