A continuación vamos a estudiar los grupos que históricamente dieron origen a su concepto.

2 Grupos simétricos y alternados

Dado un número natural n el conjunto de permutaciones[1] de $\{1, 2, \ldots, n\}$ es un grupo de orden[2] $n!$, con la operación composición de aplicaciones. Se dice grupo simétrico de grado n y se escribe Σ_n ó por necesidades de *typewritter*S_n. El neutro de este grupo, la aplicación idéntica, se denota como es usual en teoría de grupos mediante 1.

Tres tópicos fundamentales se verán en esta sección: 1) Descomposición única de una permutación en producto de, lo que llamaremos, ciclos disjuntos; 2) Paridad del número de trasposiciones en una permutación, lo que da lugar a la consideración del importante subgrupo alternado: A_n; y 3) Simplicidad de este grupo.

Ejemplo Tomando $n = 3$ son conocidos los siguientes elementos de S_3:

$$\sigma\colon S_3 \longrightarrow S_3 \ni \sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$$

$$\tau\colon S_3 \longrightarrow S_3 \ni \tau(1) = 2, \tau(2) = 1, \tau(3) = 3$$

Notación 2.1 Por razones de escritura la permutación σ dada por $\sigma(k) = i_k$ se representa mediante

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$$

Asimismo suele escribirse en ocasiones σk en lugar de $\sigma(k)$.

Definición 2.2 *Se dice ciclo de longitud $r(> 1)$ r a una permutación σ que deja fijos $n - r$ elementos y que los r elementos restantes se cambian de la manera siguiente:*

$$i_1 \longrightarrow i_2 \longrightarrow \cdots \longrightarrow i_{r-1} \longrightarrow i_r$$

escribimos

$$\sigma = (i_1, i_2, \ldots, i_{r-1}, i_r)$$

El subconjunto $\{i_1, i_2, \ldots, i_{r-1}, i_r\}$ de elementos movidos se dice soporte del ciclo. Se dice trasposición a un ciclo de longitud 2.

Ejemplos y contraejemplos En S_5, (2 1 5) y (3 4) son un ciclo de longitud 3 y una trasposición; sin embargo, (1 2)(3 4) no puede ser un ciclo.

[1] aplicaciones biyectivas

[2] Se tienen n elecciones para el primer lugar, $n - 1$ para el segundo,...

Proposición 2.3 *El orden de un ciclo coincide con su longitud.*
Demostración: Convénzase antes el lector con un ejemplo.
Sea $\sigma = (i_1, i_2, \ldots, i_{r-1}, i_r)$. Entonces,

$$\sigma^r(i_j) = \sigma^j \sigma^{r-j}(i_j) = \sigma^j(i_r) = i_j, \forall j$$

Por tanto, $\sigma^r = 1$ y $o(\sigma) \leq r$. La igualdad se deduce de que si $1 \leq s < r$ entonces, $\sigma^s(i_1) = i_{s+1} \neq i_1$.

Notación 2.4 Dos ciclos se dicen disjuntos si sus soportes lo son.

Ejemplos y contraejemplos En S_5, (215) y (34) son disjuntos; en cambio (23) y (345) no lo son.

Proposición 2.5 *Dos ciclos disjuntos permutan.*
Demostración: Sean σ_A y σ_B dos ciclos de soportes disjuntos A y B. Si k es un índice fuera de ambos soportes queda fijo por ambos ciclos y

$$\sigma_A \circ \sigma_B(k) = k = \sigma_B \circ \sigma_A(k)$$

Por otro lado si $k \in A$, ni $\sigma_A(k)$ ni k son de B y quedan fijos por σ_B. Así,

$$\sigma_A \circ \sigma_B(k) = \sigma_A(k) = \sigma_B \circ \sigma_A(k)$$

El mismo razonamiento aplica a los índices $k \in B$.

