# AMPLIACIÓN DE MATEMÁTICAS

## GRUPOS: DEFINICIÓN Y EJEMPLOS.

La **Teoría de Grupos** tiene muchas aplicaciones desde Cristalografía hasta **Criptografía**, pasando por la resolución de ecuaciones. Nosotros vamos a ver rudimentos de la teoría y algunas aplicaciones a la computación y a la Criptografía.

**Definición 1.** *Un conjunto* $(\mathbb{G}, *)$ *con una operación* $*$*, definida sobre él, se dice que es un*

- ***Grupo*** *si* $(\mathbb{G}, *)$ *tiene las propiedades asociativa, existe un elemento neutro y cada elemento de* $\mathbb{G}$ *tiene un opuesto o inverso.*
- ***Grupo Conmutativo o Abeliano*** *si* $(\mathbb{G}, *)$ *es un grupo y además la operación* $*$ *es* ***conmutativa****.*

*(Ver el Capítulo de Introducción para la definición precisa de cada propiedad).*

**Observación 1.** *El adjetivo Abeliano viene en honor de N.H. Abel (1802-1829), brillante y joven matemático noruego, el cuál uso Grupos para probar que, en general, la ecuación polinómica de grado mayor o igual a 5 no puede resolverse por radicales. Lo que quiere decir que no se puede encontrar una fómula con sumas, productos y raíces de modo que con ellas describamos las soluciones de la ecuación.*

*Abel dá también nombre al premio de matemáticas de mayor cuantía economica que se otorga en el mundo. Claro, lo concede el gobierno noruego.*

**Proposición 1.** *El elemento neutro* $e$ *de un grupo* $(\mathbb{G}, *)$ *así como cada inverso* $g^{-1}$ *de* $g \in \mathbb{G}$ *son únicos.*

***Demostración:***

- Supongamos que $e$ y $e'$ son dos elementos neutros. Entonces

$$e * e' = e' \qquad \text{pero también} \qquad e * e' = e$$

por tanto $e = e'$.

- Si $g_1$ y $g_2$ son dos inversos de $g \in \mathbb{G}$, entonces

$$g_1 * (g * g_2) = g_1 * e = g_1$$
$$(g_1 * g) * g_2 = e * g_2 = g_2,$$

ahora, por la propiedad asociativa, deducimos que $g_1 = g_2 \square$

**Ejemplo 1.** $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$, *y* $(\mathbb{C}, +)$ *forman cuatro grupos abelianos.*

**Ejemplo 2.** *Si* $n \in \mathbb{N}\backslash\{0\}$*, el conjunto de los* ***múltiplos*** *de* $n$

$$n\mathbb{Z} = \{nz \ : \ z \in \mathbb{Z}\}$$

*junto con la suma de enteros,* $(n\mathbb{Z}, +)$*, forma un grupo abeliano.*

**Ejemplo 3.** $(\mathbb{Z}_p\backslash\{0\}, \times)$*,* $p$ *primo,* $(\mathbb{Q}\backslash\{0\}, \times), (\mathbb{R}\backslash\{0\}, \times)$ *y* $(\mathbb{C}\backslash\{0\}, \times)$*, todos ellos son* ***grupos multiplicativos*** *abelianos.*

**Ejemplo 4.** *Sea* $X$ *un conjunto no vacío. Se considera el conjunto de las* ***biyecciones*** *definidas sobre él*

$$S_X = \{f : X \to X \ : \ f \ \text{ es una aplicación biyectiva}\},$$

*junto con la composición de funciones,* $(S_X, \circ)$*, es un grupo (en este caso no necesariamente abeliano).*

En este caso, el elemento neutro es $e = I$ la apliccación **identidad**. Y para cada $f \in S_X$ su función inversa $f^{-1}$ es el elemento inverso respecto de la operación de composición $f \circ f^{-1} = f^{-1} \circ f = I$.

Es fácil contar las biyecciones de un conjunto finito

$$\text{si} \qquad Card\, X = n \qquad \Rightarrow \qquad Card\, S_X = n!$$

Al conjunto $S_X$ se le llama **Grupo Simétrico** o **Grupo de las Permutaciones** de $X$.

