



# INSTITUTO POLITÉCNICO NACIONAL

## ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICA

ÁLGEBRA MODERNA I

---

### Apuntes Álgebra Moderna I

---

Profesor:

Escobar Gracia Cé-  
sar Alberto

Alumnos:

Ramírez León Christian Yael  
Silva Sierra Joshua Joaquín

5FM1

---

---

24 de diciembre de 2025



# Índice general



# CAPÍTULO 1

## Conceptos Previos

---

### 1.1. Divisibilidad

**Definición 1.1.1** (Divisibilidad). *Sean  $a, b \in \mathbb{Z}$ , con  $a \neq 0$ , se dice que  $a|b$  si  $\exists k \in \mathbb{Z}$  tal que  $b = ak$ .*

**Definición 1.1.2** (Máximo Común Divisor). *Sea  $a, b \in \mathbb{Z}$ , al menos uno distinto de cero, definimos a  $d \in \mathbb{Z}$  un máximo común divisor de  $a$  y  $b$ , denotado por  $(a, b)$ , si cumple:*

- I)  $d > 0$ .
- II)  $d|a$  y  $d|b$ .
- III) Si  $c|a$  y  $c|b$ , entonces  $c|d$ .

**Proposición 1.1.1** (Propiedades de la Divisibilidad). *Sean  $a, b, c \in \mathbb{Z}$ , con  $a, b \neq 0$ , entonces:*

- I) Si  $a|b$  y  $b|c$ , entonces  $a|c$ .
- II) Si  $a|b$  y  $a|c$ , entonces  $a|(b + c)$ .
- III) Si  $a|b$ , entonces  $a|bk$  para todo  $k \in \mathbb{Z}$ .
- IV) Si  $a|b$  y  $b \neq 0$ , entonces  $|a| \leq |b|$ .
- V) Si  $a|b$  y  $b|a$ , entonces  $a = \pm b$ .
- VI) Si  $a|b$ , entonces  $(a, b) = |a|$ .
- VII) Si  $c|a$  y  $c|b$ , entonces  $c = ax + by$  para algunos  $x, y \in \mathbb{Z}$ .

**Proposición 1.1.2.** *Sea  $a, b \in \mathbb{Z}$ , al menos uno distinto de cero, entonces existe un único máximo común divisor de  $a$  y  $b$ .*

**Teorema 1.1.1** (Algoritmo de la división). *Sean  $a, b \in \mathbb{Z}$ , con  $b > 0$ , entonces existen únicos  $q, r \in \mathbb{Z}$  tales que:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

## 1.2. Cardinalidad de conjuntos

Dado un conjunto  $A$ , se denotará su cardinalidad (número de elementos) como  $|A|$ . Si  $A$  es un conjunto finito, entonces  $|A|$  es un número natural. Si  $A$  es infinito, entonces  $|A| = \infty$ .

**Observación 1.1.** *Sean  $A, B$ , conjuntos finitos, con  $B \subseteq A$ . Entonces:*

$$|A \setminus B| = |A| - |B|$$

En efecto, basta notar que  $B \cup (A \setminus B) = A$  y que  $B \cap (A \setminus B) = \emptyset$ , luego  $|A| = |B \cup (A \setminus B)| = |B| + |A \setminus B|$ , así  $|A \setminus B| = |A| - |B|$ .  $\square$

**Observación 1.2.** *Sean  $A$  y  $B$  dos conjuntos finitos, entonces:*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

En efecto, Sean  $A$  y  $B$  conjuntos finitos, note que:

$$A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup (A \cap B)$$

Además:  $(A \setminus (A \cap B)), (B \setminus (A \cap B)), (A \cap B)$ , son disjuntos, más aún:

$$|A \setminus (A \cap B)| = |A| - |A \cap B|$$

$$|B \setminus (A \cap B)| = |B| - |A \cap B|$$

Así:

$$\begin{aligned} |A \cup B| &= |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B| \\ &= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

$\square$

**Proposición 1.2.1** (Principio de inclusión exclusión). *Sean  $A_1, \dots, A_n$  conjuntos finitos, se tiene:*

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

**Observación 1.3.** Suponga que  $C_1$  es la condición que cumplen los elementos  $A$  y  $C_2$  los de  $B$ , i.e.:

$$A = \{x \in \Omega : x \text{ cumple } C_1\}$$

$$B = \{x \in \Omega : x \text{ cumple } C_2\}$$

Denotemos  $N(C_i)$  a la cantidad de elementos que cumplen  $C_i$ ,  $N(C_1, C_2)$  a los que cumplen ambas,  $N(\bar{C}_i)$  a los que no cumplen y  $N(\bar{C}_1, \bar{C}_2)$  los que no cumplen  $C_1$  ni  $C_2$ , entonces:

$$N(\bar{C}_1, \bar{C}_2) = |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2))$$

