



TEMA II: EL GRUPO SIMÉTRICO

OBJETIVOS GENERALES

- 1. Hacer que el alumno asimile el concepto abstracto de estructura algebraica de grupo, y**
- 2. Conocer el grupo simétrico, como ejemplo de grupo no abeliano.**

OBJETIVOS ESPECÍFICOS

- ✓ Saber comprobar si un conjunto con una operación tiene la estructura de grupo.
- ✓ Conocer las propiedades que verifican todo grupo y saber usarlas cuando sea necesario.
- ✓ Conocer cuando un subconjunto de un grupo es un subgrupo y saber probarlo.
- ✓ Conocer la caracterización de subgrupos y saber usarla para probar que un subconjunto de un grupo es o no un subgrupo.
- ✓ Conocer el teorema de Lagrange y saber usarlo para deducir si un subconjunto puede o no ser subgrupo de un grupo.

OBJETIVOS ESPECÍFICOS

- ✓ Asimilar las propiedades fundamentales de grupos de permutaciones
- ✓ Ser capaz de realizar las operaciones básicas con permutaciones
- ✓ Conocer los conceptos de ciclo y trasposición.
- ✓ Saber descomponer una permutación en ciclos disjuntos y en trasposiciones.
- ✓ Ser capaz de calcular el número de inversiones de una permutación.
- ✓ Saber calcular la signatura de una permutación y a partir de esta deducir su paridad.
- ✓ Conocer el subgrupo alternado del grupo de las permutaciones.

BIBLIOGRAFÍA

- **“Métodos computacionales en Álgebra. Matemática discreta: grupos y grafos”. 2ª edición revisada. Ruiz Ruiz, J.F. Servicio de publicaciones de la Universidad de Jaén, 2012 (disponible en línea).**
- **“Elementos de matemática discreta”. Bujalance, E. y otros . Ed. Sanz y Torres, 2001.**
- **“Números, grupos y anillos”. Dorronsoro, J. Ed.: Addison-Wesley: Universidad Autónoma de Madrid, 1999.**
- **“Matemática discreta”. García Merayo, F. Ed.: Thomson-Paraninfo, 2005.**
- **“Matemática discreta”. Fernando J. C. y Gregori, V. Ed.: Reverté, 2012. (disponible en línea).**
- **“Álgebra lineal”. Gutiérrez García, I. y Robinson Evilla, J. Electronic books, 2012. (disponible en línea).**

DESARROLLO TEÓRICO

II.1 Introducción.

II.2 Generalidades sobre grupos.

II.3 Subgrupos.

II.4 Permutaciones, ciclos y trasposiciones.

II.5 Descomposición de una permutación.

II.6 Signatura de una permutación.


II.7 El subgrupo alternado.

1. INTRODUCCIÓN



En este tema estudiamos la estructura algebraica de **grupo**. Aunque ya hemos estudiado otras estructuras algebraicas, quizás la estructura de grupo es con la que se empieza todo estudio del Álgebra abstracta, entre las razones, por que en esta sólo interviene una operación o ley de composición.

Al estudiar estructuras algebraicas tenemos conjuntos cuyos elementos podemos operar algebraicamente, es decir, podemos combinar dos elementos del conjunto, quizás de más de una forma, para obtener otro elemento de dicho conjunto. Además estas operaciones están sujetas a ciertas reglas o propiedades que verifican y que definen la estructura. En dicho marco, se intenta probar teoremas o propiedades de estas estructuras.



Estas estructuras algebraicas y los axiomas que las definen, deben surgir de forma natural de la experiencia que resulta de observar muchos ejemplos. Las estructuras que se estudian, son estudiadas ya que casos particulares de estas estructuras han aparecido una y otra vez, porque algún matemático finalmente, se da cuenta que los ejemplos observados eran realmente casos particulares de un fenómeno general, es decir, tras observar analogías entre objetos matemáticos aparentemente distintos, investiga las raíces de estas similitudes.

