INTRODUCCIÓN A LAS PERMUTACIONES

1. Ciclos y clases de conjugación

Hemos visto que un d-ciclo es un elemento de S_n de la forma

$$c = (a_1 a_2 \dots a_d)$$

con $a_j \in \{1, 2, \dots, n\}$ y que el orden de cualquier d-ciclo es d.

También hemos visto que podemos expresar cualquier permutación de S_n de forma única como producto de ciclos *disjuntos*, es decir

$$\sigma = c_1 c_2 \dots c_l$$

donde c_j mueve ciertos elementos que no mueve ninguna de las otros ciclos c_k. También podemos ver que el *orden* de σ es el *mínimo cómun múltiplo de las longitudes sus ciclos disjuntos* c_j, ya que

$$\sigma^m = c_1^m c_2^m \dots c_l^m. \tag{1.1}$$

Así, imaginad que queremos buscar una manera de barajar 10 cartas σ que sea complicada en el sentido de que la tengamos que repetir muchas veces para que las cartas vuelvan a estar ordenadas. Como las longitudes de los ciclos de σ deben sumar 10, podemos comprobar que la mejor opción es coger σ por ejemplo

$$\sigma = (12)(345)(6789\,10),$$

que habrá que repetirla $2 * 3 * 5 = 30$ veces, debido a (**??**).

Ahora queremos ver cómo son las clases de conjugación de S_n. Para $\mathrm{SL}(2, K)$ dijimos que era posible ver si dos matrices eran conjugadas simplemente mirando a su traza; buscamos una caracterización de ese estilo para S_n. Para ello, nuestra fórmula básica va a ser

$$g(a_1 a_2 \dots a_d) g^{-1} = (g(a_1) g(a_2) \dots g(a_d)), \tag{1.2}$$

es decir, al conjugar un d-ciclo c por $g \in S_n$ aparece otro d-ciclo con coefcientes las imágenes por g de los coeficientes de c. Esto quiere decir que un conjugado de un d-ciclo sólo puede ser un d-ciclo. Pero además, cualesquiera dos d-ciclos son conjugados. Si los d-ciclos son $(a_1 \dots a_d)$ y $(b_1 \dots b_d)$, entonces escogiendo cualquier permutación g que satisfaga $g(a_i) = b_i$, por (**??**) tendría que

$$g(a_1 \dots a_d) g^{-1} = (b_1 \dots b_d).$$

Así, los d-ciclos forman una clase de conjugación para cualquier d. Esto se puede extender a cualquier producto de ciclos disjuntos, y así tenemos que

Lema 1.1 (Clases de conjugación en S_n)**.** *Dos permutaciones de S_n son conjugadas si y sólo si en su expresión en producto de ciclos disjuntos las longitudes de los ciclos coinciden.*

Así, (123) y (241) serían conjugados en S_5, pero (12)(34) y (13)(452) no lo serían. En S_4 tenemos las siguientes clases de conjugación:

- 4-ciclos (6 elementos).
- 3-ciclos (8 elementos).
- 2-ciclos (6 elementos).
- 2-ciclos $\times$ 2-ciclos (3 elementos).
- La identidad (1 elemento).

Si nos piden buscar el cambio de base para escribir (154)(23) como conjugado de (132)(45), tendríamos que buscar g para que

$$g(132)(45)g^{-1} = (g(1)g(3)g(2))(g(4)g(5)) = (154)(23).$$

Así, si tomamos $g(1) = 1$, $g(3) = 5$, $g(2) = 4$, $g(4) = 2$, $g(5) = 3$ funciona. Como producto de ciclos $g = (24)(35)$.

2. Trasposiciones

Decimos que una permutación es una *trasposición* si sólo intercambia dos elementos de $\{1, 2, \dots, n\}$. Es decir, si envía i a j y j a i. Podemos escribir esa permutación como el ciclo

$$(ij)$$

y de hecho vemos que las trasposiciones son exactamente los dos ciclos. Podemos verlas como las permutaciones más simples. Por otra parte, es muy sencillo ver que podemos construir cualquier permutación a base de trasposiciones, es decir que *las trasposiciones generan S_n.*

Podemos ver un elemento de $\sigma \in S_n$ como una manera de desordenar una lista de n elementos, en el sentido de que envía el elemento en la posición i-ésima a la posición $\sigma(i)$-ésima. Es decir

$$x_1x_2 \dots x_n \mapsto x_{\sigma^{-1}(1)}x_{\sigma^{-1}(2)} \dots x_{\sigma^{-1}(n)}.$$