En efecto, Note que:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |A^c \cap B^c| = |(A \cup B)^c| = |\Omega \setminus (A \cup B)| = |\Omega| - |A \cup B| \\ &= |\Omega| - (|A| + |B| - |A \cap B|) \\ &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \end{aligned}$$

□

**Ejemplo 1.1.** Sea  $\Omega = \{x \in \mathbb{Z} : 1 \leq x \leq 1000\}$  ¿Cuántos enteros de estos no son divisibles por 3 o 5?

Sol. Consideremos:

$$C_1 : x \text{ sea divisible por 3}$$

$$C_2 : x \text{ sea divisible por 5}$$

Así  $N(C_1) = 333$ ,  $N(C_2) = 200$ ,  $N(C_1, C_2) = 66$ .

Luego:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \\ &= 1000 - (333 + 200 - 66) \\ &= 533 \end{aligned}$$

Sea  $A_1, \dots, A_n$  una colección finita de conjuntos finitos, definidos:

$$A_i = \{x \in \Omega : x \text{ cumpla } C_i\}, \quad C_i \text{ condición.}$$

Definamos de este modo:

$$S_1 = N(C_1) + \dots + N(C_n)$$

$$S_2 = N(C_1, C_2) + \dots + N(C_1, C_n) + N(C_2, C_3) + \dots + N(C_{n-1}, C_n)$$

⋮

$$S_i = \sum_{1 \leq j_1 < \dots < j_i \leq n} N(C_{j_1}, \dots, C_{j_i})$$

⋮

$$S_n = N(C_1, \dots, C_n)$$

Por el principio de inclusión exclusión generalizado:

$$N(\bar{C}_1, \dots, \bar{C}_n) = |\Omega| - (S_1 - S_2 + \dots + (-1)^{n-1} S_n)$$

### 1.3. Enteros Módulo $n$

**Definición 1.3.1.** Sea  $n \in \mathbb{Z}$ ,  $n > 1$ , se define la relación de  $a \sim b$  si y sólo si  $n \mid (a - b)$ , es decir,  $a$  es congruente con  $b$  módulo  $n$ .

Es fácil ver que esta es una relación de equivalencia en  $\mathbb{Z}$ . Ahora, definamos en el conjunto cociente  $(\mathbb{Z}/\sim)$  las siguientes operaciones:

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a} \cdot \bar{b} &= \overline{a \cdot b}\end{aligned}$$

Con  $a, b \in \mathbb{Z}$ . Entonces las operaciones están bien definidas, i.e., no dependen del representante de clase.

En efecto, sea  $\bar{a} = \bar{a}_1$ ,  $\bar{b} = \bar{b}_1 \iff a \sim a_1$  y  $b \sim b_1 \iff n \mid (a - a_1) \wedge n \mid (b - b_1)$ .

Esto implica:

$$n \mid (a - a_1) + (b - b_1) = (a + b) - (a_1 + b_1) \iff (a + b) \sim (a_1 + b_1) \iff \overline{a + b} = \overline{a_1 + b_1}$$

Análogamente para el producto.

□

Al conjunto de clases de equivalencia módulo  $n$  junto con las operaciones definidas se les denotará por  $\mathbb{Z}/n\mathbb{Z}$  o  $\mathbb{Z}_n$ .

### 1.4. Función $\varphi$ de Euler

**Definición 1.4.1** (Función  $\varphi$  de Euler). Definimos la función  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  como:

$$n \mapsto |\{a \in \mathbb{N} : (a, n) = 1 \wedge a \leq n\}|$$

**Proposición 1.4.1.** Sean  $p, q \in \mathbb{Z}^+$  primos distintos:

- I)  $\varphi(p) = p - 1$
- II)  $\varphi(p^k) = p^{k-1}(p - 1)$ ,  $k \in \mathbb{N}$
- III)  $\varphi(p^k q^t) = \varphi(p^k) \cdot \varphi(q^t)$ ,  $k, t \in \mathbb{N}$

*Demostración.* .

