MA1101-5. Introducción al Álgebra. Otoño 2014.
Profesor: José Soto
Auxiliares: Camilo Gómez Araya, Sélim Cornet.
Fecha: 6 de Junio 2014

Trabajo dirigido 5

Grupos, subgrupos, morfismos

P1 (Control 5 - año 2009)

Sea $A = (\mathbb{R}\backslash\{0\}) \times (\mathbb{R}\backslash\{0\})$. Se define sobre A la operación $*$ por $(x, y) * (u, v) = (xu, yv)$.

1. Probar que $(A, *)$ es un grupo abeliano.
2. Sea $a \in \mathbb{R}$ fijo con $a \neq 0$. Se define $H = \{(x, y) \in A, y = x^a\}$. Probar que $(H, *)$ es un subgrupo de $(A, *)$.

Solución

P2

Sea E un conjunto cualquiera, sea $\mathfrak{S}(E) = \{f : E \to E, f \text{ es función biyectiva}\}$.

1. Probar que $(\mathfrak{S}(E), \circ)$ es un grupo.
2. Sea $a \in E$. Sea $H = \{f \in \mathfrak{S}(E), f(a) = a\}$. Probar que $(H, \circ)$ es subgrupo de $(\mathfrak{S}(E), \circ)$.

Solución

P3

Sea $(G, *)$ un grupo.

1. Sea $f : G \to G$ un morfismo. Definimos su núcleo, $\ker(f) = \{x \in G, f(x) = e\}$. Probar que f es inyectiva si y soló si, $\ker(f) = \{e\}$.
2. Sea $a \in G$, sea $\tau_a : G \to G$ definida por $\tau_a(x) = a * x * a^{-1}$. Probar que τ_a es un morfismo de grupos.
3. Demostrar que para todos $a, b \in G, \tau_a \circ \tau_b = \tau_{a*b}$.
4. Probar que τ_a es un isomorfismo, encontrar su aplicación recíproca.

Solución

Grupos finitos, teorema de Lagrange

P4

Sea $(G, *)$ un grupo finito, sea $f : G \to G$ un morfismo. Probar que $|\ker(f)|$ divide a $|G|$.
Solución

Anillos

P6

Probar que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad, encontrar sus elementos invertibles.
Solución

P7 (Control 5, año 2011)

Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Un subconjunto $I \subseteq A$ se dirá *ideal* de A si:

(i). $(I, +)$ es subgrupo de $(A, +)$

(ii). $\forall b \in I, \forall a \in A, b \cdot a \in I$.

1. Verificar que $2\mathbb{Z} = \{2k | k \in \mathbb{Z}\}$ es un ideal del anillo $(\mathbb{Z}, +, \cdot)$.
2. Sea $f : (A, +, \cdot) \to (B, \oplus, \odot)$ un morfismo de anillos. Demostrar que $f^{-1}(\{0_B\})$ es un ideal de A.
3. Sea I un ideal de A. Probar que si $1_A \in I$, entonces $I = A$. Deducir que si I contiene un elemento invertible, entonces $I = A$.

Solución

P8

Sea $(A, +, \cdot)$ un anillo de Boole, es decir tal que $\forall x \in A, x^2 = x \cdot x = x$.

1. Probar que $\forall x, y \in A, xy + yx = 0_A$. Deducir que para todo $x \in A, x + x = 0_A$, y luego que A es conmutativo.
2. Definimos en A la relación $\preccurlyeq$ por $x \preccurlyeq y \Leftrightarrow yx = x$. Probar que $\preccurlyeq$ es una relación de orden en A.