Para ver que las trasposiciones generan S_n sólo hay que darse cuenta de que podemos desordenar una lista haciendo sucesivos cambios de dos elementos. Por ejemplo si queremos reproducir la permutación

$$abcde \mapsto debac$$

hacemos

$$abcde \mapsto dbcae \mapsto decab \mapsto debac$$

que escrito en forma de ciclos es

$$(14)(235) = (35)(25)(14)$$

Así, si queremos ver como trasposiciones el ciclo $\sigma = (d, d-1, \dots 3, 2, 1)$, vemos que su efecto es que todos se mueven una posición a la izquierda, es decir

$$x_1x_2x_3x_4 \dots x_{d-1}x_d \mapsto x_2x_3x_4x_5 \dots x_dx_1$$

y para reproducirlo hacemos

$$x_1x_2x_3x_4 \dots \mapsto x_2x_1x_3x_4 \dots \mapsto x_2x_3x_1x_4 \dots \mapsto x_2x_3x_4x_1 \dots$$

que escrito con ciclos queda

$$(d, d-1, \dots 3, 2, 1) = (d, d-1) \dots (43)(32)(21).$$

Una vez demostrado esto, vemos que en general debe quedar

$$(a_da_{d-1} \dots a_3a_2a_1) = (a_da_{d-1}) \dots (a_3a_2)(a_2a_1)$$

por lo que los d-ciclos se pueden construir con trasposiciones, y por eso lo mismo ocurre con productos de ciclos.

3. Subgrupo Alternado

Sabemos que $\mathrm{O}(d, \mathbb{R})$ tiene un subgrupo especial de índice 2, que consiste en las aplicaciones ortogonales que preservan la orientación, es decir cuyo determinante es positivo. Dicho subgrupo es $\mathrm{SO}(d, \mathbb{R})$, ya que una matriz ortogonal tiene determinante 1 o -1. En el caso $d = 2$, identificamos los elementos de $\mathrm{SO}(2, \mathbb{R})$ con giros, y los que están fuera con reflexiones. Igualmente, vamos a ver que tenemos un subgrupo especial de índice 2 en S_n. Vamos a descubrirlo viendo las permutaciones como aplicaciones ortogonales. Definimos el encaje

$$\phi : S_n \to \mathrm{O}(n, \mathbb{R})$$

mediante $\phi(\sigma) = \phi_\sigma$ con ϕ_σ la aplicación lineal que envía el vector e_i de la base estándar de $\mathbb{R}^n$ a $e_{\sigma(i)}$, es decir $\phi_\sigma(e_i) = e_{\sigma(i)}$. Claramente, ϕ_σ es ortogonal, porque no ha cambiado la norma de los vectores de la base. De hecho, viendo ϕ_σ como matriz tenemos

$$\phi_\sigma = (e_{\sigma(1)}, e_{\sigma(2)}, \dots, e_{\sigma(n)}),$$

donde estoy poniendo dicho vectores como columnas. Como

$$\phi_\sigma(\phi_\tau(e_i)) = e_{\sigma(\tau(e_i))} = \phi_{\sigma\tau}(e_i)$$

vemos que ϕ es un homomorfismo, luego claramente es un encaje. Así, en el caso $n = 3$, ϕ envía

$$(123) \mapsto (e_3 e_1 e_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Fijaos en que estamos diciendo que S_n es isomorfo a cierto subgrupo de $\mathrm{O}(n, \mathbb{R})$ (y lo mismo podría haber hecho cambiando $\mathbb{R}$ por $\mathbb{C}$ o $\mathbb{Z}_p$). Esto nos permite olvidarnos de las permutaciones y trabajar sólo con matrices, en el caso de que nos gusten más las matrices. En todo caso, definimos el *subgrupo alternado* A_n de S_n como

$$A_n = \phi^{-1}(\mathrm{SO}(n, \mathbb{R})),$$

es decir, como la permutación que son enviadas por ϕ a matrices que preservan la orientación (con determinante 1). Otra manera de verlo, si definimos

$$\det : \mathrm{O}(n, \mathbb{R}) \to \{-1, 1\}$$

el homomorfismo que envía una matriz a su determinante, tenemos que

$$A_n = \ker(\det \phi).$$

Por tanto, A_n es un subgrupo de S_n de índice 2. Veamos que de forma explícita que permutaciones están en él. Como sabemos que las trasposiciones generan S_n, es suficiente ver si están o no en A_n. Como

$$(12) \mapsto (e_2 e_1 e_3 e_4 \ldots e_n),$$
$$\det(e_2 e_1 e_3 e_4 \ldots e_n) = -\det I = -1$$

luego vemos que $\det \phi(12) = -1$ y por tanto $(12) \notin A_n$. Además, como cualquier otra trasposición es conjugada a (12), tenemos que

$$\det \phi(ij) = \det \phi g(12)g^{-1} = -(\det \phi g)^2 = -1,$$

por propiedades de los determinantes o por cálculo directo, luego cualquier trasposición va a parar al -1. Así, tenemos que $\sigma \in A_n$ precisamente cuando puede escribirse como un número par de trasposiciones. Es decir A_n *son las permutaciones que se pueden escribir como un número par de trasposiciones.* Por eso a los elementos de A_n se les llaman *permutaciones pares*, y al homomorfismo $\det \phi$ se le llama *signo.*

Como un d-ciclo puede ponerse como $d + 1$ trasposiciones, tenemos que un d-ciclo está en A_n si y sólo si d es impar. Además, como

$$(ij)(jk) = (ijk) \qquad (ij)(kl) = (ijk)(jkl)$$

tenemos que A_n también es *el subgrupo de A_n generado por los 3-ciclos.*

Finalmente, usando las clases de conjugación de S_n veremos en los problemas que A_n es un grupo simple si $n \geq 5$.