- I) Es evidente.
- II) Sea  $\Omega = \{x \in \mathbb{N} : x \leq p^k\}$ , sea  $a \in \Omega$  tal que  $(a, p^k) \neq 1$ .

Así  $(a, p) \neq 1$ , más aún  $a = pl$  para algún  $l \in \mathbb{N}$ . Luego, como  $a \in \Omega$ ,  $a = pl \leq p^k$ , por lo cual  $l \leq p^{k-1}$ . De este modo:

$$|\{a \in \Omega : p \mid a\}| = |\{a \in \Omega : a = pl, l \in \mathbb{N}\}| = |\{l \in \mathbb{N} : l \leq p^{k-1}\}| = p^{k-1}$$

Ahora:

$$\begin{aligned}\varphi(p^k) &= |\{a \in \Omega : (a, p^k) = 1\}| \\ &= |\Omega| - |\{a \in \Omega : p \mid a\}| \\ &= p^k - p^{k-1} = p^{k-1}(p - 1)\end{aligned}$$

- III) Consideremos  $\Omega = \{x \in \mathbb{N} : x \leq p^k q^t, k, t \in \mathbb{N}\}$ ,  $A = \{a \in \Omega : p \mid a\}$  y  $B = \{b \in \Omega : q \mid b\}$ .

Ahora  $A \cap B = \{a \in \Omega : p \mid a \wedge q \mid a\}$ . Note que de manera análoga a ii), tenemos:

$$|A| = p^{k-1} q^t, \quad |B| = p^k q^{t-1}$$

Por otro lado si  $a \in A \cap B$ , tenemos  $p \mid a \wedge q \mid a \implies \exists l \in \mathbb{N}$  tal que  $a = pql$ . Además como  $pql = a \leq p^k q^t$ , se sigue que  $l \leq p^{k-1} q^{t-1}$ , por lo cual:

$$|A \cap B| = p^{k-1} q^{t-1}$$

Por último, sabemos que  $\varphi(p^k q^t) = |\{a \in \Omega : (a, p^k q^t) = 1\}|$ . Por la proposición 1.2.1 tenemos:

$$\begin{aligned}\varphi(p^k q^t) &= |\Omega| - (|A| + |B| - |A \cap B|) \\ &= p^k q^t - p^{k-1} q^t - p^k q^{t-1} + p^{k-1} q^{t-1} \\ &= q^t (p^k - p^{k-1}) - q^{t-1} (p^k - p^{k-1}) \\ &= (p^k - p^{k-1})(q^t - q^{t-1}) \\ &= [p^{k-1}(p-1)][q^{t-1}(q-1)] \\ &= \varphi(p^k) \cdot \varphi(q^t)\end{aligned}$$

□

**Proposición 1.4.2.** Sean  $p_1, \dots, p_n \in \mathbb{N}$  primos distintos, sean  $k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$ :

$$\begin{aligned}\varphi(p_1^{k_1} \cdots p_n^{k_n}) &= p_1^{k_1} \cdots p_n^{k_n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right) \\ &= \varphi(p_1^{k_1}) \cdots \varphi(p_n^{k_n})\end{aligned}$$

*Demostración.* Falta demostrar. □

**Observación 1.4.** Observe que dados  $n, m \in \mathbb{N}$ , tales que  $(m, n) = 1$ , entonces:

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

*En efecto,* Por el teorema fundamental de la aritmética, podemos expresar  $n = p_1^{k_1} \dots p_l^{k_l}$ ,  $m = q_1^{t_1} \dots q_r^{t_r}$ , con  $p_1, \dots, p_l, q_1, \dots, q_r \in \mathbb{N}$  primos distintos y  $k_1, \dots, k_l, t_1, \dots, t_r \in \mathbb{N} \cup \{0\}$ , así:

$$\begin{aligned}\varphi(n \cdot m) &= \varphi(p_1^{k_1} \dots p_l^{k_l} q_1^{t_1} \dots q_r^{t_r}) \\ &= \varphi(p_1^{k_1} \dots p_l^{k_l}) \cdot \varphi(q_1^{t_1} \dots q_r^{t_r}) \\ &= \varphi(n) \cdot \varphi(m)\end{aligned}$$

□

# CAPÍTULO 2

## Grupos

---

---

### 2.1. Grupos

**Definición 2.1.1** (Grupo). *Un grupo es un conjunto no vacío  $G$  junto con una operación  $\circ : G \times G \rightarrow G$ , que satisface:*

I) *font Asociatividad:*  $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$

II) *font Elemento neutro:*  $\exists e \in G : a \circ e = a \quad \forall a \in G$

III) *font Inverso:*  $\forall a \in G \quad \exists b \in G : a \circ b = e$

Se denota a esta estructura:  $(G, \circ, e)$ , en caso de no conocer la identidad  $(G, \circ)$ . Además, para facilitar la notación el inverso de  $a$  elemento de un grupo se denota como  $a^{-1}$ .

