# Estructuras Algebraicas - Introducción a la teoría de grupos

Las estructuras de datos mediante las cuales es posible representar los datos en un ordenador y manipularlos para resolver problemas, son estructuras algebraicas.

Con buenas estructuras algebraicas de datos es posible obtener buenas soluciones algorítmicas a problemas computacionales. La estructura en la que nos vamos a concentrar es la de **Grupos**.

La teoría de grupos es una teoría que se aplica en distintos temas de la informática como por ejemplo en el estudio de máquinas de estado finito y de lenguajes formales.

Es una teoría moderna en la historia de la matemática que aunque tuvo resultados importantes antes se consolidó en pleno siglo XXI.

## 1 Estructuras Algebraicas

Una ***Estructura Algebraica*** es un conjunto no vacío dotado con una o más operaciones. Estas operaciones están definidas en el producto cartesiano (pueden ser n-arias aunque aquí vamos a concentrarnos en operaciones unarias y binarias) y serán cerradas.
Esto es, supongamos que $A$ es el conjunto no vacío, si a cada elemento del producto cartesiano se le asigna unívocamente un elemento del conjunto $A$ diremos que la operación está bien definida, o que es una operación n-aria en $A$ .

Dependiendo de las propiedades que tengan estas operaciones la estructura recibirá un nombre diferente.

Por ejemplo, dado un conjunto no vacío $A$ y una operación $*$ sobre $A$, si $* : A \times A \to A$ se llamará operación binaria.

**Ejemplo 1.1.**

*Sea $A$ el conjunto de los números naturales.*
*Si a cada par de números naturales se le asigna el número natural que corresponde a su suma se estará definiendo una operación binaria sobre $A$, pero si en lugar de asignar el correspondiente a la resta no se definirá una operación cerrada (para cada par de elementos de $A$) y por lo tanto no será una operación binaria.*
*Tampoco se tendrá una operación binaria si se pretende asignar a cada par de naturales* un natural cualquiera mayor que cualquiera de ellos*: aquí, si bien el resultado será siempre natural, no estará unívocamente determinado*

Cuando tenemos conjuntos finitos podemos definir las operaciones por medio de tablas: por ejemplo, si $A = \{a, b\}$

| $*$ | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $b$ | $a$ |

Veamos que *hace* esta operación:

$$a * a = b$$
$$a * b = a$$
$$b * a = b$$
$$b * b = a$$

Definida la operación binaria $*$ sobre $A$ se diremos que:

$*$ es ***conmutativa*** si, para todo $a$ y $b$ en $A$, resulta $a * b = b * a$

$*$ es ***asociativa*** si, cualesquiera sean $a$, $b$ y $c$ en $A$, resulta $a * (b * c) = (a * b) * c$

$(A, *)$ tiene ***elemento neutro*** si existe en $A$ un elemento $e$ tal que para todo $a$ en $A$ valga que $a * e = e * a = a$.

Si $(A, *)$ tiene un elemento neutro $e$, se dirá que un elemento $a$ de $A$ tiene ***inverso*** si existe $a'$ en $A$ tal que $a * a' = a' * a = e$.

**Propiedades de las operaciones (binarias)**

Existen algunos resultados generales que sólo dependen de las propiedades que verifique la operación, esto es: para demostrarlas no se necesita especificar ni $A$ ni la operación en particular sino sólo a las propiedades que cumple la operación.

- Si para una operación $*$ en $A$ existe un elemento neutro, éste es único.

  *Supongamos que hay dos neutros,*$e_1$, $e_2$ *y veamos que son iguales*
  *Como* $e_1$ *es neutro,*$e_2 * e_1 = e_2$. *De la misma forma,* $e_1 * e_2 = e_1$ *ya que* $e_2$ *es neutro*
  *Entonces:* $e_1 = e_1 * e_2 = e_2 * e_1 = e_2$

- Si para una operación asociativa $*$ en $A$ existe un elemento neutro $e$ y un elemento del conjunto, $a$, tiene inverso $a^{-1}$ entonces éste es único. *La demostración se deja como ejercicio*

- Si para una operación $*$ asociativa en $A$ existe un elemento neutro $e$ y todo elemento tiene su inverso, entonces vale en $A$ la llamada *propiedad cancelativa* : $a * b = a * c \Rightarrow b = c$ (de modo similar, $b * a = c * a \Rightarrow b = c$)

  *Suponemos que* $a * b = a * c$ *(vamos a ver que* $b = c$*)*
  *Como por hipótesis todo elemento de* $A$ *tiene inverso por la operación* $*$*, operamos a cada lado de la igualdad con el inverso de* $a$*,* $a'$*, que sabemos que existe*
  $a' * (a * b) = a' * (a * c)$*, y como la operación es asociativa,* $(a' * a) * b = (a' * a) * c$ .
  *Luego,* $e * b = e * c$ *y entonces* $b = c$.

