

# MA1101-6 Introducción al Álgebra 2020, Otoño

Profesora: Paulina Cecchi B.

Auxiliar: Patricio Yáñez Alarcón

Correo: pyanez@dim.uchile.cl



## 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,  $(K, \Delta)$  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 llamara 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]:**  $f: A \rightarrow B$  Sera morfismo entre dos anillos  $(A, +, \cdot)$  y  $(B, +, \cdot)$  si:

$$\begin{aligned} f(x + y) &= f(x) + f(y) \\ f(x \cdot y) &= f(x) \cdot f(y) \\ f(1) &= 1 \end{aligned} \quad (A, +, \cdot) \rightarrow (B, +, \cdot)$$

▪ **[Algebra 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:

$a$  es cancelable en  $(A, \cdot) \Leftrightarrow a$  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  $(\mathbb{K}, +, \cdot)$  sera 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 reciproco 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.

## Resumen

▪ **[Homomorfismos]:** Una función  $f: A \rightarrow B$  es un morfismo entre las estructuras algebraicas  $(A, *)$  y  $(B, \Delta)$  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  $(B, \Delta)$ , entonces se tienen las siguientes propiedades:

- I) Si  $(A, *)$  es asociativa, entonces  $(B, \Delta)$  tambien lo es.
- II) Si  $(A, *)$  es conmutativa, entonces  $(B, \Delta)$  tambien lo es.
- III) Si  $e$  es neutro para  $(A, *)$ , entonces  $f(e)$  lo es para  $(B, \Delta)$ .
- IV) Si  $a$  tiene inverso  $b$  para  $(A, *)$ , entonces  $f(a)$  tiene inverso  $f(b)$  para  $(B, \Delta)$ .

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

- I) Si  $e_B \in f(A)$ , entonces  $e_B = f(e_A)$ .
- II) 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  $(B, \Delta)$  y  $g: B \rightarrow C$  un homeomorfismo de  $(B, \Delta)$  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  $(B, \Delta)$  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  $(B, \Delta)$ , entonces  $f^{-1}: B \rightarrow A$  es un isomorfismo entre  $(B, \Delta)$  y  $(A, *)$ .

▪ **[Estructura de funciones]:** Sea  $(B, *)$  una e.a., entonces  $(B^A, *)$  sera 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]:**

- I) Si  $(B, *)$  es asociativa, entonces  $(B^A, *)$  tambien.
- II) Si  $(B, *)$  es conmutativa, entonces  $(B^A, *)$  tambien.

III) 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]:**

- I) Si  $(A_1, *_1), (A_2, *_2)$  son asociativas, entonces  $(A_1 \times A_2, \otimes)$  tambien.
- II) Si  $(A_1, *_1), (A_2, *_2)$  son conmutativas, entonces  $(A_1 \times A_2, \otimes)$  tambien.
- III) Si  $(A_1, *_1), (A_2, *_2)$  poseen neutros  $e_1$  y  $e_2$ , entonces  $(A_1 \times A_2, \otimes)$  posee neutro  $(e_1, e_2)$
- IV) 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:

- I)  $\forall a, b \in G, a * x_1 = b \Leftrightarrow x_1 = a^{-1} * b$   
 $\forall a, b \in G, x_2 * a = b \Leftrightarrow x_2 = b * a^{-1}$   
Es decir, las ecuaciones tienen una única solución.
- II)  $\forall a \in G$  las funciones  $I_a(x) = a * x$  y  $D_a(x) = x * a$  son biyectivas.
- III) El unico elemento idempotente es el neutro.
- IV) Si  $(K, \Delta)$  una e.a. y  $f: G \rightarrow K$  morfismo, entonces  $(f(G), \Delta)$  es grupo.
- V) Si  $(K, \Delta)$  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).

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

- 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.

$$f^{-1} = g$$

$$f: A \rightarrow B$$

$$g: f(A) \rightarrow A$$

$x *_B y^{-1} \in f(C)$  yo quiero  
 Sea spg  $x, y \in f(C)$   
 si  $x \in f(C)$ ,  $\exists a \in C$ , tq  $x = f(a)$   
 si  $y \in f(C)$ ,  $\exists b \in C$ , tq  $y = f(b)$

arbitrario.