**Ejemplo 5.** *Sea $M_{n\times n},\ n>1$, el conjunto de la* ***Matrices Cuadradas*** *de orden n sobre el cuerpo de los números reales $\mathbb{R}$ (o en general sobre cualquier cuerpo $\mathbb{F}$). Consideramos las matrices de determinante no nulo. Así, con respecto al* ***producto*** *de matrices, este conjunto forma un grupo (no Abeliano). Lo notamos por $(GL(n,\mathbb{R}),\times)$ y le damos el nombre de* ***Grupo General Lineal****.*

Si nos acordamos del **Algebra Lineal**, toda **aplicación lineal** $f:\mathbb{R}^n\to\mathbb{R}^n$ venía dada por una matriz $A_f\in M_{n\times n}$ de modo que para cada $\overrightarrow{x}\in\mathbb{R}^n$ se tiene que $f(\overrightarrow{x})=A_f\overrightarrow{x}$.

La matriz de la composición de dos aplicaciones lineales $f$ y $g$ venía dada por el producto de matrices $A_{f\circ g}=A_fA_g$. Además el determinante no nulo de la matriz $|A_f|\neq 0$ es equivalente a que la aplicación $f$ es biyectiva.

Así conectando con el ejemplo anterior, la matriz identidad $I\in(GL(n,\mathbb{R}),\times)$ es el elemento neutro del grupo y para cada $A\in(GL(n,\mathbb{R}),\times)$ su **matriz inversa** es el elemento inverso de $A$ respecto del producto.

**Observación 2.** *Si $X=\mathbb{R}^n$, entonces $GL(n,\mathbb{R})\subset S_X$. Más adelante diremos que el grupo General Lineal es un* ***subgrupo*** *del grupo de biyecciones sobre $\mathbb{R}^n$.*

**Ejemplo 6.** *Sean $X$ un conjunto y $P(X)$ el conjunto de* ***las partes*** *de $X$, es decir el conjunto de todos los subconjuntos de $X$. Sobre $P(X)$ se define la operación $\triangle$ por*

$$\begin{array}{rccl} \triangle\ :\ P(X)\times P(X) & \to & P(x) & \\ (A,B) & \to & A\triangle B & = (A\backslash B)\cup(B\backslash A)=(A\cup B)\backslash(A\cap B). \end{array}$$


FIGURA 1. Diferencia Simétrica.

*Así $(P(x),\triangle)$ es un Grupo Abeliano.*

En este conjunto $P(X)$, el elemento neutro es $e=\emptyset$. Y para cada $A\in P(X)$, él mismo es su inverso. Por otro lado, es fácil determinar

que

$$CardP(X) = 2^{CardX}.$$

**Ejemplo 7.** *Sea $P_n$ un **polígono regular** de $n$ lados, podemos escribir*

$$P_n = \{\sqrt[n]{1}\} = \{e^{\frac{2\pi}{n}ki} \ : \ k = 0, 1, 2, .., n-1\},$$

*teniendo en cuenta solo los vértices. Se considera el conjunto $D_n$ de las **rotaciones** de ángulo $k\frac{2\pi}{n}$ y las **reflexiones** sobre el polígono. Con la composición, $(D_n, \circ)$ es un grupo no abeliano llamado **Grupo Diedral** de grado $n$.*

Tenemos $n$ rotaciones $\begin{cases} a & \text{rotación} \quad \frac{2\pi}{n} \\ a^2 & \text{rotación} \quad 2\frac{2\pi}{n} \\ \vdots & \\ a^n & \text{rotación} \quad n\frac{2\pi}{n}. \end{cases}$ (observemos que $a^n$ es la identidad) y $n$ reflexiones cada una definida respecto de uno de los $n$ ejes de simetría.

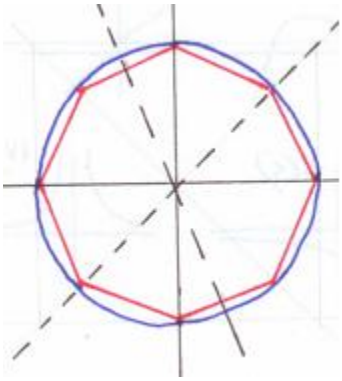

FIGURA 2. Ejes de Simétrica.

Si $b$ es una de estas simetrías, las otras son

$$a \circ b, a^2 \circ b, ....., a^{n-1} \circ b.$$

Por tanto $D_n \subset S_{P_n}$, y en este caso $CardD_n = 2n$.