Solución

Pauta

P1 (Control 5 - año 2009)

1. - Probemos primero que $*$ es ley de composición interna sobre A. Sean $(x, y), (u, v) \in A$. Se tiene $(x, y) * (u, v) = (xu, yv)$ con $xu \in \mathbb{R}\backslash\{0\}, yv\backslash\{0\}$ por lo tanto $(x, y) * (u, v) \in A$ y $*$ es ley de composición interna.
   - Probemos que $*$ es asociativa. Sean $(x, y), (u, v), (a, b) \in A$.

$$\begin{aligned}((x, y) * (u, v)) * (a, b) &= (xu, yv) * (a, b) \\ &= (xua, yvb) \\ &= (x, y) * (ua, vb) \\ &= (x, y) * ((u, v) * (a, b))\end{aligned}$$

     Esto demuestra que $*$ es asociativa.
   - Probemos que $*$ es conmutativa. Sean $(x, y), (u, v) \in A$.
     $(x, y) * (u, v) = (xu, yv) = (ux, vy) = (u, v) * (x, y)$, por lo tanto $*$ es conmutativa.
   - Probemos que $*$ tiene neutro. Sea $(x, y) \in A$.
     $(x, y) * (1, 1) = (x \times 1, y \times 1) = (x, y)$ y por conmutatividad, $(1, 1) * (x, y) = (x, y)$. Se concluye que $(1, 1)$ es neutro para $*$.
   - Probemos que todo elemento de A tiene inverso por $*$. Sea $(x, y) \in A$. Como $x \neq 0, y \neq 0$, $\frac{1}{x}$ y $\frac{1}{y}$ están bien definidos. Ahora, $(x, y) * (\frac{1}{x}, \frac{1}{y}) = (1, 1)$, así $(\frac{1}{x}, \frac{1}{y})$ es el inverso de (x, y). Por lo tanto todos los elementos son invertibles.

   Todo esto prueba que $(A, *)$ es un grupo abeliano.

2. - $H \neq \varnothing$ pues $(1, 1) \in A$.
   - Sea $(x, y) \in A$. Así, $y = x^a \neq 0$, por lo tanto $(x, y) \in A$, lo que demuestra que $H \subseteq A$.

- Sean $(x_1, y_1), (x_2, y_2) \in H$. Probemos que $(x_1, y_1) * (x_2, y_2)^{-1} \in H$.

$$\begin{aligned}(x_1, y_1) * (x_2, y_2)^{-1} &= (x_1, x_1^a) * (x_2, x_2^a)^{-1} \\ &= (x_1, x_1^a) * (\frac{1}{x_2}, \frac{1}{x_2^a}) \\ &= (\frac{x_1}{x_2}, (\frac{x_1}{x_2})^a) \in H.\end{aligned}$$

Con esto concluimos que H es subgrupo de A.

Volver al enunciado

P2

1. - Sabemos que la composición de dos funciones biyectivas es biyectiva, por lo tanto $\circ$ es una ley de composición interna.
   - Sabemos que la composición de funciones es asociativa.
   - La ley $\circ$ tiene neutro, Id_E.
   - Sabemos que toda función biyectiva tiene un inverso.

   Se concluye así que $(\mathfrak{S}(E), \circ)$ es un grupo.

2. - $H \neq \varnothing$ pues $Id_E \in \mathfrak{S}(E)$ y $Id_E(a) = a$, por lo tanto $Id_E \in H$.
   - Por definición de H, se tiene $H \subseteq \mathfrak{S}(E)$.
   - Sean $f, g \in H$. Demostremos que $f \circ g^{-1} \in H$. Para eso, basta probar que $f \circ g^{-1}(a) = a$. Sabemos que $g(a) = a \Rightarrow a = g^{-1}(g(a)) = g^{-1}(a)$. Luego, $f \circ g^{-1}(a) = f(a) = a$, y $f \circ g^{-1} \in H$.

   Entonces, H es subgrupo de $\mathfrak{S}(E)$.

Volver al enunciado

P3

1. $\Rightarrow$: supongamos que f sea inyectiva. Ya sabemos que $f(e) = e$ pues f es un morfismo, entonces $\{e\} \subseteq \ker(f)$. Sea $x \in \ker(f)$. Entonces $f(x) = e = f(e)$, luego por inyectividad de f, $x = e$ y $\ker(f) \subseteq \{e\}$. Se concluye que $\ker(f) = \{e\}$.
   $\Leftarrow$: supongamos que $\ker(f) = e$. Sean $x_1, x_2 \in G$ tales que $f(x_1) = f(x_2)$. Entonces:

