

FM1002 Fundamentos del Álgebra abstracta

Profesores: Sebastián Tapia, Sebastián Reyes Riffo, Leslie Jiménez

Auxiliares: Nicolás Cornejo, Camilo Carvajal, Jordan Urra, Pablo Araya, Bruno Moreno, Ignacio Fierro



Para estudiantes de Educación Básica y Media.

Resumen Estructuras Algebraicas

1. **Ley de Composición Interna:** Dado un conjunto no vacío A y una operación $*$. Una ley de composición interna (l.c.i.) es aquella donde al tomar $x, y \in A$ la operación entre ambos sigue estando en el conjunto, es decir, $x * y \in A$.

Ejemplos:

- a) $+$ en $\mathbb{R}$.
- b) $\cdot$ en $\mathbb{Q}$.

2. **Estructura Algebraica:** Si $*$ es una l.c.i (es decir, una operación) definida en el conjunto A , al par $(A, *)$ le llamaremos Estructura Algebraica.

Ejemplos:

- a) $(\mathbb{R}, +)$
- b) $(\mathbb{Q}, \cdot)$

3. **Propiedades básicas** Sea $(A, *)$ una estructura algebraica.

- a) **Asociatividad:** Diremos que $*$ es asociativo si:

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

- b) **Elemento Neutro:** Diremos que $e \in A$ es el elemento neutro para $*$ si:

$$(\forall x \in A)e * x = x * e = x$$

- c) **Elemento Inverso:** Diremos que x tiene elemento inverso para $*$ si:

$$(\exists y \in A) : y * x = x * y = e$$

- d) **Conmutatividad:** Diremos que $*$ es conmutativo si:

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

4. **Grupo:** Sea $(G, *)$ una estructura algebraica. Diremos que G es un grupo si:

- a) $*$ es asociativo
- b) $(G, *)$ posee neutro $e \in G$.
- c) Todo elemento $x \in G$ posee inverso $x^{-1} \in G$

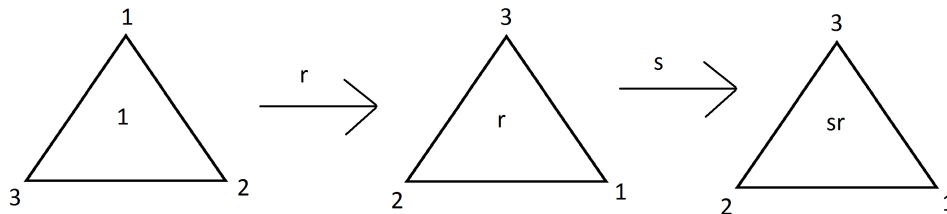
Si en particular cumple con ser conmutativo diremos que es un **Grupo Abelian**

Ejemplos:

- a) $(\mathbb{R}, +)$
- b) $(\mathbb{Q} \setminus \{0\}, \cdot)$
- c) $(\mathbb{Z}_p, +_p)$

Ahora veamos un par de grupos interesantes:

- I **Grupo Diedral** Se denota D_n y es el conjunto donde están todas las simetrías y rotaciones de un polígono de n lados. Por ejemplo en el conjunto de D_3 :



El primer triángulo es la identidad donde no se realiza ninguna rotación o reflexión y se denota por 1, luego el segundo triángulo es una rotación denotada con la letra r y el tercer triángulo es una simetría luego de una rotación denotado por sr . El conjunto D_3 y D_4 , está compuesto por los siguientes elementos:

$$D_3 = \{1, r, r^2, s, sr, sr^2\}$$

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

En general en el conjunto D_n hay $2n$ elementos, que serían los siguientes:

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

- II **Grupo Simétrico** Se denota S_n y es el conjunto donde están todas las permutaciones del conjunto $\{1, 2, 3, 4, \dots, n\}$. Por ejemplo en S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Para escribir los elementos de S_n se usa la notación de ciclos. Por ejemplo para escribir el elemento del ejemplo anterior como ciclo queda:

$$(1 \ 2 \ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Finalmente un ejemplo de composición de ciclos en S_4 sería el siguiente:

$$(1 \ 2 \ 3 \ 4) \circ (2 \ 4) = (1 \ 2) (3 \ 4)$$

5. **Subgrupo:** Sea $(G, *)$ un grupo, y sea $H \subseteq G$ con $H \neq \emptyset$. Diremos que H es un subgrupo de G si $(H, *)$ también es un grupo. Todo grupo tiene dos subgrupos que llamaremos **triviales**:

$$(G, *) \text{ y } (\{e\}, *)$$

Ejemplos:

- a) Para $(\mathbb{R}, +)$ un subgrupo es $(\mathbb{Q}, +)$
 - b) Para $(\mathbb{Q} \setminus \{0\}, \cdot)$ un subgrupo es $(\{-1, 1\}, \cdot)$
 - c) Para $(\mathbb{Z}_4, +_4)$ un subgrupo es $(\{[0]_4, [2]_4\}, +_4)$
6. **Reticulado:** A un grupo G , se le puede construir un reticulado, que es una red de grupos, que permite visualizar los subgrupos de G , y la cantidad de elementos que poseen, los reticulados se construyen colocando el grupo completo arriba, y luego uniendo hacia abajo mediante líneas los subgrupos de G , donde la cantidad de elementos que poseen los subgrupos va disminuyendo, y se unen mediante líneas los subgrupos.
7. **Teorema de Lagrange:** Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo cualquiera de el. Entonces $|H|$ divide a $|G|$.

Ejemplos:

- a) Para $(\mathbb{Z}_4, +_4)$ un subgrupo es $(\{[0]_4, [2]_4\}, +_4)$ donde podemos ver que $|\{[0]_4, [2]_4\}| = 2$ divide a $|\mathbb{Z}_4| = 4$
 - b) Para $(\mathbb{Z}_3, +_3)$ los unicos subgrupos posibles son los triviales ya que $|\mathbb{Z}_3| = 3$ donde sus divisores son 3 y 1.
8. **Anillo:** Una estructura $(A, +, \cdot)$ se llamara anillo si:
- a) $(A, +)$ es grupo abeliano.
 - b) $\cdot$ es asociativa.
 - c) $\cdot$ distribuye con respecto a $+$.

Si la operacion $\cdot$ posee neutro en A , diremos que $(A, +, \cdot)$ es un **anillo con unidad**. Si $\cdot$ es conmutativa, diremos que $(A, +, \cdot)$ es un **anillo conmutativo**.