

SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA II

Nombre	C.I.	No. de prueba
--------------	-----------	---------------------

Duración: 4 horas.

Ejercicio 1.

- A. Sea $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \text{ y } ad - bc = 1 \right\}$. Probar que G con la multiplicación de matrices es un grupo.
- B. Fijamos $n \in \mathbb{N}$ y $K = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} : \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n \text{ y } ad - bc \equiv 1 \pmod{n} \right\}$ con la multiplicación de matrices. Sea $\varphi : G \rightarrow K$ el homomorfismo dado por $\varphi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$.
Hallar $\ker \varphi$, el núcleo de φ . (NOTA: no es necesario probar que K es un grupo ni que φ es un homomorfismo)
- C. Enuncie el Primer Teorema de isomorfismos para grupos.

Ejercicio 2. Sea G un grupo finito y H un subgrupo de G .

- A. Definimos en G la siguiente relación: si $x, y \in G$, $x \sim y \Leftrightarrow xy^{-1} \in H$. Probar que \sim es una relación de equivalencia en G .
- B. Enunciar y probar el Teorema de Lagrange para grupos finitos.
- C. Sea K otro grupo finito y $\varphi : G \rightarrow K$ un homomorfismo. Probar que si $g \in G$ es tal que $\text{mcd}(o(g), |K|) = 1$, entonces $g \in \ker(\varphi)$.

Ejercicio 3.

- A. Sea G un grupo y $g, h \in G$ tales que $gh = hg$ y $\text{mcd}(o(g), o(h)) = 1$.
Probar que $o(gh) = o(g)o(h)$.
- B. Sea $G = U(31)$. Calcular $o(5)$ y $o(29)$ y concluir que 21 es raíz primitiva módulo 31.
- C. Con Fulano fijamos el primo $p = 31$ y $g = 21$ para el intercambio de clave con el método de Diffie-Hellman. Nosotros elegimos $m = 14$ y Fulano nos envía $x = 7$. Calcular la clave común k .

Ejercicio 4. En este ejercicio se puede utilizar que si $\sigma \in S_n$ entonces $\sigma(a_1, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$ (fue probado en el práctico 6). Sea $n \geq 5$ y $a, b, c, d, e \in \{1, 2, 3, \dots, n\}$ cinco números distintos.

- A. (i) Hallar σ_1 y σ_2 en S_n tales que: σ_1 y σ_2 son 3-ciclos, $\sigma_1(a) = b$, $\sigma_2(d) = a$ y $\sigma_2\sigma_1 = (ab)(cd)$.
(ii) Probar que si N es un subgrupo de A_n que contiene a todos los 3-ciclos, entonces $N = A_n$.
- B. Sea N tal que $N \subset A_5$, $N \triangleleft S_5$ y $\sigma = (abc) \in N$. Probar que $N = A_5$.
- C. (i) Hallar $\tau \in S_n$ tal que $(abcde)\tau = (adb)$.
(ii) Hallar $\gamma \in S_n$ tal que $(ab)(cd)\gamma = (abe)$.
- D. Probar que si $\{e\} \neq N \subset A_5$ y $N \triangleleft S_5$, entonces $N = A_5$. (Sugerencia: Probar que necesariamente N contiene un 3-ciclo).