$$\begin{aligned}& f(x_1) = f(x_2) && \\ \Leftrightarrow\ & f(x_1) * f(x_2)^{-1} = e && \text{multiplicando en ambos lados por } f(x_2)^{-1} \\ \Leftrightarrow\ & f(x_1) * f(x_2^{-1}) = e && \text{pues } f \text{ es morfismo} \\ \Leftrightarrow\ & f(x_1 * x_2^{-1}) = e && \text{pues } f \text{ es morfismo} \\ \Leftrightarrow\ & x_1 * x_2^{-1} \in \ker(f) && \text{por definición del núcleo} \\ \Leftrightarrow\ & x_1 * x_2^{-1} = e && \text{dado que } \ker(f) = \{e\} \\ \Leftrightarrow\ & x_1 = x_2 && \text{multiplicando en ambos lados por } x_2\end{aligned}$$

   Así, $x_1 = x_2$ y f es inyectiva.

2. Sean $x, y \in G$.

$$\begin{aligned}\tau_a(x * y) &= a * x * y * a^{-1} \\ &= a * x * e * y * a^{-1} \\ &= a * x * a^{-1} * a * y * a^{-1} \\ &= \tau_a(x) * \tau_a(y)\end{aligned}$$

   Entonces τ_a es un morfismo.

3. Sean $a, b \in G$. Ya tenemos que $\tau_a \circ \tau_b$ y τ_{a*b} tienen mismo dominio y recorrido. Sea $x \in G$.

$$\begin{aligned} \tau_a \circ \tau_b(x) &= \tau_a(b * x * b^{-1}) \\ &= a * b * x * b^{-1} * a^{-1} \\ &= a * b * x * (a * b)^{-1} \\ &= \tau_{a*b}(x) \end{aligned}$$

   Y por lo tanto, $\tau_a \circ \tau_b = \tau_{a*b}$.

4. Probemos primero que τ_a es biyectiva, mostrando que $\ker(\tau_a) = \{e\}$. Sea $x \in \ker(f)$.

$$\begin{aligned} & \tau_a(x) = e \\ \Leftrightarrow \quad & a * x * a^{-1} = e \\ \Leftrightarrow \quad & x = a^{-1} * a \\ \Leftrightarrow \quad & x = e \end{aligned}$$

   Entonces $\ker(f) = \{e\}$, luego por 1., τ_a es inyectiva.
   Veamos ahora que τ_a es sobreyectiva. Sean $x, y \in G$.

$$\begin{aligned} & y = \tau_a(x) \\ \Leftrightarrow \quad & y = a * x * a^{-1} \\ \Leftrightarrow \quad & a^{-1} * y * a = x \\ \Leftrightarrow \quad & \tau_{a^{-1}}(y) = x \end{aligned}$$

   Entonces τ_a es sobreyectiva, por lo tanto es biyectiva, y su función inversa está dada por $(\tau_a)^{-1} = \tau_{a^{-1}}$.

Volver al enunciado

P4

Probaremos que $\ker(f)$ es un subgrupo de G, para poder aplicar el teorema de Lagrange.

- Dado que $f(e) = e$ pues f es morfismo, $e \in \ker(f)$ y $\ker(f) \neq \varnothing$.
- Se tiene que $\ker(f) \subseteq G$ por definición del núcleo.
- Sean $x, y \in \ker(f)$.

$$\begin{aligned} f(x * y^{-1}) &= f(x) * f(y^{-1}) \\ &= e * f(y)^{-1} \\ &= e^{-1} \\ &= e \end{aligned}$$

  Así, $x * y^{-1} \in \ker(f)$.

Se concluye que $\ker(f)$ es subgrupo de G. Como G es finito, se puede aplicar el teorema de Lagrange, que nos dice que $|\ker(f)|$ divide a $|G|$.
Volver al enunciado

P6

- $(\mathbb{Z}, +)$ es un grupo abeliano, pues $+$ es asociativa y conmutativa, posee un neutro (0) y todo $k \in \mathbb{Z}$ tiene inverso $-k \in \mathbb{Z}$.
- Además, $\cdot$ es asociativa, conmutativa y distribuye con respeto a $+$. Así, $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo. Como 1 es neutro para $\cdot$, $\mathbb{Z}$ tiene unidad.

