Tema 11.- El grupo de las permutaciones. El grupo alternado

11.1 El grupo S_n

Dado un conjunto A, notamos por S_A el grupo de las biyecciones de A en A con la composición. Si $n \geq 1$ es un número natural, S_n denota el grupo de las biyecciones del conjunto $\{1, \ldots, n\}$ sobre sí mismo. Los elementos de S_n se denominarán *permutaciones*.

PROPOSICIÓN 11.1.1.– Se tienen las siguientes propiedades:

1. S_n es un grupo finito con $|S_n| = n!$.
2. Si $n > 2$ entonces S_n no abeliano.

TEOREMA 11.1.2.– (*Cayley*) Sea G un grupo finito. Existe $n \geq 1$ tal que G es isomorfo a un subgrupo de S_n.

NOTACIÓN 11.1.3.–

1. Para los elementos de S_n se usará la notación usual de aplicaciones, o bien, dada $\sigma \in S_n$ con $\sigma(1) = a_1, \ldots, \sigma(n) = a_n$, se escribirá

$$\sigma \overset{not.}{=} \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

   entendiéndose pues que σ hace corresponder a cada uno de los números que están en la primera fila el que está debajo.

2. Para la multiplicación de permutaciones se usará el mismo convenio (de derecha a izquierda) que para la composición de aplicaciones. Por ejemplo, en S_3

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

DEFINICIÓN 11.1.4.– Un elemento $\sigma \in S_n$ es un *ciclo de longitud* m ($m \leq n$) cuando existe $I = \{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ tal que:

1. $\sigma(a_i) = a_{i+1}$, $\forall i = 1, 2, \ldots, m-1$, $\sigma(a_m) = a_1$.
2. $\sigma(j) = j$, $\forall j \notin I$.

En tal caso, al ciclo σ lo notaremos[1] simplemente por $(a_1 a_2 \ldots a_m)$ y al número m lo llamaremos *longitud del ciclo* σ. Con esta notación se tiene:

$$(a_1 a_2 \ldots a_m) = (a_2 \ldots a_m a_1) = \ldots = (a_m a_1 \ldots a_{m-1}).$$

EJEMPLO 11.1.5.–

[1] Hay que tener en cuenta que esta notación no hace referencia al grupo de permutaciones que estemos considerando.

1. En S_4 un ciclo de longitud 4 es

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

2. En S_4 un ciclo de longitud 3 es

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

PROPOSICIÓN 11.1.6.– El orden de un ciclo σ de longitud m es también m.

DEFINICIÓN 11.1.7.– Diremos que dos ciclos $(a_1 \dots a_m)$ y $(b_1 \dots b_r)$ de S_n son disjuntos si para todos $i,\ j,\ 1 \leq i \leq m,\ 1 \leq j \leq r,\ a_i \neq b_j$.

LEMA 11.1.8.– Sean $\sigma,\ \sigma' \in S_n$ dos ciclos disjuntos. Entonces $\sigma \cdot \sigma' = \sigma' \cdot \sigma$.

TEOREMA 11.1.9.– (*Descomposición en ciclos disjuntos*) Toda permutación de S_n se puede descomponer en un producto de ciclos disjuntos. Esta descomposición es única, salvo el orden de los factores.

PRUEBA: Vamos a probar primero la existencia de la descomposición y luego su unicidad. Sea

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

una permutación arbitraria de S_n. Si $\sigma = 1$, ya está. Supongamos que $\sigma \neq 1$, y sea b un número tal que $\sigma(b) \neq b$. Se construye entonces $\sigma^2(b)$, $\sigma^3(b)$, etc., hasta que, por este procedimiento, se vuelva a obtener b al cabo, digamos, de $i+1$ pasos. Entonces, el ciclo

$$(b \quad \sigma(b) \quad \sigma^2(b) \dots \sigma^i(b))$$

describe parte de la permutación σ. Si el resto de la permutación no contiene números o consta de números que permanecen invariantes, esta demostrado el resultado, pues σ es, entonces, un ciclo. En caso contrario, se repite el procedimiento anterior con ese resto y así sucesivamente. Después de un número finito de pasos se tiene la descomposición.

