Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Primer semestre 2024**
Instituto de Matemática y Estadística

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 Solución

Ejercicio 1

(a) *Definir subgrupo.*

Dado un grupo $(G, \times, e_G)$, un subconjunto $H \subseteq G$ es un subgrupo de G, si cumple:

(i) (cerrado con la operación): si $h, \tilde{h} \in H$, entonces $h \times \tilde{h} \in H$,

(ii) (neutro): $e_G \in H$.

(iii) (cerrado por inversos): si $h \in H$, entonces $h^{-1} \in H$.

(b) *Enunciar y demostrar el Teorema de Lagrange.*

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

Ver la prueba en las notas del curso: Teorema 3.8.1 (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* $H = S_3$.

Como $H \subseteq S_3$, para probar que $H = S_3$ basta con probar que $|H| = |S_3|$.

Por el Teorema de Lagrange: $|H|$ divide a $|S_3| = 3! = 6$. Es decir: $|H| \in \{1, 2, 3, 6\}$. Queremos probar que $|H| = 6$. Para esto vamos a descartar los otros valores.

Como H es subgrupo de S_3, sabemos que $e_{S_3} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in H$. Por lo tanto, ya tenemos tres elementos distintos en H: σ_1, σ_2 y e_{S_3}. Es decir: $|H| \geq 3$.

Si conseguimos otro elemento $g \in H$, distinto a los tres que ya tenemos, vamos a tener $|H| > 3$; por lo que tendrá que cumplirse $|H| = 6$. Un candidato a este cuarto elemento es

la composición $g = \sigma_1 \circ \sigma_2 \in H$. Esta composisión es:

$$g = \sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Este elemento es distinto a los tres que ya teníamos. Por lo tanto $|H| = 6$.

Una prueba alternativa, que no utiliza Lagrange, consiste en: afirmar que $H \subseteq S_3$ por ser subgrupo; expresar cada elemento de S_3 como composición de elementos de H; y argumentar que todos estos elementos pertenecen a H por ser cerrado por la operación (dado que H es un subgrupo).

Ejercicio 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.*

Los órdenes del núcleo y de la imagen de f cumplen la siguiente relación:

$$|Im(f)||\ker(f)| = |G|. \tag{1}$$

Este resultado es el Teorema de órdenes (Teorema 3.9.8 de las notas del curso).

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

Esta es la Proposición 3.9.3 de las notas del curso. Dado $g \in G$, sabemos que $g^{o(g)} = e_G$; donde $o(g)$ es el orden del elemento g. Aplicando f a ambos lados, y usando propiedades de morfismos, se obtiene:

$$g^{o(g)} = e_G \Rightarrow f\left(g^{o(g)}\right) = f(e_G) \Leftrightarrow (f(g))^{o(g)} = e_K.$$

Esto implica que $o(f(g)) \mid o(g)$. En esta última implicancia utilizamos el siguiente resultado: $h^k = e \Leftrightarrow o(h)|k$. Proposición 3.7.8 (numeral 4) de las notas del curso.

(b) *Hallar todos los morfismos no triviales entre D_3 y $\mathbb{Z}_2$.*

Por la parte (a), (ii), sabemos que cualquier morfismo $f : D_3 \to \mathbb{Z}_2$, debe cumplir:

$$o(f(g)) \mid o(g),\ \forall\ g \in D_3.$$

El grupo diedral D_3 se compone de 6 elementos: 3 simetrías s_i, y 3 rotaciones r_j. El orden de estos elementos es:

$$o(s_i) = 2,\ \forall\ i, \quad o(r_j) = 3,\ \forall\ j.$$

Por otro lado $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, con: $o(\overline{0}) = 1$ y $o(\overline{1}) = 2$. De estos dos valores, el único que divide a $3 = o(r_j)$, es $1 = o(\overline{0})$. Por lo tanto, la única opción para las rotaciones es tomar: $f(r_j) = \overline{0}$. Es decir: todas las rotaciones deben pertenecer al núcleo del morfismo f.

Por otro lado, para cada simetría tenemos dos opciones: $f(s_i) = \overline{0}$, o $f(s_i) = \overline{1}$. Si asignamos todas las simetrías al elemento neutro de $\mathbb{Z}_2$, obtenemos el morfismo trivial. Por lo tanto, alguna de las simetrías debe ser asignada al $\overline{1}$. Esto implica que el morfismo debe ser sobreyectivo: $|Im(f)| = 2 = |\mathbb{Z}_2|$.

Reemplazando estos valores en la relación de la Ecuación (1), se obtiene el orden que debe tener el núcleo:

$$|Im(f)||\ker(f)| = |G| \Leftrightarrow 2|\ker(f)| = 6 \Leftrightarrow |\ker(f)| = 3.$$

Como ya tenemos las 3 rotaciones en el núcleo, esto implica que no podemos asignar más elementos al núcleo. Entonces todas las simetrías deben se asignadas al $\overline{1}$.