Observación 2.6 El orden de escritura de los índices de un ciclo no es único

$$(215) = (152) = (521)$$

Pero

$$(215) \neq (125)$$

En general,

$$(i_1, i_2, \ldots, i_{r-1}, i_r) = (i_2, i_2, \ldots, i_r, i_1) = \cdots = (i_r, i_1, \ldots, i_{r-2}, i_{r-1})$$

Teorema 2.7 *Toda permutación $\sigma \neq 1$ es producto de un número finito de ciclos disjuntos. Además la descomposición es única salvo el orden de los factores.*
Demostración: La demostración de la existencia trata de construir los ciclos correspondientes. Al efecto, sea i_1 un índice en $\{1, \ldots, n\}$ movido por la permutación. La sucesión

$$i_1 \longrightarrow i_2 \longrightarrow \cdots \longrightarrow i_r \longrightarrow \cdots$$

es finita

Paso 1: *El primer índice repetido en la sucesión anterior es i_1.*

En efecto, sean $i_1, i_2, \cdots, i_r$ distintos dos a dos y $\sigma(i_r) = i_k, k \leq r$. Si $k > 1$ $\sigma(i_{k-1}) = i_k = \sigma(i_r)$, luego $i_{k-1} = i_r$ contradicción.

Por tanto, podemos considerar el ciclo $(i_1, i_2, \cdots, i_r)$. Si $r = n$ o los índices restantes quedan fijos, hemos terminado con un ciclo. En caso contrario, sea j_1

un índice restante movido por σ. Razonando como antes encontramos un nuevo ciclo $(j_1, j_2, \cdots, j_s)$. Este proceso puede iterarse hasta agotar los términos que se mueven por σ.
Sean

$$(i_1, i_2, \cdots, i_r), (j_1, j_2, \cdots, j_s), \ldots, (k_1, k_2, \cdots, k_t) \quad (*)$$

los ciclos encontrados.

Paso 2: *Los ciclos encontrados son disjuntos dos a dos.*

En efecto, consideremos los soportes de los ciclos ordenados como aparecen en $(*)$, y sea l_p el primer índice repetido. Por construcción, no puede ser el primer índice de un ciclo; es decir, $p > 1$. Ahora, si l_p es índice de un ciclo anterior $(j_1, j_2, \cdots, j_s)$ l_{p-1} y un j_k dan la misma imagen. Por tanto, l_{p-1} es un índice repetido, contrario a nuestra elección.

Finalmente, es obvio que

$$\sigma = (i_1, i_2, \cdots, i_r)(j_1, j_2, \cdots, j_s) \cdots (k_1, k_2, \cdots, k_t)$$

Unicidad
Sean $c_1 \cdots c_r = d_1 \cdots d_s$ dos descomposiciones de σ en producto de ciclos disjuntos. Razonaremos por inducción sobre el $\min(r, s)$ que $r = s$ y que, salvo el orden de los factores, $c_i = d_i$, $\forall i$
Si dicho mínimo es 1 se tiene $c = d_1 \cdots d_s$. Ahora, por ser disjuntos, es fácil ver que $c = d_i$, para algún i. Como ciclos disjuntos conmutan, podemos suponer $i = 1$; si s fuera mayor que 1, simplificando, la permutación idéntica $1 = d_2 \cdots d_s$ movería los índices de estos ciclos, que es imposible. Necesariamente, $s = 1$.

Supongamos ahora que $\min(r, s) > 1$. Entonces, razonando como antes $c_1 = d_1$ y simplificando $c_2 \cdots c_r = d_2 \cdots d_s$ Por inducción, $r - 1 = s - 1$ y, salvo el orden, $c_j = d_j, j > 2$.

Ejemplo

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

Corolario 2.8 *El orden de* $\sigma = (i_1, i_2, \cdots, i_r)(j_1, j_2, \cdots, j_s) \cdots (k_1, k_2, \cdots, k_t)$ *es el* mcm *de* $(r, s, \ldots, t)$.
Demostración: Sencilla pues los ciclos disjuntos conmutan y la potencia de un ciclo no mueve cifras fuera de su soporte.

Ejemplo En S_7 el orden de $\begin{pmatrix} 2 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix}$ es 6.

