

MA1101-6 Introducción al Álgebra 2023, Otoño

Profesor: Leonardo Sánchez.

Auxiliar: Patricio Yáñez Alarcón

Correo: pyanez@dim.uchile.cl



Auxiliar 12: Anillos-Cuerpos-Divisores de 0

Resumen

- **[Subgrupo]:** Sea $(G, *)$ grupo y $\emptyset \neq H \subseteq G$. Diremos que H es subgrupo de G si $(H, *)$ es grupo.
- **[Propiedades subgrupos]:**
 1. Si $e \in G$ es el neutro de G y $e_H \in H$ es neutro de H entonces $e = e_H$.
 2. Además, sea $x \in H$. $x^{-1} \in G$ es el inverso de x en $(G, *)$, y $\bar{x}$ es el inverso de x en $(H, *)$. Entonces $x^{-1} = \bar{x}$.
- **[Caracterización Subgrupos]:** Sea $H \neq \emptyset$. Entonces:

$$(H, *) \text{ es subgrupo de } (G, *) \Leftrightarrow \forall x, y \in H, x*y^{-1} \in H$$
- **[Subgrupo imagen]:** Sea $(G, *)$ grupo, (K, Δ) una estructura algebraica y $f : G \rightarrow K$ un morfismo. Si H es subgrupo de $(G, *)$, entonces $f(H)$ es subgrupo de $(f(G), \Delta)$.
- **[Lagrange]:** Si $(H, *)$ es subgrupo del grupo finito $(G, *)$, entonces $|H|$ divide a $|G|$.
- **[Anillo]:** Una e.a. $(A, +, \cdot)$ se llamará anillo si:
 - $(A, +)$ es grupo abeliano.
 - $\cdot$ es asociativa y posee elemento neutro en $A \setminus \{0\}$.
 - $\cdot$ distribuye con respecto a $+$.
 En el caso de ser $\cdot$ conmutativo, $(A, +, \cdot)$ será anillo conmutativo.
- **[Morfismos de anillos]:** $f : A \rightarrow B$ Será morfismo entre dos anillos $(A, +, \cdot)$ y $(B, +, \cdot)$ si:

$$\begin{aligned} f(x + y) &= f(x) + f(y) \\ f(x \cdot y) &= f(x) \cdot f(y) \\ f(1) &= 1 \end{aligned}$$
- **[Álgebra en anillos]:** Si $(A, +, \cdot)$ es anillo y $x, y \in A$:
 - $0 \cdot x = x \cdot 0 = 0$
 - $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$
 - $(-x) \cdot (-y) = x \cdot y$
 - $-x = (-1) \cdot x = x \cdot (-1)$
- **[Divisores de cero y dominio de integridad]:** Sea $(A, +, \cdot)$ un anillo. Un elemento $a \neq 0$ es divisor de 0 si $\exists y \neq 0$ tal que $a \cdot y = 0$ o $y \cdot a = 0$. A un anillo conmutativo y sin divisores de 0 lo llamaremos dominio de integridad.
- **[Propiedad]:** Si $(A, +, \cdot)$ anillo, entonces:

$$a \text{ es cancelable en } (A, \cdot) \Leftrightarrow a \text{ no es divisor de cero}$$
- **[Cuerpo]:** Una estructura $(\mathbb{K}, +, \cdot)$ se llamará cuerpo si:
 - $(\mathbb{K}, +, \cdot)$ es anillo conmutativo.
 - Todo elementos en $\mathbb{K} \setminus \{0\}$ es invertible para $\cdot$.
 Equivalentemente $(\mathbb{K}, +, \cdot)$ será cuerpo si y solo si:
 - $(\mathbb{K}, +)$ es grupo abeliano.
 - $(\mathbb{K} \setminus \{0\}, \cdot)$ es grupo abeliano.
 - $\cdot$ distribuye con respecto a $+$.
- **[Caracterización cuerpos finitos]:** Si $(\mathbb{K}, +, \cdot)$ es cuerpo, entonces $\mathbb{K}$ no tiene divisores de 0 ($\mathbb{K}$ es dominio de integridad). El recíproco se tiene si $|\mathbb{K}|$ es finito, es decir: Si $(\mathbb{K}, +, \cdot)$ es dominio de integridad con $|\mathbb{K}|$ finito, entonces $(\mathbb{K}, +, \cdot)$ es cuerpo.