En cuanto a la unicidad, observemos que dos ciclos disjuntos conmutan. Supongamos que

$$\sigma = \sigma_p \dots \sigma_2 . \sigma_1 = \tau_q \dots \tau_2 . \tau_1$$

fuesen dos descomposiciones de σ en producto de ciclos disjuntos. Sea a_1 un número que no permanece invariante por σ. Es evidente que a_1 debe estar en un ciclo y sólo uno de entre los $\{\sigma_p, \dots, \sigma_2, \sigma_1\}$, y en uno y sólo uno de entre los $\{\tau_q, \dots, \tau_2, \tau_1\}$. Por la conmutatividad se puede suponer que a_1 está en σ_1 y en τ_1. Como los números que aparecen en σ_1 (respec. en τ_1) permanecen invariantes por el resto de los ciclos σ_i (respec. τ_i), el elemento a_1 ha de transformarse en un mismo elemento a_2 mediante σ_1 y mediante τ_1.

Por la misma razón, a_2 debe transformarse en un mismo elemento a_3 mediante σ_1 y τ_1, y así sucesivamente. Esto prueba que $\sigma_1 = \tau_1$. Repitiendo convenientemente este razonamiento, se deduce que $p = q$ y los ciclos σ_i son iguales a los τ_i. □

EJEMPLO 11.1.10.– En S_7 se verifica que:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix} = (135) \cdot (26) \cdot (47).$$

COROLARIO 11.1.11.– El grupo S_n está generado por el conjunto de los ciclos.

COROLARIO 11.1.12.– Sea $\sigma \in S_n$. Sea $\sigma = \sigma_1 \cdot \cdots \cdot \sigma_k$ la descomposición de σ en producto de ciclos disjuntos. Entonces $o(\sigma) = \text{m.c.m}(o(\sigma_1), \ldots, o(\sigma_k))$.

DEFINICIÓN 11.1.13.– Una *trasposición* es un ciclo de orden dos.

TEOREMA 11.1.14.– Toda permutación de S_n, distinta de 1, se puede descomponer como producto de trasposiciones.

PRUEBA: En virtud del teorema anterior, basta probar que todo ciclo de S_n puede ser descompuesto en producto de trasposiciones. Sea, pues, $\sigma = (a_1 a_2 \ldots a_m)$. Es claro que: $\sigma = (a_1 a_2 \ldots a_m) = (a_1 a_m) \ldots (a_1 a_3)(a_1 a_2)$. □

NOTA 11.1.15.– Al contrario que con la descomposición en producto de ciclos disjuntos, la descomposición de una permutación en producto de trasposiciones no es única. Por ejemplo, $(2\ 3) = (1\ 3) \cdot (2\ 3) \cdot (1\ 2)$.

TEOREMA 11.1.16.– La paridad del número de trasposiciones de cualquier descomposición de una permutación $\sigma \in S_n$ como producto de trasposiciones no depende de la descomposición.

PRUEBA: Sea $\varphi : S_n \to \mathbf{GL}(n, \mathbb{R})$ la aplicación que asocia a cada permutación σ la matriz $\sigma(I)$ que se obtiene permutando las filas de la matriz identidad según indica σ. Comprobamos que φ es un homomorfismo de grupos. Es claro que $\det \varphi(\tau) = -1$ siempre que τ sea una trasposición, y por tanto la paridad del número de trasposiciones de cualquier descomposición de σ viene dada por $\det \varphi(\sigma)$. □

DEFINICIÓN 11.1.17.– Para cada $\sigma \in S_n$, el *signo* de σ, $\varepsilon(\sigma)$, está definido por:

$$\varepsilon(\sigma) := (-1)^{(\text{número de trasposiciones de una descomposición cualquiera de } \sigma)} = \det \varphi(\sigma).$$

Una permutación $\sigma \in S_n$ se llama par o impar según que su signo sea 1 ó -1.

Nótese que $\varepsilon : S_n \to \{-1, 1\}$ es un homomorfismo de grupos, donde la operación en el segundo grupo es la dada por la multiplicación usual (se trata de un grupo cíclico de orden 2).