**Ejemplo 2.1.** *Sea  $\mathbb{Z}$ , y la suma usual en los números enteros, es claro que es un grupo.*

**Ejemplo 2.2.**  $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$  son grupos.

**Ejemplo 2.3.**  $(\mathbb{Z}/n\mathbb{Z}, +)$  es un grupo.

*En efecto,* Anteriormente se había probado que  $+$  es cerrado y está bien definida  $\bar{a} + \bar{b} = \overline{a + b}$ .

I)  $+$  es asociativa, pues:

$$\bar{a} + \overline{(b + c)} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{(a + b)} + \bar{c}$$

II) Note que la identidad es  $\bar{0}$ , ya que:

$$\bar{a} + \bar{0} = \overline{a + 0} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$$

III) Ahora dado  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ , note que  $a + (-a) = 0$ , luego:

$$\begin{aligned}\overline{a + (-a)} &= \bar{0} \\ \bar{a} + \overline{(-a)} &= \bar{0}\end{aligned}$$

Así  $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z} \quad \exists \overline{(-a)} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} + \overline{(-a)} = \bar{0}$ .

□

**Ejemplo 2.4.** Sean  $A$  un conjunto no vacío, sea  $V$  un espacio vectorial, sea  $\mathcal{H}$  el conjunto de funciones  $f : A \rightarrow V$ , definamos la operación suma sobre  $\mathcal{H}$  como:

$$\begin{aligned}+ : \mathcal{H} \times \mathcal{H} &\rightarrow \mathcal{H} \\ (f + g)(a) &\mapsto f(a) + g(a) \quad \forall a \in A\end{aligned}$$

En efecto, note:

I) Sean  $f, g, h \in \mathcal{H}$ , sea  $a \in A$ :

$$\begin{aligned}[(f + g) + h](a) &= (f + g)(a) + h(a) \\ &= (f(a) + g(a)) + h(a) \\ &= f(a) + (g(a) + h(a)) \\ &= f(a) + (g + h)(a) \\ &= [f + (g + h)](a)\end{aligned}$$

$$\therefore (f + g) + h = f + (g + h)$$

II) Tenemos  $\underline{0} \in \mathcal{H}$ , definida por:  $\underline{0}(a) = 0 \quad \forall a \in A$ , sea  $f \in \mathcal{H}$ , sea  $a \in A$ ,

$$(f + \underline{0})(a) = f(a) + \underline{0}(a) = f(a) + 0 = f(a)$$

Así  $f + \underline{0} = f$ , i.e.  $\underline{0}$  es el elemento neutro.

III) Sea  $f \in \mathcal{H}$ , sea  $a \in A$ , note que existe  $-f(a)$ , tal que:

$$f(a) + (-f(a)) = 0 \quad \forall a \in A,$$

entonces  $-f$  es inverso de  $f$ .

□

**Ejemplo 2.5.** Sea  $V$  un espacio vectorial real, entonces  $(V, +)$  es un grupo.

**Ejemplo 2.6.**  $(\mathcal{M}_{m \times n}(\mathbb{R}), +)$  es un grupo.

**Ejemplo 2.7.** Sea  $GL_{(n)}(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : \det(A) \neq 0\}$ , con el producto de matrices forma un grupo.

**Ejemplo 2.8.** Considera  $\mathbb{Z}/n\mathbb{Z}$ , sea  $G \subseteq \mathbb{Z}/n\mathbb{Z}$ , el conjunto

$$G = \{\bar{a} : (a, n) = 1\}$$

entonces  $(G, \cdot)$  con la op. definida por el producto de clases es un grupo.

En efecto, Note:

I)  $\forall \bar{a}, \bar{b}, \bar{c} \in G, \quad \bar{a}(\bar{b} \cdot \bar{c}) = \bar{a}(\overline{\bar{b} \cdot \bar{c}}) = \overline{\bar{a}(\bar{b} \cdot \bar{c})} = \overline{(ab)c} = \overline{(ab)} \cdot \bar{c} = (\bar{a}\bar{b})\bar{c}$ .

