

PRÁCTICO 8: GRUPOS - ÓRDENES, GRUPOS CÍCLICOS Y TEOREMA DE LAGRANGE.

## Órdenes y Grupos cíclicos

### Ejercicio 1.

- Sean  $G = GL(2, \mathbb{R})$  el grupo multiplicativo de las matrices invertibles  $2 \times 2$  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  $o(A) = 4$ ,  $o(B) = 3$ , y que  $AB$  tiene orden infinito.
- Sea  $(G, \cdot)$  un grupo conmutativo. Probar que si  $o(A)$  y  $o(B)$  son finitos, entonces  $o(AB)$  es finito.
- Hallar elementos  $a, b \in \mathbb{Z}_2 \times \mathbb{Z}$  que cumplan:  $o(a) = o(b) = \infty$ ,  $o(a+b)$  finito y mayor a 1. La operación del grupo es la suma coordenada a coordenada.

### Ejercicio 2.

Considere el grupo multiplicativo  $U(18)$ .

- Halle un representante de cada clase de equivalencia de  $U(18)$ .
- Escriba la tabla de Cayley de  $U(18)$ .
- Halle el orden de cada elemento de  $U(18)$ , y determine si  $U(18)$  es **cíclico**.

### Ejercicio 3.

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

### Ejercicio 4.

Sea  $G$  un grupo. Dado  $a \in G$ , probar que se cumple:  $a^n = e_G \Leftrightarrow o(a) | n$ .

### Ejercicio 5.

Sea  $G$  un grupo finito y  $g \in G$  un elemento cualquiera del grupo.

- Probar que se cumple:  $g^k = g^m$  si y solo si  $k \equiv m \pmod{o(g)}$ .
- Probar que  $o(g^m) = \frac{o(g)}{\text{mcd}(m, o(g))}$ . Sugerencia: Sea  $d = \text{mcd}(m, o(g))$ . Sean  $n^*$  y  $m^*$  los cofactores de  $m$  y  $o(g)$ . Es decir:  $\text{mcd}(m^*, n^*) = 1$ ,  $o(g) = dn^*$  y  $m = dm^*$ . Probar que el orden de  $g^m$  es  $n^*$ .
- Supongamos que  $G$  es **cíclico**, de orden  $n$ . Sea  $g$  un **generador** de  $G$ . Probar que  $g^m$  es también un generador de  $G$  si y solo si  $\text{mcd}(m, n) = 1$ .
- Usando la parte anterior, probar que un grupo cíclico  $G$ , de orden  $n$ , tiene  $\varphi(n)$  generadores.

### Ejercicio 6.

Considere los grupos  $\mathbb{Z}_4$ ,  $U(5)$  y  $U(6)$ . Para cada uno de estos grupos:

- Hallar el orden de cada uno de los elementos del grupo.
- Determinar si el grupo es cíclico.
- En caso de que el grupo sea cíclico, calcular todos sus elementos generadores.

### Ejercicio 7.

En cada caso, calcular el **subgrupo generado** por:

- $\bar{2}$  como elemento de  $U(5)$ , y luego como elemento de  $U(7)$ .
- $\bar{1}$  como elemento de  $\mathbb{Z}_6$ , y como elemento de  $\mathbb{Z}_n$ , para  $n \geq 2$ .
- $\bar{2}$  como elemento de  $\mathbb{Z}_5$ , de  $\mathbb{Z}_6$ , y de  $\mathbb{Z}_n$ , para  $n \geq 2$ .

## Teorema de Lagrange

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

**Ejercicio 8.** Sea  $G$  un grupo con neutro  $e$ . Sean  $H$  y  $K$  subgrupos finitos de  $G$ .

- Probar que  $|H \cap K|$  divide a  $\text{mcd}(|H|, |K|)$ .
- Usando lo anterior, probar que si  $|H|$  y  $|K|$  son coprimos, entonces  $H \cap K = \{e\}$ .
- Hallar los posibles valores de  $|H|$  si  $K \subsetneq H \subsetneq G$ ,  $|G| = 660$  y  $|K| = 66$ .

**Ejercicio 9.**

- Probar que si  $a \in U(n) \Rightarrow o(a) | \varphi(n)$ .
- Hallar el resto de dividir  $2^{20}$  entre 253. Sugerencia:  $2^8 = 256$ .
  - Sabiendo además que  $2^{55} \equiv -45 \pmod{253}$ , hallar el orden de  $\bar{2}$  en  $U(253)$ .

**Ejercicio 10.** Sea  $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  una función biyectiva. Probar que el inverso de  $f$  es:

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

## Ejercicios adicionales

**Ejercicio 11.** Sea  $G$  un grupo, con  $G \neq \{e\}$ . Probar las siguientes afirmaciones.

- Si  $G$  es cíclico, todo subgrupo de  $G$  también es cíclico. Sugerencia: sea  $g$  un generador de  $G$ . Dado un subgrupo  $H$ , considere la menor potencia  $m \geq 1$ , tal que  $g^m \in H$ .
- Si los únicos subgrupos de  $G$  son los triviales, entonces  $G$  es cíclico, finito y  $|G|$  es primo.