El nombre de una estructura algebraica $(A, *)$ (conjunto A dotado de una operación $*$) indica qué propiedades verifica la operación y permite asegurar que se cumplirán ciertos resultados, sin importar los elementos o la operación en particular de que se trate.

- Se dirá que $(A, *)$ tiene estructura de ***grupoide*** si la operación $*$ es una operación binaria.

- Se dirá que $(A, *)$ tiene estructura de ***semigrupo*** si $*$ es asociativa. Si además $*$ es conmutativa se dirá un ***semigrupo conmutativo***.

- Se dirá que $(A, *)$ tiene estructura de ***monoide*** si $*$ es asociativa y existe en $A$ elemento neutro para $*$ .Será ***monoide conmutativo*** si $*$ es además conmutativa.

- Se dirá que $(A, *)$ tiene estructura de ***grupo*** si $*$ es asociativa, existe en $A$ elemento neutro para $*$ y cada elemento de $A$ tiene inverso.
  Si $*$ es además conmutativa se llamará ***grupo conmutativo*** *(o* ***Abeliano****)*

- Si tengo dos operaciones binarias, que en general se llaman *suma* y *producto*, la terna ordenada $(A, +, .)$ tiene estructura de **anillo** si $(A, +)$ es un grupo conmutativo, el producto es asociativo y se satisfacen

  1. Distributividad por la izquierda: para cualesquiera $a, b, c \quad a(b + c) = ab + ac$
  2. Distributividad por la derecha: para cualesquiera $a, b, c \quad (a + b)c = ac + bc$

  Si el producto es conmutativo la estructura se llama **anillo conmutativo**.

  Un anillo $(A, +, .)$ tiene **elemento unitario** si existe $a \in A$ que sea neutro para el producto, éste neutro debe ser diferente al nuestro de la otra operación.

- Un anillo conmutativo con elemento unitario se dice que es un **dominio de integridad** si se cumple para todo $a, b \in A$ que $a.b = 0$ implica $a = 0$ ó $b = 0$

**Ejemplos 1.2.** *1. Los enteros con la multiplicación constituyen un monoide conmutativo.*

*2. Los racionales positivos con la multiplicación: $(Q^+, +)$ forman un grupo conmutativo*

*3. Las matrices cuadradas con el producto forman un monoide (no conmutativo). El neutro es la matriz Identidad*

*4. - Dado un conjunto $C$, el conjunto de partes de $C$ con la operación unión, $(P(C), \cup)$, constituye un monoide conmutativo cuyo elemento neutro es el $\emptyset$*

*- el conjunto de partes de $C$ con la operación intersección , $(P(C), \cap)$, constituye un monoide conmutativo cuyo elemento neutro es $C$*

Sea $(S, *)$ un semigrupo. Para cualquier $a \in S$ definimos

$$a^1 = a$$
$$a^n = a * a^{n-1} \quad n = 2, 3, 4....$$

**Observación**: Cualquiera sea $n \in N$ se indicará con $a^n$ el resultado de operar $a$ consigo mismo $n$ veces, esto es $a * a * \cdots * a = a \cdot \ldots a$

A partir de esto , es sencillo demostrar las leyes de los exponentes :

Dado un semigrupo $(S, *)$, $a \in S$ y $m, n$ naturales, valen:

- $a^m * a^n = a^{m+n}$
- $(a^m)^n = a^{m.n}$

## 2 Grupos

Como dijimos más arriba, consideraremos un conjunto no vacío $G$, sobre el que se ha definido una operación binaria asociativa $*$ , para la cual existe un elemento neutro $e \in G$ , y de modo tal que para cada elemento exista un inverso (en el conjunto).