A finales del siglo XVIII y comienzos del XIX se estaba estudiando, caso tras caso, distintos ejemplos este objeto que hoy llamamos grupo; sin embargo, no fue sino hasta ya bastante avanzado el siglo XIX cuando se introdujo la noción de grupo abstracto.



La idea de grupo estaba contenida en algunos trabajos matemáticos durante la segunda mitad del siglo XVIII y todo el siglo XIX. Todas ellas se referían a casos particulares de grupos, principalmente **grupos de permutaciones**.

El estudio de la resolución de ecuaciones algebraicas fue el que aglutinó más trabajos y desde donde más tarde germinó las ideas usadas para definir el concepto abstracto de grupo. El matemático que más contribuyó durante el siglo XVIII a este tema fue J.L. Lagrange (1736-1813).

Los trabajos de Lagrange influyeron posteriormente en matemáticos como Ruffini (1765-1822), Abel (1802-1829), y Galois (1811-1832) quien usó por primera vez la palabra grupo.



Finalmente fue, Cayley (1821-1895) quien propuso una definición abstracta de la estructura muy semejante a la que hoy conocemos. Ni sus contemporáneos estaban preparados para manejar una definición tan abstracta, ni Cayley estaba convencido de que fuera necesaria, puesto que él mismo continuó trabajando con las permutaciones

A principios del siglo XX las ideas ya estaban maduras para que una definición abstracta de grupo no ofreciera problemas. Varios matemáticos publicaron artículos durante la primera década de este siglo en donde, con ligeras modificaciones, aparecería el concepto abstracto de grupo tal como nosotros lo definimos. A partir de aquí los matemáticos empezaron a trasladar a este contexto más general las definiciones y los resultados de sus antepasados sobre grupos de permutaciones.

2. GENERALIDADES SOBRE GRUPOS



Un **grupo** es un par $(G, *)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \rightarrow G$ verificando las siguientes propiedades:

- i. Elemento Neutro: Existe $e \in G$ tal que $e * g = g = g * e$ para cada $g \in G$.
- ii. Elemento simétrico: Para cada $g \in G$, existe $g' \in G$ tal que $g * g' = e = g' * g$.
- iii. Asociativa: $(f * g) * h = f * (g * h)$ para cada $f, g, h \in G$.

Se dirá que es un **grupo abeliano** o **conmutativo** si además verifica:

- iv. Conmutativa: $f * g = g * f$ para cada $f, g \in G$.

Ejemplos:

1. $(\mathbb{N}, +)$ no es un grupo.
2. $(\mathbb{Z}, +)$ es un grupo conmutativo.

Ejercicio 1. Comprobar que el conjunto $G = \{2,3,4,5\}$ con la operación dada por la tabla de la derecha es un grupo conmutativo:

*	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

Otros ejemplos son:

1. Al igual que \mathbb{Z} , \mathbb{Q} , \mathbb{R} y \mathbb{C} son grupos aditivos abelianos.
2. \mathbb{Q}^* , \mathbb{R}^* y \mathbb{C}^* son grupos multiplicativos abelianos.
3. $(\mathbb{Z}_n, +)$ es un grupo conmutativo para todo $n \geq 2$.
4. $(\mathbb{Z}_p - \{0\}, \cdot)$, con p primo, es un grupo conmutativo.
5. Sea S un conjunto no vacío, las aplicaciones biyectivas de S en S es un grupo no conmutativo, con la composición.

Ejercicio 2. Comprobar que $(\mathbb{Z}_3, +)$ es un grupo conmutativo.



Si la operación del grupo es la suma, es decir, $(G, +)$ grupo, entonces notaremos al elemento neutro $e = 0$ y al simétrico $a' = -a$ y lo llamaremos **opuesto**.

Si la operación del grupo es el producto, es decir, (G, \cdot) grupo, entonces notaremos al elemento neutro $e = 1$ y al simétrico $a' = a^{-1}$ y lo llamaremos **inverso**.

Proposición 2.1. Sea $(G, *)$ un grupo. Entonces el elemento neutro y el simétrico son únicos.

Ejercicio 3. Comprobar que $\mathbb{R} - \{-1\}$ con la operación $x * y = xy + x + y$ es un grupo conmutativo.