“Mañana se triunfa equipo”

Pato

P1. Sean $(A, *_A)$, $(B, *_B)$ grupos y $f : A \rightarrow B$ morfismo.

- Demuestre que si $(C, *_A)$ es subgrupo entonces $(f(C), *_B)$ también lo es.
- Demuestre que si $(D, *_B)$ es subgrupo entonces $(f^{-1}(D), *_A)$ también lo es.

P2. $(G, *)$ un grupo abeliano y $H, K \subseteq G$ dos subgrupos de G . Probar que el conjunto

$$H * K = \{h * k \mid h \in H, k \in K\}$$

es subgrupo de $(G, *)$.

P3. Sea $X = \{f : \mathbb{R} \rightarrow \mathbb{R} : f(x) = \frac{ax+b}{cx+d}, \text{ con } a, b, c, d \in \mathbb{R}, \text{ y } ab - cd = 1\}$. Demuestre que $(X, \circ)$ es subgrupo de $(\mathbb{R}^{\mathbb{R}}, \circ)$.

P4. Sea $(A, +, \cdot)$ un anillo conmutativo.

- Si $a \in A$ es un divisor del 0 y $b \in A$, tal que $a \cdot b \neq 0$, entonces $a \cdot b$ es divisor del 0.
- Demuestre que si el producto de dos elementos es divisor del 0, entonces al menos uno de ellos es divisor del 0.

P5. Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Se define $G \subseteq A$ por

$$G = \{a \in A \mid a \text{ tiene inverso para } \cdot\}$$

- Mostrar que $(G, \cdot)$ es un grupo abeliano.
- Sea $H = \{a^2 \mid a \in G\}$. Pruebe que H es subgrupo de G .
- Si $A = \mathbb{Z}_8$, encuentre G y H .

P6. Subgrupos y Lagrange

Sea $(G, *)$ un grupo abeliano, y sean P y Q dos subgrupos de G . Se define

$$P * Q = \{z \in G \mid \exists (p, q) \in P \times Q \text{ tal que } z = p * q\}$$

- Pruebe que $P \subseteq P * Q$ y $Q \subseteq P * Q$.
- Pruebe que $P * Q$ es subgrupo de G .
- Suponga que $|G| = 36$, $|P| = 12$ y $|Q| = 18$. Concluya que $P * Q = G$

P7. Anillos

Sea $(K, +, \cdot)$ un cuerpo y $(A, \oplus, \odot)$ un anillo. Sea $f : K \rightarrow A$ morfismo entre $(K, +, \cdot)$ y $(A, \oplus, \odot)$ con $1_A \neq 0_A$. Demuestre que:

- $f(0_K) = 0_A$
 - $\forall x \in K, f(-x) = -f(x)$
 - $(f(K), \oplus)$ es un subgrupo de $(A, \oplus)$
- $f(x) = 0_A \Leftrightarrow x = 0_K$
- f inyectiva.

Resumen

- **[Homomorfismos]**: Una función $f : A \rightarrow B$ es un **morfismo** entre las estructuras algebraicas $(A, *)$ y (B, Δ) si:

$$\forall x, y \in A, f(x * y) = f(x) \Delta f(y)$$

Si f es biyectiva se dirá **isomorfismo**.

- **[Props epimorfismos]**: Si $f : A \rightarrow B$ epimorfismo entre $(A, *)$ y (B, Δ) , entonces se tienen las siguientes propiedades:

- Si $(A, *)$ es asociativa, entonces (B, Δ) también lo es.
- Si $(A, *)$ es conmutativa, entonces (B, Δ) también lo es.
- Si e es neutro para $(A, *)$, entonces $f(e)$ lo es para (B, Δ) .
- Si a tiene inverso b para $(A, *)$, entonces $f(a)$ tiene inverso $f(b)$ para (B, Δ) .

- **[Props. más generales]**: Sea f un morfismo de $(A, *)$ a (B, Δ) , con neutros e_A y e_B :

- Si $e_B \in f(A)$, entonces $e_B = f(e_A)$.
- Si $e_B \in f(A)$ y $a \in A$ tiene inverso b , entonces $f(a)$ tiene inverso $f(b)$.