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

↓ morfismo

$\in f(C)$

Por enunciado  $(A, *_A)$   
 grupo  
 $\Rightarrow *_A$  cerrado  
 (= l.c.i.)

$$\Rightarrow x *_B y^{-1} \in f(C)$$

■ [Subgrupo]: Sea  $(G, *)$  grupo y  $\emptyset \neq H \subseteq G$ . Diremos que  $H$  es subgrupo de  $G$  si  $(H, *)$  es grupo.

■ [Propiedades subgrupos]:

- Si  $e \in G$  es el neutro de  $G$  y  $e_H \in H$  es neutro de  $H$  entonces  $e = e_H$ .
- 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:

$$(H, *) \text{ es subgrupo de } (G, *) \Leftrightarrow \forall x, y \in H, x *_B y^{-1} \in H$$

$$\begin{aligned} & \Leftrightarrow b *_A b^{-1} = e_A / f \\ & \Leftrightarrow f(b *_A b^{-1}) = f(e_A) \\ & \Leftrightarrow f(b) *_B f(b^{-1}) = e_B / f(b) \text{ (por la izq)} \\ & \Leftrightarrow f(b) *_B f(b) *_B f(b^{-1}) = f(b) \\ & \Leftrightarrow e_B *_B f(b^{-1}) = f(b) \\ & \Leftrightarrow f(b^{-1}) = f^{-1}(b) \end{aligned}$$

→ conmutativo

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

↳ Asoc, In, Inversos

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

es subgrupo de  $(G, *)$ .

→ arbitrarios

Sea  $x, y \in H * K$ ,  $x \in H * K$ ,  $x = h_1 * k_1$ ,  $h_1 \in H, k_1 \in K$

P.D.Q.  $x * y^{-1} \in H * K$   $y \in H * K$ ,  $y = h_2 * k_2$ ,  $h_2 \in H, k_2 \in K$

tomando  $x * y^{-1} = (h_1 * k_1) * (h_2 * k_2)^{-1}$

$$= (h_1 * k_1) * (k_2^{-1} * h_2^{-1})$$

de antemano  $K, H$  son subgrupos

$$= (h_1 * k_1) * (h_2^{-1} * k_2^{-1})$$

$$= (k_1 * h_1) * (h_2^{-1} * k_2^{-1})$$

$$= k_1 * (h_1 * h_2^{-1}) * k_2^{-1}$$

$\in H$

$$= (k_1 * (h_1 * h_2^{-1})) * k_2^{-1}$$

$$= ((h_1 * h_2^{-1}) * k_1) * k_2^{-1}$$

$$= (h_1 * h_2^{-1}) * (k_1 * k_2^{-1}) \in H * K$$

$$\in H * K$$

$$\hat{h} = h_1 * h_2^{-1} \in H$$

$$\hat{k} = k_1 * k_2^{-1} \in K$$

$$= \hat{k} * \hat{h} \in H * K$$

$$(k_2^{-1}) * h_2^{-1}$$

$\cap$

$\cap$

$K$

$H$

$$H, K \subseteq G$$

Cumple conmutatividad

para  $*$

$$k_2 \in K \Rightarrow k_2 \in G$$

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

- (a) 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. ACAB
- (b) Demuestre que si el producto de dos elementos es divisor del 0, entonces al menos uno de ellos es divisor del 0.

■ [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.