II)  $\bar{1} \in G$ , pues  $(1, n) = 1$ , además  $\forall \bar{a} \in G \quad \bar{a} \cdot \bar{1} = \bar{a}$ .

III) Sea  $\bar{a} \in G$ , entonces  $(a, n) = 1$ , por tanto  $\exists x, y \in \mathbb{Z}$ , tal que:

$$ax + ny = 1$$

Tomando la clase:

$$\bar{1} = \overline{ax + ny} = \overline{ax} + \overline{ny} = \bar{a}\bar{x} + \bar{n}\bar{y} = \bar{a}\bar{x} + \bar{0}\bar{y} = \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x}$$

i.e. existe  $\bar{x} \in G$ , tal que  $\bar{a} \cdot \bar{x} = 1$ .

□

**Definición 2.1.2** (Grupo abeliano). *Sea  $(G, \circ, e)$  un grupo, si cumple que  $a \circ b = b \circ a \quad \forall a, b \in G$ , diremos que es un grupo abeliano.*

**Ejemplo 2.9.**  $(\mathbb{Z}, +, 0)$  es abeliano.

**Ejemplo 2.10.**  $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$  es abeliano.

**Ejemplo 2.11.**  $((\mathbb{Z}/n\mathbb{Z})^*, \cdot, \bar{1})$  es abeliano.

**Proposición 2.1.1.** *Sea  $(G, \circ)$  un grupo, sea  $g \in G$  tal que  $g \circ g = g$  entonces  $g = e$ .*

*Demostración.* Como  $g \in G \implies \exists g' \in G$  tal que  $g \circ g' = e$ , luego:

$$g = g \circ e = g \circ (g \circ g') = (g \circ g) \circ g' = g \circ g' = e$$

□

**Proposición 2.1.2.** *Sea  $(G, \circ)$  grupo,  $g \in G$ , entonces:*

$$g^{-1} \circ g = g \circ g^{-1} = e$$

*Demostración.*

$$(g^{-1} \circ g) \circ (g^{-1} \circ g) = (g^{-1} \circ (g \circ g^{-1})) \circ g = (g^{-1} \circ e) \circ g = g^{-1} \circ g$$

Luego por la prop. anterior:

$$g^{-1} \circ g = e, \quad \text{i.e. } g \circ g^{-1} = g^{-1} \circ g = e$$

□

**Proposición 2.1.3.** Si  $(G, \circ)$  es un grupo y  $g \in G$ , entonces:

$$e \circ g = g \circ e = g$$

*Demuestra*ción.

$$e \circ g = (g \circ g^{-1}) \circ g = g \circ (g^{-1} \circ g) = g \circ e = g = g \circ e$$

□

**Proposición 2.1.4.** Sea  $(G, \circ)$  un grupo, el elemento neutro  $e$ , es único.

*Demuestra*ción. Supongamos que existe  $e' \in G$  tal que  $g \circ e' = g$ ,  $\forall g \in G$ , en particular:

$$e = e \circ e' = e' \circ e = e', \quad \text{i.e. } e \text{ es único.}$$

□

**Ejemplo 2.12.** Sea  $G_1 = \mathbb{Z}/n\mathbb{Z}$ , sea  $G_2 = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$ , entonces se tienen los grupos:  $(G_1, +, \bar{0})$ ,  $(G_2, \cdot, \bar{1})$ , es claro que no son iguales ya que:  $|G_1| = n$ ,  $|G_2| = \varphi(n)$ .

**Proposición 2.1.5.** Si  $(G, \circ)$  es un grupo y  $g \in G$ , entonces  $g^{-1}$  es único.

*Demuestra*ción. Suponga  $g' \in G$  tal que  $g \circ g' = e$ , entonces:

$$g^{-1} = g^{-1} \circ e = g^{-1} \circ (g \circ g') = (g^{-1} \circ g) \circ g' = e \circ g' = g'$$

□

## 2.2. Subgrupos

**Definición 2.2.1** (Subgrupo). Sea  $(G, \circ, e)$  un grupo, sea  $H \subseteq G$  un subconjunto de  $G$ , diremos que  $H$  es un subgrupo de  $G$ , si con la misma operación  $\circ$ , definida en  $G$ , forma un grupo. Se denotará  $H \leq G$ .

**Ejemplo 2.13.** Sea  $(G = \mathbb{Z}, +, 0)$ , para algún  $a \in \mathbb{Z}$ , definamos:

$$H_a = \{t \in \mathbb{Z} : t = na, n \in \mathbb{Z}\}$$

entonces  $(H_a, +, 0)$  es un subgrupo de  $G$ .