Proposición 2.2. Sea $(G, *)$ un grupo. Entonces se verifica:

1. Si $a * b = e = b * a \Rightarrow a = b'$ y $a' = b$
2. Leyes de cancelación a izquierda y derecha:
 $\forall a, b, c \in G \quad a * b = a * c \Rightarrow b = c \quad \text{y} \quad b * a = c * a \Rightarrow b = c.$
3. Si $a * b = b \Rightarrow a = e$ y $b * a = b \Rightarrow a = e.$
4. $\forall a, b \in G, (a * b)' = b' * a'.$
5. $\forall a \in G, (a')' = a.$

Ejercicio 4. Definir una estructura de grupo conmutativo en el conjunto $G = \{a, b, c\}$ de forma que c es el elemento neutro.

3. SUBGRUPOS



Sea $(G, *)$ un grupo, diremos que un subconjunto no vacío H de G es un **subgrupo** de G si verifica:

1. Si $e \in G$ es el elemento neutro de G entonces $e \in H$.
2. Para cada $a \in H$, su simétrico $a' \in H$.
3. Para cada $a_1, a_2 \in H$, $a_1 * a_2 \in H$, es decir, H es cerrado para la operación $*$.

Obsérvese que en tal caso $(H, *)$ también tiene estructura de grupo.

Proposición 2.3. (Caracterización de subgrupo) Dado $(G, *)$ un grupo, y $H \neq \emptyset$ un subconjunto de G . Entonces:

H es subgrupo de G , si y sólo si, para cada par de elementos $a, b \in H$, entonces $a * b' \in H$, siendo b' es el simétrico de b .

Ejemplos:

1. $\{e\}$ y G son subgrupos improprios de $(G, *)$.
2. \mathbb{N} no es un subgrupo de $(\mathbb{Z}, +)$.

Ejercicio 5. En el grupo conmutativo $G = \{2,3,4,5\}$ con la operación dada por la tabla de la derecha, comprobar si $H_1 = \{2, 3\}$, $H_2 = \{2, 4\}$ y $H_3 = \{2, 5\}$ son subgrupos de G .

*	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

Teorema 2.4. Todos los subgrupos de $(\mathbb{Z}, +)$ son de la forma $n\mathbb{Z}$, para algún $n \geq 0$.

Ejercicio 6. Comprobar que $3\mathbb{Z}$ es un subgrupo de \mathbb{Z} y que \mathbb{Z}^+ no lo es.



Llamaremos **orden** de un grupo $(G, *)$, finito, y lo denotaremos por $|G|$, al número de elementos de G (es decir, el cardinal de G).


Diremos que H es un subgrupo **propio** de G , si $1 < |H| < |G|$. Los únicos subgrupos no propios de G son $\{e\}$ y el mismo G .

Teorema 2.5. (Teorema de Lagrange): Sea $(G, *)$ un grupo finito y H un subgrupo de G . Entonces $|H|$ es un divisor de $|G|$.

El resultado anterior nos evitará comprobar si ciertos subconjuntos son subgrupos de un grupo G , aquellos cuyo cardinal no sea un divisor del cardinal de G .

Ejercicio 7. Calcular todos subgrupo del grupo conmutativo $G = \{2,3,4,5\}$ del ejercicio 1.

4. PERMUTACIONES, CICLOS Y TRASPOSICIONES



Dado un conjunto finito S , a toda aplicación biyectiva de S en S la llamaremos **permutación**. Desde el punto de vista combinatorio, dado un conjunto S de n elementos, llamaremos **permutación simple** (o sin repetición) de n elementos a cada una de las listas que podemos formar que contenga a los n elementos y que cada una difiera de otra únicamente en el orden de colocación de los elementos.

Ejercicio 8. Calcular todas las permutaciones para el conjunto $S = \{1, 2, 3\}$.

