

Introducción al Álgebra (15-1)

Control 5 Pauta Problema 1

$(G, *)$ es grupo con neutro e , no necesariamente abeliano y para $a \in G$ se define $f_a: G \rightarrow G$, $f_a(x) = a * x * a^{-1}$

i) Probar que $f_e = \text{id}_G$ y $\forall a, b \in G$ $f_{a * b} = f_a \circ f_b$

(0.5) En efecto, $\forall x \in G$, $f_e(x) = e * x * e^{-1} = e * x * e = x = \text{id}_G(x)$ pues $e^{-1} = e$
 También $\forall x \in G$, $f_{a * b}(x) = (a * b) * x * (a * b)^{-1} = a * b * x * b^{-1} * a^{-1} =$

(0.5) $= f_a(b * x * b^{-1}) = f_a(f_b(x)) = f_a \circ f_b$. Así $f_{a * b} = f_a \circ f_b$

ii) Probar que $\forall a \in G$, f_a es un isomorfismo de $(G, *)$ en $(G, *)$ y encluye que f_a es invertible en $f_a^{-1} = f_{a^{-1}}$ y que $\{f_a | a \in G\}, 0$ es grupo.

Morfismo: Sean $x, y \in G$ y como $a^{-1} * a = e$ se tiene, asociando,

(10) $f_a(x * y) = a * (x * y) * a^{-1} = (a * x * a^{-1}) * (a * y * a^{-1}) = f_a(x) * f_a(y)$

Biyección: Basta probar que f_a es invertible: Por (i) $f_e = f_{a * a^{-1}} = f_a \circ f_{a^{-1}} = \text{id}_G$

(10) entonces, f_a es invertible y $f_a^{-1} = f_{a^{-1}}$

$\{f_a | a \in G\}, 0$ es un grupo pues: Es cerrado ya que la composición de isom. es isomorfismo, tiene por neutro el isomorfismo $f_e = \text{id}_G$, la ley \circ es la

(20) (para todas las funciones) y cada f_a tiene inverso $f_{a^{-1}}$
 (OBS: La biyección también puede probarse en inyectivo y sobreyectivo)

iii) Si $H(G) = \{a \in G | f_a = \text{id}_G\}$ entonces $(H(G), *)$ es subgrupo de $(G, *)$ y

$$a \in H(G) \Leftrightarrow \forall x \in G, a * x = x * a$$

Subgrupo: Por demostrar que $\forall x, y \in H(G) \Rightarrow (x * y^{-1}) \in H(G)$

En efecto, $x, y \in H(G) \Rightarrow f_x = f_y = \text{id}_G$, pero $f_{x * y^{-1}} = f_x \circ f_{y^{-1}} = f_x \circ f_y^{-1} = \text{id}_G \circ \text{id}_G$

(15) Así $f_{x * y^{-1}} = \text{id}_G \Rightarrow x * y^{-1} \in H(G)$

Por último $a \in H(G) \Leftrightarrow f_a = \text{id}_G \Leftrightarrow \forall x \in G, a * x * a^{-1} = x \Leftrightarrow \forall x \in G, a * x = x * a$

(0.5) donde en la igualdad anterior se operó por $/ * a$.

Pauta Problema 2

Para $p \in \mathbb{N} - \{0\}$, $p\mathbb{Z}$ es el conjunto de los múltiplos enteros de p y en la estructura $(p\mathbb{Z}, +, *)$, $+$ es la suma usual y $*$ está definida por $\forall x, y \in p\mathbb{Z}, x * y = \frac{xy}{p}$

i) Demostrar que $(\mathbb{Z}, +, \cdot)$, el anillo de los enteros, es isomorfo a $(p\mathbb{Z}, +, *)$

Considerar la función $f: (\mathbb{Z}, +, \cdot) \rightarrow (p\mathbb{Z}, +, *)$

$$x \longrightarrow f(x) = px$$

Bijeción: $f(x)$ es biyectiva pues $f^{-1}(x) = \frac{x}{p}$ es tal que $f(f^{-1}(x)) = p \cdot \frac{x}{p} = x$

6.8 es decir $f \circ f^{-1}(x) = x = \text{id}_{\mathbb{Z}}$

(También puede probarse la inyectividad y sobreyectividad)

6.7 Morfismos: Sean $x, y \in \mathbb{Z}$, $f(x+y) = p(x+y) = px + py = f(x) + f(y)$

$$\text{y } f(xy) = p \cdot xy = \frac{px \cdot py}{p} = (px) * (py) = f(x) * f(y)$$

6.0 Sigue que $(\mathbb{Z}, +, \cdot)$ es isomorfo a $(p\mathbb{Z}, +, *)$

ii) $(p\mathbb{Z}, +, *)$ es anillo conmutativo con unidad por ser isomorfo,

6.5 (demostrado en (i)) el anillo de los enteros (con $0_{\mathbb{Z}} = 0$ y $1_{\mathbb{Z}} = 1$)
El cero y la unidad de este anillo son las imágenes por el morfismo del cero y la unidad de \mathbb{Z} . Así $0_{p\mathbb{Z}} = f(0) = p \cdot 0 = 0$ y $1_{p\mathbb{Z}} = f(1) = p \cdot 1 = p$

6.5 $(p\mathbb{Z}, +, *)$ no es cuerpo pues $(\mathbb{Z}, +, \cdot)$ no lo es

iii) $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ y consideremos $(\mathbb{Z}_7 - \{0\}, \cdot)$ $(\mathbb{Z}_7 - \{0\} = \{1, 2, 3, 4, 5, 6\})$

Cual de los conjuntos $A_1 = \{1, 6\}$, $A_2 = \{1, 4, 5\}$, $A_3 = \{1, 3, 5, 6\}$ y $A_4 = \{1, 2, 4\}$ $\text{cardinal}(\mathbb{Z}_7 - \{0\}) = 6$

Con la operación \cdot es grupo abeliano.

6.0 Se sabe que $(\mathbb{Z}_7 - \{0\}, \cdot)$ es grupo abeliano, de modo que los conjuntos anteriores con \cdot serán grupos si son subgrupos de $(\mathbb{Z}_7 - \{0\}, \cdot)$. Por Teorema de Lagrange se descarta A_3 pues $|A_3| = 4$ que no es divisor de 6. A_1 y A_4 lo son, basta ver sus cerrados para \cdot . Por último (A_2, \cdot) no es grupo: $4 \cdot 5 = 6 \notin A_2$