*Demuestra*ción. Claramente  $H_a \subseteq G$ , además  $+$  es cerrada en  $H_a$ , pues si  $n_1a, n_2a \in H_a \implies n_1a + n_2a = (n_1 + n_2)a \in H_a$ .

I)  $+$  es asociativa, porque hereda la asociatividad de  $G$ .

II)  $0 \in H_a$ , ya que  $0 = 0 \cdot a \in H_a$ , además  $na + 0 = na \quad \forall na \in H_a$ .

III) Si  $na \in H_a$ , como  $n \in \mathbb{Z} \implies -n \in \mathbb{Z}$ , así  $\exists -na \in H_a \implies na + (-na) = 0$ .

□

**Ejemplo 2.14.** Sea  $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ , entonces  $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ , este es llamado el grupo especial lineal.

**Observación 2.1.** Sea  $(G, \circ, e)$  grupo, sea  $H \leq G$ , entonces  $e \in H$ .

En efecto, como  $H \neq \emptyset$ ,  $\exists g \in H$ , además  $\exists g^{-1} \in H$  al ser un subgrupo, así:

$$g \circ g^{-1} = e, \quad \text{i.e. } e \in H.$$

□

**Proposición 2.2.1.** Si  $(G, \circ, e)$  es un grupo y  $\{H_\lambda\}_{\lambda \in I}$  es una colección arbitraria de subgrupos, entonces:

$$\bigcap_{\lambda \in I} H_\lambda, \text{ es un subgrupo de } G.$$

*Demostración.* Como  $H_\lambda \leq G \quad \forall \lambda \in I$ ,  $\bigcap_{\lambda \in I} H_\lambda \neq \emptyset$  pues  $e \in H_\lambda \quad \forall \lambda \in I$ . Sean  $a, b \in \bigcap_{\lambda \in I} H_\lambda$ , entonces  $a, b \in H_\lambda \quad \forall \lambda \in I$ , además  $\circ$  es cerrada en  $\bigcap_{\lambda \in I} H_\lambda$ , ya que  $a \circ b \in H_\lambda \quad \forall \lambda \in I$ , así  $a \circ b \in \bigcap_{\lambda \in I} H_\lambda$ . Luego:

I)  $\circ$  es asociativa en  $\bigcap_{\lambda \in I} H_\lambda$ , ya que es asociativa en  $H_\lambda, \forall \lambda \in I$ .

II)  $e \in \bigcap_{\lambda \in I} H_\lambda$ .

III) Dado que  $a \in \bigcap_{\lambda \in I} H_\lambda$ , entonces  $a \in H_\lambda \forall \lambda \in I$ , así  $\exists a^{-1} \in H_\lambda \forall \lambda \in I$  tal que  $a \circ a^{-1} = e$ , luego  $a^{-1} \in \bigcap_{\lambda \in I} H_\lambda$ .

□

**Proposición 2.2.2.** Sea  $(G, \circ, e)$  un grupo, sean  $H, K \leq G$ , entonces  $H \cup K$  es un subgrupo de  $G$  si y sólo si  $H \subseteq K \vee K \subseteq H$ .

*Demostración.* Será demostrada primero la reciprocidad.

( $\Leftarrow$ ) Basta notar que si  $H \subseteq K$ ,  $H \cup K = K$  y  $K \leq G$ , así  $H \cup K \leq G$ . Análogo si  $K \subseteq H$ .

( $\Rightarrow$ ) Sea  $H \cup K \leq G$ . Supongamos que  $H \not\subseteq K \wedge K \not\subseteq H$ , sean  $a \in H \setminus K$  y  $b \in K \setminus H$ . Sea  $c = a \circ b$ . Como  $H \cup K \leq G$ , entonces  $c \in H \cup K$ , así  $c \in H \vee c \in K$ .

Si  $c \in H \implies a^{-1} \circ c = b \in H$ , lo cual no puede ser (pues  $b \in K \setminus H$ ). Si  $c \in K \implies c \circ b^{-1} = a \in K$ , lo cual no puede ser (pues  $a \in H \setminus K$ ).

Por lo cual  $H \subseteq K \vee K \subseteq H$ .

□

**Definición 2.2.2** (Orden de un grupo). Sea  $(G, \circ, e)$  un grupo, el orden del grupo será la cardinalidad de  $G$  y se denota  $|G|$ .