- **[Composición]**: Si $f : A \rightarrow B$ un homeomorfismo de $(A, *)$ en (B, Δ) y $g : B \rightarrow C$ un homomorfismo de (B, Δ) en $(C, \bullet)$, entonces la composición de f con g , $g \circ f : A \rightarrow C$, es un morfismo de $(A, *)$ en $(C, \bullet)$.

- **[Estructuras isomorfas]**: Dos estructuras $(A, *)$ y (B, Δ) son isomorfas, denotado $(A, *) \cong (B, \Delta)$, si existe una función $f : A \rightarrow B$ isomorfismo.

Obs.: $\cong$ es una relación de equivalencia.

- **[Isomorfismo inverso]**: Si $f : A \rightarrow B$ es un isomorfismo entre $(A, *)$ y (B, Δ) , entonces $f^{-1} : B \rightarrow A$ es un isomorfismo entre (B, Δ) y $(A, *)$.

- **[Estructura de funciones]**: Sea $(B, *)$ una e.a., entonces $(B^A, *)$ será una e.a., donde si $f, g \in B^A$ definimos $f * g : A \rightarrow B$ por:

$$(f * g)(x) = f(x) * g(x)$$

- **[Propiedades varias]**:

- Si $(B, *)$ es asociativa, entonces $(B^A, *)$ también.
- Si $(B, *)$ es conmutativa, entonces $(B^A, *)$ también.

- Si $(B, *)$ tiene neutro e , entonces $f \in (B^A, *)$ dado por $f(x) = e$ (función constante) es neutro de $(B^A, *)$

- **[Estructura de pares ordenados]**: Sean $(A_1, *_1)$ y $(A_2, *_2)$ e.a., se define la l.c.i. $\otimes$ sobre $A_1 \times A_2$ por: Para $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$:

$$(a_1, a_2) \otimes (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$$

- **[Propiedades varias]**:

- Si $(A_1, *_1), (A_2, *_2)$ son asociativas, entonces $(A_1 \times A_2, \otimes)$ también.
- Si $(A_1, *_1), (A_2, *_2)$ son conmutativas, entonces $(A_1 \times A_2, \otimes)$ también.
- Si $(A_1, *_1), (A_2, *_2)$ poseen neutros e_1 y e_2 , entonces $(A_1 \times A_2, \otimes)$ posee neutro (e_1, e_2)
- Si a_1, a_2 poseen inversos b_1, b_2 en $(A_1, *_1), (A_2, *_2)$, entonces (a_1, a_2) posee inverso (b_1, b_2) en $(A_1 \times A_2, \otimes)$.

- **[Grupo]**: Sea $(G, *)$ una e.a., diremos que:

- Es **grupo** si $*$ es asociativa, tiene neutro y todo elemento posee inverso.
- Es **grupo abeliano** si es grupo y $*$ es conmutativa.

- **[Propiedades grupos]**: Sea $(G, *)$ grupo, entonces:

- $\forall a, b \in G, a * x_1 = b \Leftrightarrow x_1 = a^{-1} * b$
 $\forall a, b \in G, x_2 * a = b \Leftrightarrow x_2 = b * a^{-1}$
 Es decir, las ecuaciones tienen una única solución.
- $\forall a \in G$ las funciones $I_a(x) = a * x$ y $D_a(x) = x * a$ son biyectivas.
- El único elemento idempotente es el neutro.
- Si (K, Δ) una e.a. y $f : G \rightarrow K$ morfismo, entonces $(f(G), \Delta)$ es grupo.
- Si (K, Δ) una e.a., un morfismo $f : G \rightarrow K$ es monomorfismo (inyectivo) si y solo si $f^{-1}(\{e_K\}) = \{e_G\}$

- **[Grupos importantes]**:

- Si $(G, *)$ es grupo (abeliano) y $A \neq \emptyset$, entonces $(G^A, *)$ es grupo (abeliano)
- Si $(G_1, *_1), (G_2, *_2)$ son grupos (abelianos), entonces $(G_1 \times G_2, \otimes)$ es grupo (abeliano).