ÓRBITAS Y ESTABILIZADORES

1. Objetivos

Si X es un conjunto cualquier, hemos definido el *grupo simétrico de* X como el grupo de todas la permutaciones de X,

$$\mathrm{Sym}(X) = S_X = \{f : X \to X : f \text{ biyección } \}.$$

con la operación composición de funciones. Si dos conjuntos X e Y tienen el mismo cardinal, entonces $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$. En particular, si $|X| = n$ tenemos que $\mathrm{Sym}(X) \cong S_n$ que es el grupo simétrico de $\{1, 2, \dots, n\}$.

Muchas veces, X viene acompañado de cierta estructura que nos interesa comprender, y para comprenderla una herramienta muy útil suele ser fijarnos en el subgrupo G de $\mathrm{Sym}(X)$ que deja fija dicha estructura.

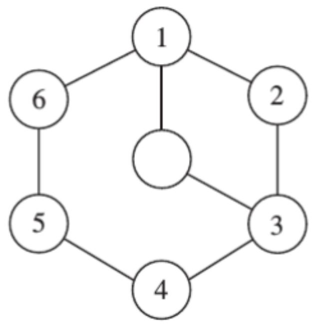
Así, nos va a interesar saber calcular subgrupos de $\mathrm{Sym}(X)$. Por eso, vamos a decir que un grupo G es un *grupo de permutaciones* si es un subgrupo de $\mathrm{Sym}(X)$.

El estudio de dichos grupos tiene apliación en problemas de álgebra, geometría, teoría de números, física, etc. Nosotros vamos a ver su aplicación a un caso más sencillo: resolver puzles. De hecho, ya vimos en el capítulo A1 el ejemplo del cubo de Rubik modificado, cuyo grupo asociado era

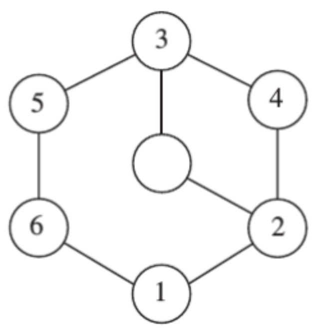
$$G = \langle r, b, u \rangle \leq S_7$$

con $r = (2543)$, $b = (4567)$ y $u = (1652)$. Pasar de una determinada posición a la inicial es equivalente a ver que el movimiento correspondiente está en G y a expresarlo como una palabra en r, b, u.

Ahora vamos a fijarnos en un ejemplo más sencillo sacado del libro de la bibliografía *Contemporary Mathematics*. Partimos de la posición original



y podemos mover discos contiguos a cualquier lugar que quede vacío. Entonces, podemos plantearnos si es posible llegar a la siguiente posición,



llamémosla m, y si es posible cómo hacerlo.

Si sólo nos intersan las posiciones donde el disco del centro queda libre, podemos ver los movimientos como elementos de S_6. De hecho, podemos ver cuál es el grupo G de todos los movimientos.

Una posibilidad es mover el número que está en la posición 1 al centro, luego desplazar todos los de las posiciones del 3 al 6 en dirección de las agujas del reloj, y finalmente el 1 al hueco que queda. Dicho movimiento es

$$r = (13456).$$

Si en vez de usar el 6 para llenar el hueco usamos el 2, tenemos el movimiento

$$s = (132).$$

Si comenzamos metendo el de la posición 3 al medio, tendríamos los movimientos (231) y (65431), que son los inversos de s y r respectivamente, por lo que

$$G = \langle r, s \rangle \leq S_6.$$

La posición m corresponde al movimiento (desde la posición inicial)

$$m = (1423)(56).$$

Así, nuestra pregunta inicial se reduce a ver si $m \in G$ y cómo escribirlo en términos de r y s.

2. Órbitas

Una de las herramientas que nos va a ayudar a ver cómo es un grupo de permutaciones $G \leq S_X$ son las órbitas de elementos.

Si $Y \subset X$, decimos que Y es un subconjunto G-invariante si $G(Y) = Y$ como conjuntos. Si es así, tenemos que $G(Y^c) = Y^c$, luego podemos partir X en dos subconjuntos G-invariantes disjuntos $X = Y \cup Y^c$. Si encontramos otro conjunto $Z \subset Y$ G-invariante podríamos encontrar una partición de X más fina en conjuntos G-invariantes.

Este procedimiento es similar al que haríamos con subespacios invariantes por aplicaciones lineales. De hecho, también podemos decir que un subconjunto G-invariante $Y \subset X$ es *irreducible* si no puede partirse en dos subconjuntos no triviales G-invariantes.

Cualquier subconjuto G-invariante Y tiene algún suconjunto irreducible. De hecho si $y \in Y$, el mínimo conjunto G-invariante que contiene a y es

$$\mathrm{Orb}_G(y) = \{g(y) \in X : g \in G\},$$

lo que se llama la *órbita* de y por G.