Dado el conjunto $S = \{1, 2, \dots, n\}$, llamaremos S_n al conjunto de las permutaciones de n elementos:

$$S_n = \{f: S \rightarrow S / f \text{ es una aplicación biyectiva}\}.$$

Los elementos de S_n habitualmente los escribiremos mediante

$$\sigma \in S_n, \quad \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Ejercicio 8. Calcular todas las permutaciones para el conjunto $S = \{1, 2, 3\}$.

σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$S \rightarrow S$	$S \rightarrow S$	$S \rightarrow S$	$S \rightarrow S$	$S \rightarrow S$	$S \rightarrow S$
$1 \mapsto 1$	$1 \mapsto 1$	$1 \mapsto 2$	$1 \mapsto 2$	$1 \mapsto 3$	$1 \mapsto 3$
$2 \mapsto 2$	$2 \mapsto 3$	$2 \mapsto 1$	$2 \mapsto 3$	$2 \mapsto 1$	$2 \mapsto 2$
$3 \mapsto 3$	$3 \mapsto 2$	$3 \mapsto 3$	$3 \mapsto 1$	$3 \mapsto 2$	$3 \mapsto 1$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



Teorema 2.6. Para cada $n \geq 3$, (S_n, \circ) es un grupo no abeliano al que llamamos **grupo simétrico** y su orden es $|S_n| = n!$.


La operación en este grupo es la composición, por tanto, si $\sigma_k, \sigma_j \in S_n$ entonces la permutación $\sigma_k \sigma_j \in S_n$ vendrá dada para cada $m \in \{1, 2, \dots, n\}$ mediante $\sigma_k \sigma_j (m) = \sigma_k (\sigma_j (m))$.

Ejercicio 9. Calcular la composición $\sigma_2 \sigma_4$ y $\sigma_4 \sigma_2$ de S_3 , y comprobar que S_3 no es un grupo abeliano.

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

Ejercicio 10. Calcular la permutación inversa de σ_5 y σ_6 en S_3 .

Ejercicio 11. Calcular la tabla de operaciones de S_3 .



Una permutación $\sigma \in S_n$ se dirá que es un **ciclo** si existe un subconjunto $\{i_1, i_2, \dots, i_r\} \subseteq S = \{1, 2, \dots, n\}$ para algún $1 \leq r \leq n$, tal que

$$\begin{cases} \sigma(i_j) = i_{j+1} & j = 1, 2, \dots, r-1 \\ \sigma(i_r) = i_1, \\ \sigma(k) = k & k \in S - \{i_1, i_2, \dots, i_r\} \end{cases}$$

La denotaremos por $\sigma = (i_1 \ i_2 \dots i_k)$ y k se dirá que es la **longitud** del ciclo.

Ejercicio 12. Comprobar que la siguiente permutación de $\tau \in S_6$ es un ciclo, ¿de qué longitud?

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 6 & 5 & 3 \end{pmatrix}$$

Llamaremos **trasposición** a todo ciclo de longitud 2.



Proposición 2.7. Si $\tau \in S_n$ es un ciclo de longitud r entonces $\tau^r = \text{Id}$.

Ejercicio 13. Comprobar τ^4 es la permutación identidad, donde $\tau \in S_6$ es el ciclo del ejercicio 12.


Ejercicio 14. Comprobar que $(2\ 3\ 4)(1\ 5\ 6) = (1\ 5\ 6)(2\ 3\ 4)$, es decir, la composición de estos dos ciclos en S_6 satisface la propiedad conmutativa, ¿por qué?

Dos ciclos $(i_1\ i_2\ \dots\ i_k), (j_1\ j_2\ \dots\ j_m) \in S_n$, diremos que son **disjuntos** si $\{i_1\ i_2\ \dots\ i_k\} \cap \{j_1\ j_2\ \dots\ j_m\} = \emptyset$. Es decir, los elementos que mueve cada uno quedan fijos por el otro.

Proposición 2.8. La composición de ciclos disjuntos es conmutativa.



5. DESCOMPOSICIÓN DE UNA PERMUTACIÓN



Teorema 2.9. (Teorema de estructura) Toda permutación de S_n , distinta de la identidad, descompone de forma única, salvo el orden, como composición de ciclos disjuntos.