**Ejemplo 8.** $(\{0\}, +)$ *es un grupo con* $Card\{0\} = 1$.

**Ejemplo 9.** $(\{0, 1, 2, ..., 8, 9\}, +)$ *no forma un grupo ya que no está bien definida la operación ($1 + 9$ no está definida dentro del conjunto).*

**Ejemplo 10.** $(\mathbb{Z}_{10}, +) = (\{[0], [1], ...., [9]\}, +)$ *es, en cambio, un grupo abeliano.*

**Ejemplo 11.** $(\mathbb{Z}, -)$ ***no*** *es un grupo (ya que, por ejemplo,* $3-(7-9) = 5 \neq -13 = (3-7)-9$*).*

**Ejemplo 12.** $(\mathbb{Z}_n^*, \times) = (\{[m] \in \mathbb{Z}_n \ : \ existe\ [m]^{-1}\}, \times)$ *es un grupo conmutativo.*

Esto último lo vimos al estudiar la función de Euler ($\phi(n) = Card\mathbb{Z}_n^*$).

**Definición 2.** *Dado* $(\mathbb{G}, *)$ *un grupo, se llama* ***orden*** *de* $\mathbb{G}$ *(*$|\mathbb{G}|$*) al número de elementos de* $\mathbb{G}$*, es decir*

$$|\mathbb{G}| = Card\mathbb{G}.$$

**Ejemplo 13.**
- *Para* $(2\mathbb{Z}, +)$, $|2\mathbb{Z}| = \infty$.
- *Si* $X = \{1, 2, ..., n\}$*, entonces* $|S_X| = n!$
- $|D_n| = 2n$.

**Definición 3.** *(****Tabla de la Operación****). Dado un grupo* $(\mathbb{G}, *)$ ***finito*** *(e.d.* $|\mathbb{G}| < \infty$*), con*

$$\mathbb{G} = \{g_1, g_2, ..., g_n\}$$

*podemos definir (o escribir) la operación que define al grupo a través de una tabla:*

| $*$ | $g_1$ | $g_2$ | $\cdots$ |
|---|---|---|---|
| $g_1$ | $g_1 * g_1$ | $g_1 * g_2$ | $\cdots$ |
| $g_2$ | $g_2 * g_1$ | $g_2 * g_2$ | |
| $\vdots$ | | | $\cdots$ |
| $\vdots$ | | | $\cdots$ |
| $g_n$ | $g_n * g_1$ | $g_n * g_2$ | $\cdots$ |
| | | | |

| $\cdots$ | $g_n$ |
|---|---|
| | $g_1 * g_n$ |
| | $g_2 * g_n$ |
| | |

| | |
|---|---|
| | |
| | $g_n * g_n$ |
| | |

*donde los "productos"* $g_i * g_j \in \mathbb{G}$.

A través de tablas como éstas es fácil ver donde está el elemento neutro o el inverso de cada elemento; o saber si la operación es conmutativa o no.

**Ejemplo 14.** *Sea* $(P(\{a, b\}, \triangle)$ *las partes de un conjunto de dos elementos con la operación de la diferencia simétrica. Su tabla es*

| $\triangle$ | $\emptyset$ | $\{a\}$ | $\{b\}$ | $\{a,b\}$ |
|---|---|---|---|---|
| $\emptyset$ | $\emptyset$ | $\{a\}$ | $\{b\}$ | $\{a,b\}$ |
| $\{a\}$ | $\{a\}$ | $\emptyset$ | $\{a,b\}$ | $\{b\}$ |
| $\{b\}$ | $\{b\}$ | $\{a,b\}$ | $\emptyset$ | $\{a\}$ |
| $\{a,b\}$ | $\{a,b\}$ | $\{b\}$ | $\{a\}$ | $\emptyset$ |

donde $\emptyset$ indica el conjunto vacío. Éste es claramente el elemento neutro. Como la tabla es **simétrica respecto de la diagonal** la operación es conmutativa. Además es fácil observar que cada elemento de $P(\{a,b\})$ es su propio inverso.

**Ejemplo 15.** *La tabla de* $(\mathbb{Z}_6^*, \times) = (\{[1],[5]\}, \times)$ *es*

| $\times$ | $[1]$ | $[5]$ |
|---|---|---|
| $[1]$ | $[1]$ | $[5]$ |
| $[5]$ | $[5]$ | $[1]$ |

## Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

*E-mail address*: Cesar_Ruiz@mat.ucm.es