Por lo tanto: si existe un morfismo no trivial $f : D_3 \to \mathbb{Z}_2$, este debe ser de la forma:

$$f(r_j) = \overline{0},\ \forall\ j, \quad f(s_i) = \overline{1},\ \forall\ i.$$

Resta ver que esta asignación de valores es un morfismo. Es decir, tenemos que probar que se cumple: $f(g \circ h) = f(g) + f(h)$, para todo $g, h \in D_3$. Tenemos 4 posibles casos. Para comprobar la igualdad en cada caso, conviene recordar que se cumple:

$$r_i \circ r_j = r_k, \quad s_i \circ s_j = r_k, \quad s_i \circ r_j = s_k, \quad r_i \circ s_j = s_k.$$

Usando esto:

- $f(s_i \circ s_j) = f(r_k) = \overline{0} = \overline{1} + \overline{1} = f(s_i) + f(s_j)$
- $f(s_i \circ r_j) = f(s_k) = \overline{1} = \overline{1} + \overline{0} = f(s_i) + f(r_j)$
- $f(r_i \circ s_j) = f(s_k) = \overline{1} = \overline{0} + \overline{1} = f(r_i) + f(s_j)$
- $f(r_i \circ r_j) = f(r_k) = \overline{0} = \overline{0} + \overline{0} = f(r_i) + f(r_j)$

Ejercicio 3

(a) *Definir raíz primitiva módulo n.*

Dado un $n \in \mathbb{Z}^+$, un entero $g \in \{1, \ldots, n\}$ es raíz primitiva módulo n, si $\langle \overline{g} \rangle = U(n)$. Es decir: $\overline{g}$ es un generador del grupo multiplicativo $U(n)$.

(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 $a \equiv b \pmod{p-1}$.*

$$r^a \equiv r^b \pmod{p} \Leftrightarrow r^a r^{-b} \equiv 1 \pmod{p} \Leftrightarrow r^{a-b} \equiv 1 \pmod{p} \Leftrightarrow o(\overline{r}) | (a-b).$$

Como r es una raíz primitiva módulo p, y p es primo, se tiene: $o(\overline{r}) = |U(p)| = \varphi(p) = p-1$. Por lo tanto:

$$r^a \equiv r^b \pmod{p} \Leftrightarrow o(\overline{r}) | (a-b) \Leftrightarrow (p-1) | (a-b) \Leftrightarrow a \equiv b \pmod{p-1}.$$

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

Queremos probar que $\overline{5}$ es un generador de $U(43)$. Esto equivale a probar que $o(5) = |U(43)|$. Como 43 es primo: $|U(43)| = \varphi(43) = 42$.

El Teorema de Lagrange garantiza que $o(5) \mid |U(43)| = 42$. Como $42 = 2 \times 3 \times 7$, esto equivale a decir que: $o(5) \in \{1, 2, 3, 6, 7, 14, 21, 42\} = \mathrm{Div}_+(42)$. Haciendo cuentas:

$$5^1 \equiv 5 \pmod{43},\ 5^2 = 25 \equiv 25 \pmod{43},\ 5^3 = 125 \equiv 39 \pmod{43},$$

$$5^6 = 39 \times 39 \pmod{43} = (-4) \times (-4) \equiv 16 \pmod{43},$$

$$5^7 = 16 \times 5 \equiv 37 \pmod{43},$$

$$5^{14} = 37 \times 37 \pmod{43} = (-6) \times (-6) \equiv 36 \pmod{43},$$

$$5^{21} = 37 \times 36 \pmod{43} = (-6) \times (-7) \equiv 42 \pmod{43}.$$

Como todas estas potencias son no congruentes con 1, se concluye que ninguna es el orden de $\overline{5}$. Por lo tanto, la única opción es: $o(\overline{5}) = 42$.

Otra opción es utilizar la Proposición 4.1.4 (numeral 4) de las notas del curso. Como $42 = 2 \times 3 \times 7$, este resultado garantiza que basta con probar que $\overline{5}^k \neq \overline{1}$, para todo

$$k \in \left\{ \frac{42}{2}, \frac{42}{3}, \frac{42}{7} \right\} = \{21, 14, 6\}.$$

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

Por definición, $k \equiv \log_5 39 \pmod{42}$, si cumple: $5^k \equiv 39 \pmod{43}$. Por lo tanto, para hallar k, podemos ir probando hasta obtener una potencia que cumpla la congruencia:

$$5^1 = 5 \equiv 5 \pmod{43},\ 5^2 = 25 \equiv 25 \pmod{43},\ 5^3 = 125 \equiv 39 \pmod{43}.$$

Por lo tanto: $\log_5 39 \equiv 3 \pmod{42}$.

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

Por la Parte (c,ii), sabemos que $5^3 \equiv 39 \pmod{43}$. Por lo tanto, buscamos $k \in \mathbb{Z}$, tal que: $5^{27k} \equiv 5^3 \pmod{43}$. Por la Parte (b), esto equivale a que se cumpla: $27k \equiv 3 \pmod{42}$. Esta es una ecuación diofántica: $27k - 42y = 3$. Como $\text{mcd}(27, 42) = 3$, que divide a 3, sabemos que la ecuación tiene solución entera. Dividiendo entre 3 de ambos lados de la ecuación, esta equivale a: $9k - 14y = 1$. Es fácil ver que una solución de esta diofántica es: $(k, y) = (-3, -2)$. Por lo tanto: $k \equiv -3 \pmod{14} \equiv 11 \pmod{14}$.