A la notación anterior la llamaremos **notación cíclica**. Si tenemos un ciclo de longitud 1, este será la aplicación identidad y no aparecerá en la notación cíclica.

Ejercicio 15. Descomponer en ciclos disjuntos la permutación de S_6 :


$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 6 & 1 \end{pmatrix}$$

Un ciclo $\sigma = (i_1 i_2 \dots i_k)$ se puede escribir como composición de trasposiciones como sigue:

$$\sigma = (i_1 i_2 \dots i_k) = (i_1 i_k) \dots (i_1 i_3)(i_1 i_2)$$

o bien,

$$\sigma = (i_1 i_2 \dots i_k) = (i_1 i_2) (i_2 i_3) \dots (i_{k-1} i_k)$$



En ambos casos escribimos el ciclo σ como producto de $k - 1$ trasposiciones, donde k es la longitud del ciclo.


Como consecuencia de lo anterior y del teorema de estructura:

Corolario 2.10. Toda permutación de S_n , distinta de la identidad, descompone como composición de trasposiciones.

Ejercicio 16. Descomponer en trasposiciones las siguientes permutaciones de S_6 .

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 6 & 5 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 6 & 1 \end{pmatrix}$$

6. SIGNATURA DE UNA PERMUTACIÓN



Dada una permutación $\sigma \in S_n$. Diremos que $i, j \in \{1, 2, \dots, n\}$ presentan una **inversión** en σ si y sólo si

$$i < j \text{ y, sin embargo, } \sigma(i) > \sigma(j).$$

Denotaremos por $\gamma(\sigma)$ o $I(\sigma)$ al número de inversiones que hay en σ .


Ejercicio 17. Calcular el número de inversiones de las permutaciones de S_6 del ejercicio anterior.

Llamaremos **signatura** de σ y escribiremos:

$$\text{sign}(\sigma) = (-1)^{\gamma(\sigma)}.$$

Una permutación $\sigma \in S_n$, se dirá que es **par** si el número de inversiones que hay en σ es par, esto es, si $\text{sign}(\sigma) = 1$. De igual forma, $\sigma \in S_n$, se dirá que es **impar** si $\gamma(\sigma)$ es impar, es decir, $\text{sign}(\sigma) = -1$.

Ejercicio 18. ¿Cuál es la signatura de las permutaciones del ejercicio previo? ¿Son pares o impares?



Ejercicio 19. Calcular la signatura de la transposición $\tau = (3\ 6)$ de S_6 y de la composición $\tau\sigma$ donde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 6 & 1 \end{pmatrix}$$

Proposición 2.11. Toda trasposición de S_n es impar.

Lema 2.12. Si τ es una trasposición de S_n , entonces
$$\text{sign}(\tau\sigma) = -\text{sign}(\sigma).$$

Proposición 2.13. Si $\sigma \in S_n$ y $\sigma = \tau_1 \dots \tau_p$ donde τ_i son trasposiciones, entonces $\text{sign}(\sigma) = (-1)^p$.

Lema 2.14. Si $\sigma \in S_n$ y $\sigma = \tau_1 \dots \tau_p = \tau'_1 \dots \tau'_q$ donde τ_i y τ'_j son trasposiciones, entonces p y q tienen la misma paridad.

Proposición 2.15. Si $\sigma, \beta \in S_n$, entonces
$$\text{sign}(\sigma\beta) = \text{sign}(\sigma)\text{sign}(\beta).$$

7. EL SUBGRUPO ALTERNADO



Llamamos subgrupo alternado A_n , al subconjunto de S_n formado por todas las permutaciones pares.

$$A_n = \{\sigma \in S_n / \text{sign}(\sigma) = 1\}$$

Ejercicio 20. Calcular el subgrupo alternado A_3 .

Usando la proposición 2.15 es fácil comprobar el siguiente resultado:

Proposición 2.16. Si σ y τ son dos permutaciones pares entonces $\sigma\tau$, σ^{-1} y τ^{-1} también son permutaciones pares.

Proposición 2.17. A_n es un subgrupo de S_n y $|A_n| = \frac{n!}{2}$