1) Si:  $a \neq 0$  es  $\text{div } 0$ , si  $\exists x \neq 0, x \in A$  ACAB  
 $\boxed{a \cdot x = 0} = x \cdot a$

2)  $\exists b \in A, a \cdot b = 0$

a) PDQ  $a \cdot b$  es  $\text{div } 0$

$a \cdot b \neq 0, \exists l \in A, l \neq 0$  t.q.  $(a \cdot b) \cdot l = 0$  es suficiente  $(a \cdot b) \cdot l$  y  $a \cdot (b \cdot l)$  pues  $(A, +, \cdot)$  Anillo conmutativo

Basta encontrar  $l$  que cumpla lo pedido

por hipótesis  $\exists x \in A, \text{t.q. } x \neq 0$  porque  $a$  es  $\text{div } 0$

$$a \cdot x = 0 \quad / \cdot b, b \neq 0$$

$$\Leftrightarrow b \cdot (a \cdot x) = b \cdot 0$$

$$\Leftrightarrow b \cdot (a \cdot x) = 0 \quad \downarrow \text{Asoc } (A, +, \cdot)$$

$$\Leftrightarrow (b \cdot a) \cdot x = 0 \quad \downarrow \text{Comm } (A, +, \cdot)$$

$$\Leftrightarrow (a \cdot b) \cdot x = 0$$

Como  $x \neq 0, (a \cdot b) \neq 0$  sea  $x = l$  luego  $(a \cdot b)$  será  $\text{div } 0$

b)  $(a \cdot b \text{ es } \text{div } 0) \Rightarrow a \text{ div } 0 \vee b \text{ div } 0$

$a \cdot b \text{ es } \text{div } 0 \Leftrightarrow a \cdot b \neq 0, \exists x \in A, x \neq 0 \text{ t.q. } (a \cdot b) \cdot x = 0$  (Estoy en  $(A, +, \cdot)$  anillo conmutativo)

$(a \cdot b) \cdot x = 0$ , si  $x$  fuera  $\text{div } 0, x \neq 0$ ,  $x \cdot l = 0$   $l \neq 0$

i) si  $a$  es  $\text{div } 0$ .

ii) sup que  $a$  no es  $\text{div } 0$ .

$$\Rightarrow a = 0 \Rightarrow a \cdot b = 0 \quad \times$$



luego  $b \cdot x = 0$

$\Rightarrow b \text{ div } 0$ , porque por hipótesis  $x \neq 0$

is  $b \text{ div } 0$

ii)  $b$  no sea  $\text{div } 0 \Rightarrow b = 0 \Rightarrow a \cdot b = 0 \quad \times$

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

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

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

i)  $G$  grupo abeliano

- Asocia porque  $(A, +, \cdot)$  Anillo  $\Rightarrow (A, \cdot)$  Asocia  $\Rightarrow (G, \cdot)$  Asocia
  - Neutro, si: pues  $(A, +, \cdot)$  Anillo conmutativo con unidad
  - Inverso, por definición de  $G$
  - Conmutativa, Anillo conmutativo para  $\cdot$
- $\Rightarrow (G, \cdot)$  grupo abeliano

ii)  $H = \{a^2 \mid a \in G\}$ , sabemos  $H \subseteq G$

$H$  subgrupo  $\Leftrightarrow x, y \in H, x \cdot y^{-1} \in H$ , con  $x = a^2$  y  $y = b^2, a, b \in G$

$$\begin{aligned} x \cdot y^{-1} &= a^2 (b^2)^{-1} = a^2 \cdot (b^{-1})^2 \rightarrow b^2 (b^{-1} \cdot b^{-1}) = 1 \\ &= (a \cdot a) (b^{-1} \cdot b^{-1}) \\ &= (a b^{-1})^2, \text{ pues } (G, \cdot) \text{ es abeliano, pues } a \cdot b^{-1} \in G \end{aligned}$$

pues  $b^{-1} \in G$  si  $b \in G$

luego  $G$  subgrupo de  $(A, \cdot)$

iii)  $\mathbb{Z}_8 = \{[a] : 0 \leq a < 8, a \in \mathbb{N}\}$   
+ tabla!

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------|---|---|---|---|---|---|---|---|
| 0       | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1       | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2       | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3       | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4       | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5       | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6       | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7       | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

$$\Rightarrow G = \{1, 3, 5, 7\}$$

$$G^{-1} = \{a^{-1} \mid a \in G\}$$

$$H = \{1\}$$