Teorema 2.9 *Toda permutación no idéntica es producto de un número finito de transposiciones. La paridad de dicho número es fija.*
Demostración: El primer item es inmediato toda vez que, por ejemplo

$$\begin{pmatrix} 2 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 3 \end{pmatrix}$$

En general, para cada ciclo de longitud r se tiene la descomposición

$$(i_1, i_2, \cdots, i_r) = (i_1, i_2)(i_2, i_3)\cdots(i_{r-2}, i_{r-1})(i_{r-1}, i_r)$$

El *percal* reside en la *paridad* del número de factores. Queremos decir que una permutación puede ser producto de $2, 4, 6, 8, \ldots$ o de $1, 3, 5, 7, 9, \ldots$ transposiciones, pero no hay ninguna permutación que sea producto, a la vez, de 2 y 3 trasposiciones. En esto reside el hecho de que el cubo de Rubik se pueda hacer, y que si se *descuajeringa* a mano y luego se monta, quizá ya no se puede hacer.

Comencemos la demostración. Se trata de observar el efecto de una trasposición sobre una permutación cualquiera. Se distinguen dos casos:

Paso 1: La trasposición mueve dos índices de un ciclo.

1. $(k, h)(k, i_1, \cdots, i_r, h, j_1, \cdots, j_s) = (h, j_1, \cdots, j_s)(k, i_1, \cdots, i_r)$
2. $(k, h)(k, i_1, \cdots, i_r, h) = (k, i_1, \cdots, i_r)$
3. $(k, h)(k, h) = 1$

igualdades que se deducen por observación directa.

Paso 2: La trasposición mueve índices de ciclos distintos.

1. $(k, h)(h, j_1, \cdots, j_s)(k, i_1, \cdots, i_r) = (k, i_1, \cdots, i_r, h, j_1, \cdots, j_s)$
2. $(k, h)(k, i_1, \cdots, i_r) = (k, i_1, \cdots, i_r, h)$

igualdades que se deducen de las anteriores premultiplicando por (k, h).

Para cada permutación σ, sea $N(\sigma)$ la suma de las longitudes de sus ciclos menos el número de éstos, y pongamos $N(1) = 0$.

Paso 3: *Si τ es una trasposición, $N(\tau\sigma) = N(\sigma) \pm 1$.*

En efecto, si τ no mueve los índices de los ciclos de σ, en la ciclo-descomposición de $\tau\sigma$ aparece una trasposición más, luego $N(\tau\sigma) = N(\sigma) + 2 - 1 = N(\sigma) + 1$.
Si τ mueve sólo un índice de los ciclos de σ, estamos en la fórmula 2.2, luego $N(\tau\sigma) = N(\sigma) + 1$.
Si τ mueve los índices de ciclos diferentes de σ, estamos en la fórmula 2.1, luego $N(\tau\sigma) = N(\sigma) + 1$.
Finalmente, si τ mueve dos índices de un ciclo de σ, estamos en las fórmulas del paso 1, luego $N(\tau\sigma) = N(\sigma) - 1$.

Paso 4: *Si σ es producto de m trasposiciones, las paridades de m y $N(\sigma)$ coinciden.*

Razonaremos por inducción sobre m; para $m = 1$

$$\sigma = \tau \quad N(\sigma) = N(\tau) = 2 - 1 = 1 = m$$

Si $m > 1$, $\sigma = \tau\omega$ donde ω es producto de $m-1$ trasposiciones. Así, $N(\sigma) = N(\omega) \pm 1$; por inducción $N(\omega)$ tiene la misma paridad que $m-1$, luego $N(\sigma) = N(\omega) \pm 1$ tiene la misma paridad que m.

Puesto que $N(\sigma)$ queda determinado por σ, la paridad del número de trasposiciones en que se descompone una permutación depende exclusivamente de ésta.

Definición 2.10 *Sea σ producto de m trasposiciones. Entonces,*
i) *Si m es par, σ se dice par; en caso contrario, impar*
ii) *Se dice signatura de σ a $(-1)^m$.*

Observación 2.11 La permutación idéntica se considera par y su signatura se define como 1.

