Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Primer semestre 2024

SEGUNDO PARCIAL - 11 JULIO 2024 - DURACIÓN: 3 HORAS.

Número de parcial	Cédula	Nombre y Apellido

Las respuestas deben estar correctamente argumentadas. Se debe incluir el razonamiento utilizado para obtener cada resultado.

1. (a) Definir subgrupo.

   (b) Enunciar y demostrar el Teorema de Lagrange.

   (c) Sea $H < S_3$, tal que $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ y $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ están en H. Probar que $H = S_3$.

2. (a) Sea $f : G \to K$ un morfismo entre dos grupos finitos.

   i. Enunciar una propiedad que relacione los órdenes del núcleo y de la imagen de f.

   ii. Probar que para todo elemento $g \in G$, se cumple: $o(f(g)) \mid o(g)$.

   (b) Hallar todos los morfismos no triviales entre D_3 y $\mathbb{Z}_2$.
   Recordar: la composición de 2 rotaciones, o de 2 simetrías, es una rotación; mientras que la composición de una simetría y una rotación, es una simetría.

3. (a) Definir raíz primitiva módulo n.

   (b) Probar que si p es un número primo impar y r una raíz primitiva módulo p, entonces $r^a \equiv r^b \pmod{p}$ si y solo si $a \equiv b \pmod{p-1}$.

   (c) i. Probar que 5 es raíz primitiva módulo 43.

   ii. Calcular $\log_5 39 \in \mathbb{Z}_{42}$.

   iii. Determinar si la siguiente congruencia tiene solución $k \in \mathbb{Z}$, y en caso afirmativo hallar una solución: $5^{27k} \equiv 39 \pmod{43}$.