DEFINICIÓN 11.1.18.– Sea σ una permutación de S_n y sean $1 \leq i < j \leq n$ dos enteros. Se dirá que en σ los elementos i y j forman una *inversión* si $\sigma(i) > \sigma(j)$. Al número total de inversiones de σ se le designará por $v(\sigma)$.

Ejemplo 11.1.19.– Sea

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 7 & 6 & 4 & 2 \end{pmatrix}.$$

Se tiene lo siguiente:

a) El 3 forma inversión con el 1 y el 2.

b) El 1 no forma ninguna inversión.

c) El 5 forma inversión con el 4 y el 2.

d) El 7 forma inversión con el 6, con el 4 y el 2.

e) El 6 forma inversión con el 4 y el 2.

f) El 4 forma inversión con el 2.

Luego $v(\sigma) = 10$.

Teorema 11.1.20.– Para cada $\sigma \in S_n$ se verifica que $\varepsilon(\sigma) = (-1)^{v(\sigma)}$.

Prueba: Sea

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Si $a_n = n$ pasamos al siguiente escalón de nuestro razonamiento (i.e. a considerar a_{n-1}). Supongamos que $a_n \neq n$ y que $\sigma(i) = n$, $i < n$. Entonces n forma inversión con todos los que están a su derecha, que son $n - i$. Como es obvio que:

$$\begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n-1 & n \\ a_1 & a_2 & \dots & a_{i+1} & n & \dots & a_{n-1} & a_n \end{pmatrix} =$$

$$\begin{pmatrix} a_{i+1} & n \\ n & a_{i+1} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n-1 & n \\ a_1 & a_2 & \dots & n & a_{i+1} & \dots & a_{n-1} & a_n \end{pmatrix},$$

se ve que, para poner el n debajo del n se necesita multiplicar por $n-i$ trasposiciones (en número igual a las inversiones que forma n). Cuando esto está hecho, el número n ya no forma ninguna inversión, pero como el orden relativo de los demás se conserva, se conservan también las inversiones que formaban antes. En resumen, multiplicando por $n - i$ trasposiciones se logra una permutación del tipo

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ b_1 & b_2 & \dots & b_{n-1} & n \end{pmatrix}$$

que tiene $n - i$ inversiones menos que σ. Aplicando el mismo proceso a $n - 1$, y así sucesivamente, es ya claro que multiplicando σ por un número de trasposiciones igual a $v(\sigma)$ se llega a la permutación unidad. Por tanto $1 = \varepsilon(1) = (-1)^{v(\sigma)}.\varepsilon(\sigma)$ de donde $(-1)^{v(\sigma)} = \varepsilon(\sigma)$. □

11.2 El grupo alternado

DEFINICIÓN 11.2.1.– El subgrupo *alternado* de S_n es

$$A_n := \{\sigma \in S_n : \ \sigma \ \text{ es par}\} = \ker \varepsilon.$$

PROPOSICIÓN 11.2.2.– Dado un subgrupo H de S_n, se verifica una y sólo una de las siguientes propiedades:

1. Toda permutación de H es par, i.e. $H \subset A_n$.
2. H tiene tantas permutaciones pares como impares.

PRUEBA: Supongamos que en H hay permutaciones impares. Todas no pueden ser impares, ya que el producto de dos permutaciones impares en par. Sean $\{\sigma_1, \ldots, \sigma_r\}$ las permutaciones pares de H y $\{\tau_1, \ldots, \tau_s\}$ las permutaciones impares de H. Veamos que $r = s$. El conjunto $\{\sigma_1 \cdot \tau_1, \ldots, \sigma_r \cdot \tau_1\}$ está compuesto por r permutaciones (distintas) impares de H, luego $r \leq s$. Por otro lado, $\{\tau_1 \cdot \tau_1, \ldots, \tau_1 \cdot \tau_s\}$ son permutaciones (distintas) pares de H, luego $s \leq r$, y por tanto se tiene la igualdad. □

PROPOSICIÓN 11.2.3.– $|A_n| = \dfrac{n!}{2}$.