Ejemplos Toda trasposición es impar. Un ciclo de longitud r tiene signatura $(-1)^{r-1}$. La permutación

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

es impar (de signatura -1).

Observación 2.12 El producto de dos trasposiciones (impares) es una permutación par, luego no es un subconjunto cerrado para la multiplicación; bien al contario, el conjunto de permutaciones pares es un subgrupo normal de S_n como lo muestra el siguiente

Teorema 2.13 *La correspondencia $\epsilon: S_n \longrightarrow \{1, -1\}$ dada por $\epsilon(\sigma) = 1$ si σ es par y -1 en caso contrario, es un epimorfismo de grupos. Su núcleo, el conjunto de permutaciones pares, se designa A_n y recibe el nombre de grupo alternado de grado n.*
En lugar de $\epsilon(\sigma)$ suele escribirse ϵ_σ.
Demostración: De acuerdo con el teorema anterior ϵ es aplicación. Sean σ_i producto de m_i trasposiciones. Entonces,

$$\epsilon(\sigma_1\sigma_2) = (-1)^{m_1+m_2} = (-1)^{m_1}(-1)^{m_2} = \epsilon(\sigma_1)\epsilon(\sigma_2)$$

Observación 2.14 Nótese que $|S_n/A_n| = 2$; es decir, se trata de un subgrupo de índice 2. El grupo alternado adquiere relieve por no poseer subgrupos normales propios, para $n \geq 5$; entre otras consecuencias, este hecho dará carpetazo definitivo al secular intento de resolver la ecuación general de grado n. Tal simplicidad es nuestro próximo objetivo.

2.1 Simplicidad de A_n

Lema 2.1.1 *$A_n, (n \geq 3)$ está generado por los ciclos de longitud 3.*

Demostración: Puesto que A_3 es cíclico de orden 3, podemos suponer $n > 3$. Ahora toda permutación par es producto de un número par de trasposiciones. Agrupando de 2 en 2, cada pareja mueve cuatro índices o tres. Ahora bien

$$(a,b)(c,d) = (a,c,b)(a,c,d) \quad (a,b)(a,c) = (acb)$$

son producto de ciclos de longitud 3.

Lema 2.1.2 *Si $A_n, (n \geq 5)$ posee un subgrupo normal N con un 3-ciclo, $N = A_n$.*
Demostración: Veremos que N contiene cualquier 3-ciclo. Al efecto, sea $(a,b,c) \in N$ e (i,j,k) otro 3-ciclo. Sea $\sigma(a) = i, \sigma(b) = j, \sigma(c) = k, \ldots$. Entonces,

$$\sigma(a,b,c)\sigma^{-1} = (i,j,k)$$

Si σ es par $(i,j,k) \in N$; en caso contrario, sea $\alpha = (l,m)$ $l, m \notin \{i,j,k\}$; entonces $\alpha\sigma$ es par y

$$\alpha\sigma(a,b,c)\sigma^{-1}\alpha^{-1} = (i,j,k)$$

Observación 2.1.3 El resultado anterior es obvio para $n = 3$. El grupo alternado de grado 4 será estudiado en detalle en los ejercicios, comprobando entonces que también satisface el lema anterior.

Teorema 2.1.4 *$A_n, (n \geq 5)$ es simple.*
Demostración: Veremos que todo subgrupo normal $1 \neq N$ de A_n posee un 3-ciclo. Un tal 3-ciclo será la permutación de N con la máxima cantidad de índices fijos. Esta es nuestra estrategia.

Sea α una permutación no idéntica de N con una cantidad de índices fijos máxima.