- Sea $k \in \mathbb{Z}$.

$$\begin{aligned} & k \text{ es invertible} \\ \Leftrightarrow \quad & \exists k' \in \mathbb{Z}, kk' = 1 \\ \Rightarrow \quad & (k = k' = -1) \vee (k = k' = 1) \end{aligned}$$

Reciprocamente, 1 y -1 son invertibles (y sus inversos son respectivamente 1 y -1). Se concluye que los invertibles de $\mathbb{Z}$ son -1 y 1.

Volver al enunciado

P7

1. (i). Veamos que $(2\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$.
   - $2\mathbb{Z} \neq \varnothing$ pues $0 = 2 \times 0 \in 2\mathbb{Z}$.
   - Se tiene $2\mathbb{Z} \subseteq \mathbb{Z}$.
   - Sean $x = 2k, y = 2m \in 2\mathbb{Z}$.
     $x - y = 2k - 2m = 2(k - m) \in 2\mathbb{Z}$.

   Entonces $(2\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$.

   (ii). Sea $x = 2k \in 2\mathbb{Z}$, sea $y \in \mathbb{Z}$. $xy = 2(ky) \in 2\mathbb{Z}$.

   Con esto probamos que $2\mathbb{Z}$ es un ideal de $(\mathbb{Z}, +, \cdot)$.

2. Como f es morfismo de anillos, también es morfismo de grupos de $(A, +)$ sobre $(B, \oplus)$. Por lo tanto, $f^{-1}(0_B)$ es subgrupo de $(A, +)$ (ver P4).
   Ahora, sean $x \in f^{-1}(0_B), y \in A$.
   $f(x \cdot y) = f(x) \odot f(y) = 0_B \odot f(y) = 0_B$. Así, $x \cdot y \in f^{-1}(0_B)$.
   Se concluye que $f^{-1}(0_B)$ es un ideal de A.

3. Sea I ideal de A.
   - Supongamos que $1_A \in I$. Ya sabemos que $I \subseteq A$. Sea $a \in A$.
     Como I es ideal y que $1_A \in I, a = 1_A \cdot a \in I$. Así, $A \subseteq I$ y $I = A$.
   - Supongamos que exista $x \in I, x$ invertible. Entonces $1_A = x \cdot x^{-1} \in I$. Por lo anterior, eso implica $I = A$.

Volver al enunciado

P8

1. Sean $x, y \in A$. Como A es anillo de Boole, se tiene $(x + y)^2 = x + y$.
   Pero por otro lado, $(x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y$ pues $x^2 = x, y^2 = y$. Entonces $x+xy+yx+y = x+y$, lo que implica $xy + yx = 0_A$.
   Luego, tomando $x = y$, se tiene $x^2 + x^2 = 0_A \Leftrightarrow x + x = 0_A$.
   Tenemos entonces: $\forall x, y \in A, xy = -yx$ y $\forall x \in A, x = -x$. Se concluye que $\forall x, y \in A, xy = -yx = -(-yx) = yx$, y A es conmutativo.

2. - Sea $x \in A$. Se tiene $x \cdot x = x^2 = x$, por lo tanto $x \preccurlyeq x$ y $\preccurlyeq$ es refleja.
   - Sean $x, y, z \in A$ tales que $x \preccurlyeq y, y \preccurlyeq z$. Eso significa que $yx = x$ y $zy = y$. Por lo tanto, $zx = z(yx) = (zy)x = yx = x$. Eso significa que $x \preccurlyeq z$ y que $\preccurlyeq$ es transitiva.
   - Sean $x, y \in A$ tales que $x \preccurlyeq y$ e $y \preccurlyeq x$, o sea, $yx = x \wedge xy = y$. Como $\cdot$ es conmutativa, se tiene $x = yx = xy = y$ y $\preccurlyeq$ es antisimétrica.

   Así, $\preccurlyeq$ es una relación de orden.

Volver al enunciado