

SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA 2

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

Duración: 4 horas. **Sin** material y **sin** calculadora.

Es necesario mostrar la resolución de los ejercicios y el procedimiento para llegar a la respuesta. Presentar únicamente la respuesta final carece de valor.

Ejercicio 1. (18 puntos) Sea $H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a = \pm 1, b \in \mathbb{Z} \right\}$.

A. Probar que H es un subgrupo *abeliano* de $GL_2(\mathbb{R})$ (las matrices 2×2 invertibles con entradas reales). Aclaración: no es necesario probar que $GL_2(\mathbb{R})$ es un grupo.

B. Hallar el orden de $g = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in H$, discutiendo según a y b .

C. Sean (G_1, \cdot) y $(G_2, *)$ dos grupos con neutros e_1 y e_2 respectivamente. Probar que un homomorfismo $\varphi : G_1 \rightarrow G_2$ es inyectivo si y sólo si $\ker(\varphi) = \{e_1\}$.

D. Sea $\varphi : H \rightarrow \mathbb{Z}_2 \times \mathbb{Z}$ tal que

$$\varphi \left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right) = \begin{cases} (\bar{0}, b) & \text{si } a = 1 \\ (\bar{1}, -b) & \text{si } a = -1 \end{cases}.$$

Probar que φ es un homomorfismo. (La operación en $\mathbb{Z}_2 \times \mathbb{Z}$ es coordenada a coordenada).
¿Es φ un isomorfismo?

Ejercicio 2. (10 puntos)

A. Enunciar el Teorema de órdenes para homomorfismos de grupos.

B. Sea G un grupo con 35 elementos. Dar todos los homomorfismos posibles $\varphi : \mathbb{Z}_{35} \rightarrow G$.

C. Sea G un grupo tal que $|G| = 34$. Probar que si un homomorfismo $\varphi : G \rightarrow \mathbb{Z}_{17}$ no es trivial, entonces su núcleo ($\ker \varphi$) tiene dos elementos.

Ejercicio 3. (15 puntos) Sea $(G, *)$ un grupo y $x, y \in G$ tales que $x * y = y * x$.

Para cada una de las siguientes afirmaciones, decidir si es verdadera o falsa y justificar la respuesta. En caso de ser verdadera dar una prueba, y en caso de ser falsa dar un contraejemplo (decidir si la afirmación es verdadera o falsa sin ninguna justificación carece de valor).

A. Si $o(x)$ y $o(y)$ son finitos, entonces $o(x * y)$ es finito.

B. Si $o(x)$ y $o(y)$ son finitos, entonces $o(x * y) = \text{mcm}(o(x), o(y))$.

C. Si $\text{mcd}(o(x), o(y)) = 1$ entonces $o(x * y) = o(x)o(y)$.

Ejercicio 4. (17 puntos)

A. Probar que en $U(71)$ el orden de $\bar{2}$ es 35.

B. Hallar una raíz primitiva módulo 71.

C. Alicia y Bruno utilizan el método de Diffie-Hellman de intercambio de clave, utilizando el primo $p = 71$ y una raíz primitiva módulo 71. Alicia elige $m = 5$ y Bruno elige $n = 10$. Si Alicia le manda a Bruno $x = 3$, ¿cuál es la clave común?

D. ¿Es posible que con los datos de la parte C. Alicia y Bruno hayan elegido la raíz primitiva obtenida en la parte B?