Es común usar una notación especial cuando trabajamos con grupos. En lugar $*$ se use simplemente $\cdot$ (aunque no signifique multiplicación convencional, salvo que se lo aclare) y en ese caso el neutro se suele indicar 1 (sin que necesariamente signifique el número 1) y el inverso de $a$ se indica $a^{-1}$ (notación multiplicativa). También puede usarse una notación aditiva en cuyo caso la operación se indica con $+$ , el neutro con 0 y el inverso de a con $-a$ (tampoco $+$ y 0 significan suma y el número 0, excepto que se lo aclare).
*En general, en las demostraciones usaremos notación multiplicativa por comodidad. Más aún, también omitiremos el punto y terminará escribiéndose, simplemente, ab en lugar de* $a \cdot b$

A veces se da por sobrentendida la operación y se dice, haciendo abuso de lenguaje, que $G$ es grupo, en lugar de decir que $(G, *)$ lo es.

**Notación**: será muy útil la siguiente cuestión de notación (multiplicativa):

- Cualquiera sea $n \in N$ se indicará con $a^n$ el resultado de operar $a$ consigo mismo $n$ veces, esto es $a * a * \cdots * a = a \cdot \ldots a$
- $a^{-n}$ será el resultado de la operación $a^{-1} * a^{-1} * \cdots * a^{-1}$
- $(a^n)^{-1} = a^{-n}$

**Obs:** Se tiene, por definición, $a^n * a^{-n}$ , por lo que obtenemos $a^0 = e$

Por lo visto y demostrado antes, podemos asegurar que en cualquier grupo

- *el elemento neutro es único*
- *todo elemento tiene un único inverso*
- *valen las propiedades cancelativas*

También se verifica en todo grupo $(G, \cdot)$ que:

1. Cualquiera sea $a \in G$, $(a^{-1})^{-1} = a$

   *Para cualquier $a \in G$, existe $a^{-1}$ tal que $a.a^{-1} = e$ (por definición de inverso*
   *Por otro lado, sabemos que $(a^{-1})^{-1}$ es el inverso de $a^{-1}$, es decir $(a^{-1})^{-1}.a^{-1} = e$*
   *luego, y como el inverso es único, vale que $(a^{-1})^{-1} = a$*

2. Cualesquiera sean $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

   *Queremos probar que el inverso del producto es el producto de los inversos PERO con el orden de los factores cambiados*
   *Nuevamente usaremos la definición de inverso y su unicidad, también que la operación es asociativa*
   *por un lado, $(ab)^{-1}.(ab) = e$ pero por otro, si hacemos $(ab).(b^{-1}a^{-1})$ y nos devuelve el neutro,como los inversos son únicos nos quedará que $(ab)^{-1} = b^{-1}a^{-1}$*
   *$(ab).(b^{-1}a^{-1}) = a(b.b^{-1})a^{-1} = a.e.a^{-1} = e$, como queríamos mostrar*

**Teorema 2.1.** *Si* $(G_1, *_1)$, $(G_2, *_2)$, ....., $(G_m, *_m)$ *son grupos, entonces* $G = G_1 \times G_2 \times ..... \times G_m$ *es un grupo con la operación* $*$ *definida por*

$$(a_1, ....a_m) * (b_1, ....b_m) = (a_1 *_1 b_1, ...., a_m *_m b_m)$$

La demostración queda como ejercicio.

**Definición 2.2.** *Un grupo* $G$ *se dice que es* ***cíclico*** *si existe* $a \in G$ *tal que para todo elemento* $b \in G$ *existe un entero* $k$ *tal que* $b = a^k$.
*En este caso decimos que* $a$ *es un* ***generador*** *de* $G$ *y escribimos* $G =< a >$

**Ejemplos 2.3.**

- *El grupo de los números enteros con la suma usual es un grupo cíclico infinito, generado por el número* ***1***
- *Considerando a* $Z_4$ *como el conjunto de las clases de equivalencia de la relación de* congruencia módulo 4 *veremos que* $(Z_4, +)$ *es un grupo cíclico de orden 4 (tiene 4 elementos), generado por* $\overline{1}$.
  *Observar que* $\overline{3}$ *es otro generador, pero por el contrario* $\overline{2}$ *no genera al grupo.*