Si α no es un 3-ciclo vamos a construir una permutación no idéntica que fija más índices que α. La descomposición de ciclos disjuntos de α cumple una de:

1. Existe un ciclo de longitud $\geq 5 : (i_1, \ldots, i_5, \ldots) \cdots$
2. Existe un ciclo de longitud 4 y, por paridad, una trasposición u otro 4-ciclo:
$$(i_1, \ldots, i_4)(i_5, i_6, \ldots) \cdots$$
3. Existen dos ciclos de longitud $3 : (i_1, i_2, i_3)(i_4, i_5, i_6) \cdots$
4. Sólo existe un 3-ciclo y, por reduccción al absurdo, dos trasposiciones (al menos):
$$(i_1, i_2, i_3)(i_4, i_5)(i_6, i_7) \cdots$$
5. Sólo existen trasposiciones (dos al menos):$(i_1, i_2)(i_3, i_4) \cdots$

En el último caso α mueve al menos 4 índices $\{i_1, \ldots, i_4\}$ y, en los 4 primeros, α mueve uno más i_5. Sea $\beta = (i_3, i_4, i_5)$; entonces, $\beta\alpha\beta^{-1} \neq \alpha$ y $\sigma = \beta\alpha\beta^{-1}\alpha^{-1} \neq 1$

La permutación σ será nuestra candidata. Cualquier índice i_k, $k > 5$ es fijo por β; luego los fijados por α también quedan fijos por σ. Asimismo, $\sigma(i_2) = i_2$.

En los cuatro primeros casos, los posibles índices fijados por α son $i_k, k > 5$, luego σ fija uno más, por lo menos; y, en el último caso, los posibles índices fijados por α son $i_k, k \geq 5$; el i_5 se compensaría, en su caso, con el i_2 y como $\sigma(i_1) = i_1$, σ fija un índice más que α.

EJERCICIOS

1. Descomponer en producto de ciclos disjuntos
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 6 & 5 \end{pmatrix}$$
2. Sea $G \leq S_n, 1 \leq j \leq n$. Probar que
$$G_j = \{\sigma \in G \mid \sigma(j) = j\}$$
es un subrupo de G, que recibe el nombre de estabilizador de j en G.
3. Sea $G \leq S_n$. Probar que $j \sim k \iff \exists \sigma \in G$ con $\sigma(j) = k$ es una relación de equivalencia en $\{1, \ldots, n\}$. Designando Gj la clase de equivalencia $[j]$, probar asimismo que $[G : G_j] = \#Gj$.
4. Probar que $\sigma(i_1, i_2, \ldots, i_r)\sigma^{-1} = (\sigma i_1, \sigma i_2 \ldots, \sigma i_r)$
5. Se dice tipo de una permutación a la familia de las longitudes de sus ciclos. Probar que dos permutaciones son conjugadas si y sólo si son del mismo tipo.
6. Este ejercicio está destinado a probar que A_4 es un grupo de orden 12 que no posee subgrupos de orden 6.
   (a) Probar que los elementos del grupo A_4 son ciclos de longitud 3 o productos de dos trasposiciones
   (b) Probar que un subconjunto de orden 6 de A_4 contiene necesariamente un ciclo de longitud 3.
   (c) Probar que un subgrupo de orden 6 de A_4 contiene necesariamente un producto de trasposiciones disjuntas.
   (d) Probar que si un subgrupo de A_4 es de orden 6 el subgrupo generado por su 3-ciclo es normal en él.
   (e) Probar que el conjugado de un 3-ciclo por un par de trasposiciones de A_4 es un 3-ciclo de soporte diferente.
   (f) Deducir que el grupo A_4 no posee subgrupos de orden 6, por lo que el recíproco del teorema de Lagrange es falso.
7. Describir los subgrupos de A_4 indicando cuáles son normales y cuáles no.
8. Utilizando $(k, j) = (1, k)(1, j)(1, k)$ probar que S_n está generado por las trasposiciones $(1, 2), (1, 3), \ldots, (1, n)$
9. Utilizando $(1, k + 1) = (k, k + 1)(1, k)(k, k + 1)$ probar que S_n está generado por las trasposiciones $(1, 2), (2, 3), \ldots, (n - 1, n)$
10. Probar que dada una matriz A de orden n,
$$\det A = \sum_{\sigma \in S_n} \epsilon_\sigma a_1^{\sigma 1} \cdots a_n^{\sigma n}$$