**Definición 2.2.3.** Sea  $(G, \circ, e)$  un grupo, diremos que es un grupo finito si  $G$  es un conjunto finito. En caso contrario se le dice infinito.

**Definición 2.2.4.** Sea  $(G, \circ, e)$  un grupo, sea  $S \subseteq G$ , con  $S \neq \emptyset$ , el grupo generado por  $S$  en  $G$  denotado por  $\langle S \rangle$  es el menor de los subgrupos que lo contiene, i.e.:

$$\langle S \rangle = \bigcap_{\substack{S \subseteq H \\ H \leq G}} H$$

Si  $S$  es finito, y sea  $H = \langle S \rangle$ , diremos que  $H$  es finitamente generado.

**Ejemplo 2.15.** Todo subgrupo finito de  $G$  es finitamente generado, más aún, si  $H \leq G$  y es finito  $\langle H \rangle = H$ .

*Demuestra*ción. Dado que:

$$\langle H \rangle = \bigcap_{\substack{H' \leq G \\ H \subseteq H'}} H' \subseteq H' \quad \forall H' \leq G \text{ tales que } H \subseteq H',$$

además como  $H \leq G$  y  $H \subseteq H$ , entonces  $H$  es uno de los términos de la intersección, así:

$$\langle H \rangle \subseteq H \wedge H \subseteq \bigcap_{\substack{H' \leq G \\ H \subseteq H'}} H' = \langle H \rangle$$

Por lo tanto  $\langle H \rangle = H$ . □

**Ejemplo 2.16.**  $(\mathbb{Z}, +, 1)$  es finitamente generado, basta notar que:

$$\mathbb{Z} = \langle \{1\} \rangle$$

**Ejemplo 2.17.**  $(\mathbb{Q}, +, 1)$ ,  $\mathbb{Q}$  no es finito ni es finitamente generado.

**Proposición 2.2.3.** Sea  $(G, \circ, e)$  un grupo,  $H \subseteq G$  no vacío, entonces las cond. son equivalentes:

- I)  $H \leq G$
- II)  $\forall x, y \in H$  se tiene que  $x \circ y \in H \wedge x^{-1} \in H$ .
- III)  $\forall x, y \in H$  se tiene que  $x \circ y^{-1} \in H$ .

*Demuestra*ción. Se probarán las implicaciones en ciclo.

- I  $\Rightarrow$  II) Se sigue de la definición ya que la operación en  $G$  debe ser una operación en  $H$ , además de que si  $H$  es un subgrupo  $\forall x \in H \implies \exists x^{-1} \in H$ .
- II  $\Rightarrow$  III) Si  $x, y \in H$  por ii)  $y^{-1} \in H$ , luego  $x \circ y^{-1} \in H$  (por ii).

- III  $\Rightarrow$  I) Sea  $x \in H$ , entonces  $x \circ x^{-1} = e$ , luego, note que si  $x \in H$  entonces  $x^{-1} = e \circ x^{-1} \in H$ .

Ahora probemos que la operación es cerrada: sea  $x, y \in H$ , entonces  $y^{-1} \in H$ , más aún  $(y^{-1})^{-1} = y$ , ya que  $y^{-1} \circ y = y^{-1} \circ (y^{-1})^{-1} = e$  y por la unicidad del inverso  $(y^{-1})^{-1} = y$ . Por lo cual  $x \circ y = x \circ (y^{-1})^{-1} \in H$ , por lo tanto la operación es cerrada en  $H$ .

□

**Observación 2.2.** *Sea  $(G, \circ, e)$  un grupo, sean  $a, b \in G$  entonces:*

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

En efecto,

$$(a \circ b)(b^{-1} \circ a^{-1}) = a(b \circ b^{-1}) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$$

Por la unicidad del inverso se sigue  $b^{-1} \circ a^{-1} = (a \circ b)^{-1}$ . □

Cuando no haya perdida de generalidad para facilitar la escritura de la operación  $\circ$  en un grupo  $G$ , se denotará expresará como el producto, es decir:  $a \circ b := ab$ . Además, se podrá expresar la potencia de un elemento  $a \in G$  como:

$$a^n = \underbrace{a \cdots a}_{n-\text{veces}}$$

para  $n \in \mathbb{Z}^+$ . Si  $n = 0$ ,  $a^0 = e$  y podemos observar que  $a^{-n} = (a^n)^{-1}$  para  $n \in \mathbb{N}$ .