**Teorema 2.4.** *Todo grupo cíclico es abeliano*

*La demostración queda como ejercicio*

**Definición 2.5.** *Sea* $G$ *un grupo y* $a$ *un elemento de* $G$, *diremos que* $a$ *es de orden finito si existe un* $k$ *natural tal que* $a^k = e$. *En ese caso, definimos el* ***orden de a*** *por* $o(a) = min k \in N : a^k = e$

**Teorema 2.6.** *Grupos cíclicos finitos*
*Si* $G$ *es un grupo cíclico de orden* $m$, *entonces* $G = \{e, a, a^2, ...., a^{m-1}\}$

## 2.1 Subgrupos

**Definición 2.7.** *Dado un grupo $(G, *)$ y dado $H \subset G$, si $(H, *)$ constituye en sí mismo un grupo se dice que es un* ***subgrupo*** *de $G$.*

*Observar que es la misma operación $*$*

**Ejemplo 2.8.** *Sabemos que si sumamos dos números pares obtenemos un número par, entonces podemos pensar que si nuestro grupo son los enteros con la suma usual $(Z, +)$ el subconjunto $H = \{$enteros pares$\}$ ya que además el $0 = 2 \cdot 0$, es decir, tiene neutro y el opuesta (para la suma) de cualquier par es un número par. Obviamente la suma sigue siendo asociativa.*
*Queda para pensar si vale lo mismo para el subconjunto de los enteros impares.*

Como se ve en el ejemplo, al heredar la operación del grupo se heredan sus propiedades. Es decir, la asociatividad de $*$ en $H$ está garantizada pues se cumple para todos los elementos de $G$ , en particular se cumple para los de $H$.
También si $*$ es conmutativa en $G$ será conmutativa en $H$.

Luego, para que H sea subgrupo (o sea, un grupo) sólo será es necesario que:

- $e \in H$, el elemento neutro de $*$ en $G$ debe estar en $H$ (*recordemos que el neutro es único*)
- $a, b \in H \rightarrow a * b \in H$, la operación debe ser cerrada en $H$ (*era cerrada en $G$*)
- $a \in H \rightarrow a^{-1} \in H$, cada elemento de $H$ tiene su inverso en $H$ (*sabemos que el inverso existe pero en $G$, hay que asegurar que esté en $H$*)

Si bien con esta idea ya ahorramos pasos se puede enunciar aún en forma más concisa la condición necesaria y suficiente para que un subconjunto de un grupo resulte un subgrupo del mismo:

**Proposición 2.9.** *Dado un grupo $(G, *)$, un subconjunto $H \subset G$ resultará un subgrupo de $G$ si y sólo si :*

- $e \in H$
- *si* $a, b \in H$ *entonces* $a * b^{-1} \in H$

***Demostración:***

*vamos a usar notación multiplicativa en lugar de $*$ en la demostración* Supongamos primero que $H$ es un subgrupo.
Como es un grupo contiene al neutro, que al ser único debe ser el mismo nuetro de $G$, ya tenemos entonces que $e \in H$.
Ahora probemos la segunda condición, sean $a, b \in H$, como estamos suponiendo que es un subgrupo ambos elementos tendrán su inverso en $H$, en particular $b^{-1} \in H$, luego como la operación es cerrada en el subgrupo, $ab^{-1} \in H$.

Veamos que las condiciones son suficientes. Ya sabemos que4 la asociatividad se cumple en $H$ por cumplirse en $G$. El neutro está en $H$ por la primera condición de la hipótesis. Falta ver que la operación es cerrada en $H$ y que todo elemento tiene a su inverso en $H$ (que ya sabemos que existe y está en $G$) .
Comencemos viendo que todo elemento tiene inverso en $H$. Sea $b \in H$, como por hipótesis $e \in H$ y vale la segunda condición, $eb^{-1} \in H$, pero esto muestra que el inverso de $b$ está en $H$ como queríamos demostrar.
Por último, sean $a, b \in H$, recién mostramos que ambos elementos tendrán a sus inversos en $H$, en particular $b$. Luego tenemos $a$ y $b^{-1}$ en $H$ y como vale la segunda condición, $a(b^{-1})^{-1} \in H$ pero $a(b^{-1})^{-1} = ab$, concluyendo que la operación es cerrada en $H$.

**Teorema 2.10.** *Si $(G, *)$, es un grupo cíclico y $(H, *)$ es un subgrupo de $(G, *)$,entonces $(H, *)$ es cíclico.*