**Observación 2.3.** *Si  $S \neq \emptyset$ , es un subconjunto de un grupo  $G$ , entonces:*

$$\langle S \rangle = \{s_1^{i_1} \dots s_n^{i_n} : s_j \in S, i_j = \pm 1, j = 1, \dots, n, n \in \mathbb{N}\}$$

*Demostración.* Sea  $H = \{s_1^{i_1} \dots s_n^{i_n} : s_i \in S, i_j = \pm 1, j = 1, \dots, n, n \in \mathbb{N}\}$ . Sean  $s, t \in H$ , tales que  $s = s_1^{i_1} \dots s_n^{i_n}$ ,  $t = t_1^{j_1} \dots t_m^{j_m}$ , con  $s_1, \dots, s_n, t_1, \dots, t_m \in S$ ,  $i_1, \dots, i_n, j_1, \dots, j_m \in \{1, -1\}$ . Notemos que:

$$st^{-1} = s_1^{i_1} \dots s_n^{i_n} (t_1^{j_1} \dots t_m^{j_m})^{-1} = s_1^{i_1} \dots s_n^{i_n} t_m^{-j_m} \dots t_1^{-j_1} \in H$$

Así por la proposición 2.2.3  $H \leq G$ , así  $\langle S \rangle \subseteq H$ . Ahora sea  $N \leq G$ , tal que  $S \subseteq N$ , es claro que  $s \in N$  (cualquier elemento de esa forma está en  $N$ ), así  $H \subseteq N$ , así  $H = \langle S \rangle$ . □

## 2.3. Grupo de permutaciones

**Definición 2.3.1** (Grupo de Permutaciones). *Sea  $X$  un conjunto no vacío, sea  $\mathcal{H} = \{f : X \rightarrow X : f \text{ es biyectiva}\}$ , consideremos la composición de funciones, entonces  $\mathcal{H}$  forma un grupo llamado el grupo de permutaciones del conjunto  $X$  denotado por  $S_X$ .*

*En caso de que  $X$  sea finito, podemos enlistar los elementos de  $X$  por  $a_1, \dots, a_n$ , podemos representar con un arreglo bidimensional de renglones colocando:*

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{\sigma(1)} & a_{\sigma(2)} & \dots & a_{\sigma(n)} \end{pmatrix}$$

*Donde  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ , tal que  $\sigma(i) = j$ , si  $f(a_i) = a_j$ , de este modo podemos prescindir de los elementos de  $X$  y fijarnos solo en los subíndices e identificar a  $f$  con:*

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

*En este caso se escribirá como  $S_n$  con  $n = |X|$ .*

**Ejemplo 2.18.**  $S_3$  es el grupo formado por los elementos:

$$\{e, \sigma, \theta, \sigma \cdot \theta, \theta \cdot \sigma, \theta^2\}$$

Donde:

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \theta &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \theta^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \sigma \cdot \theta &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \theta \cdot \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

○	e	θ	σ	θ <sup>2</sup>	σ · θ	θ · σ
e	e	θ	σ	θ <sup>2</sup>	σ · θ	θ · σ
θ	θ	θ <sup>2</sup>	θ · σ	e	σ	σ · θ
σ	σ	σ · θ	e	θ · σ	θ	θ <sup>2</sup>
θ <sup>2</sup>	θ <sup>2</sup>	e	σ · θ	θ	θ · σ	σ
σ · θ	σ · θ	θ · σ	θ <sup>2</sup>	σ	e	θ
θ · σ	θ · σ	σ	θ	σ · θ	θ <sup>2</sup>	e

Es evidente que  $S_3$  no es abeliano, basta notar  $\theta \circ \sigma \neq \sigma \circ \theta$ . Además observe que si el orden de  $X$  es  $n$ ,  $|S_n| = n!$ .

**Observación 2.4.** Si  $n \geq 3$ , entonces  $S_n$  no es abeliano.

*En efecto,* Basta tomar:

$$\sigma = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ 1 & \dots & i+1 & i & \dots & n \end{pmatrix}, \quad \theta = \begin{pmatrix} 1 & \dots & j & j+1 & \dots & n \\ 1 & \dots & j & j+1 & \dots & n \end{pmatrix} \quad \text{con } i \neq j$$

y notar que  $\sigma \circ \theta \neq \theta \circ \sigma$ .

Además podemos notar que trivialmente  $S_1$  y  $S_2$  son un grupo abeliano. □



# CAPÍTULO 3

## Productos Directos

---

Definición 3.0.1. *Sea  $H$*