Por tanto, vemos que los subonjuntos G-invariantes irreducibles son justamente las órbitas de elementos de X. Por tanto, tenemos la partición de X en subconjuntos G-invariantes irreducibles

$$X = \cup_{Y \text{inv. irr} \subset X} Y = \cup_{Y \text{órbita por } G} Y.$$

En el caso de que X sea finito, mirando a los tamaños obtenemos la correspondiente *ecuación de órbitas*

$$|X| = \sum_{Y \text{órbita por } G} |Y|.$$

Si consideramos $G = \langle g \rangle \leq S_n$, vemos que las órbitas de G son los subconjuntos más pequeños invariantes por g. Por ejemplo, si $G = \langle (167)(24)(3)(5) \leq S_7$, tenemos que las órbitas de G son

$$\{1, 6, 7\}, \{2, 4\}, \{3\}, \{5\}$$

De hecho, vemos que si $G = \langle g \rangle$, las órbitas de G se corresponden con la expresión de g como producto de ciclos disjuntos.

Si $G = \langle g, h\rangle$, entonces las órbitas de G deben ser invariantes por g y h, luego van a ser unión de órbitas de g y también de h. Si por ejemplo

$$G = \langle g = (167)(24), h = (235)\rangle,$$

tenemos que las órbitas van a ser unión de órbitas de $\langle g\rangle$. Vemos que en la órbita de 2 deben estar el 3 y el 5, luego las órbitas de G quedan

$$\{1, 6, 7\}, \{2, 3, 4, 5\}.$$

Vemos que en general las órbitas de G son muy sencillas de obtener y que nos dan cierta información del grupo G.

3. Estabilizadores

Vamos a comenzar haciendo para las órbitas lo mismo que hicimos en el caso de clases de conjungación: ver cómo contar de forma teórica el número de elementos que hay en una órbita $\mathrm{Orb}_G(x)$.

Para eso, la idea es que si un elemento $g \in G$ fija x, es decir $g(x) = x$, entonces g no da nuevos elementos en la órbita de x. Eso motiva fijarnos en el subconjunto de elementos de G que fijan x, el llamado *estabilizador* de x:

$$G_x = \mathrm{Stab}_G(x) = \{g \in G : g(x) = x\}.$$

Es inmediato comprobar que el estabilizador siempre es un subgrupo de G, es decir $G_x \leq G$.

Si tenemos cualquier par de elementos $y_1 = f_1(x)$, $y_2 = f_2(x)$ en la órbita de x (es decir, con $f_1, f_2 \in G$), entonces si $y_2 = y_1$ equivale a que $f_1(x) = f_2(x)$, o lo que es lo mismo $x = f_1^{-1}f_2(x)$, es decir $f_1^{-1}f_2 \in G_x$. Pero esto lo podemos reescribir como

$$f_2 = f_1 g \qquad g \in G_x.$$

Esto no da una biyección del conjunto cociente G/G_x y $\mathrm{Orb}_G(x)$, dada por $fG_x \mapsto f(x)$. Es decir, tenemos

$$|\mathrm{Orb}_G(x)| = |G/G_x|.$$

En particular, en el caso de que G sea finito, tenemos que *el tamaño de las órbitas divide al orden del grupo*, algo que ya obtuvimos en el caso de las clases de conjugación.

Veamos que esta información es muy útil para comprender G. Por ejemplo, miremos al grupo

$$G = \langle (123), (12)(34)\rangle \leq S_4.$$

Por Lagrange, sabemos que $6 \mid |G| \mid 24$, luego el tamaño de G podría ser 6, 12 o 24. Si calculamos las órbitas de G vemos que hay una única órbita

$$\{1, 2, 3, 4\},$$

luego obtenemos que $4 \mid |G|$, y por tanto vemos que sólo quedan las posibilidades 12 y 24. Finalmente, como G está generado por permutaciones pares, tenemos que $G \leq A_4$, y por tamaños deducimos que $G = A_4$.

En el caso del grupo de antes

$$G = \langle (167)(24), (235) \rangle \leq S_7$$

por Lagrange tendríamos que $6 \mid |G| \mid 7!$, y por su descomposición en órbitas tendríamos $12 \mid |G|$, que es mejor. Aún así, quedan muchas posibilidades para G, luego con esto no habríamos acabado.

Pero la partición en órbitas nos da otra información adicional: si X se parte en órbitas Y_j, $j \leq k$ por G, eso equivale a que G sea subgrupo del subgrupo W de S_X que deja Y_j invariantes. Pero todo elemento $w \in W$ puede escribirse de manera única como

$$w = w_1 w_2 \dots w_k$$

con w_j una permutación que sólo mueve elementos de Y_j, y por tanto con w_j disjuntos. Así, $W \cong S_{Y_1} \times S_{Y_2} \times \dots S_{Y_k}$ y por eso

$$G \lesssim S_{Y_1} \times S_{Y_2} \times \dots S_{Y_k}$$

lo que implica

$$|G| \mid n_1! n_2! \dots n_k!$$

con $n_j = |Y_j|$. En el ejemplo anterior, como X se parte en una órbita de tamaño 3 y otra de 4, tendríamos que $|G| \mid 3!4! = 144$, luego tendríamos $12 \mid |G| \mid 144$, así que las posibilidades para G se reducen drásticamente.

Un caso especial es cuando X es una única órbita de G. En este caso, se dice que G es un subgrupo *transitivo* de S_X. Este caso es importante porque que G sea transitivo es equivalente que para cualesquiera $x, y \in X$, existe $g \in G$ de forma que $y = g(x)$. Aplicando nuestro resultado anterior a este caso, tendríamos que

$$|X| = |G/G_x|$$

para cualquier $x \in X$. Así, concluimos que *cualquier subgrupo transitivo de n tiene tamaño divisible por n*. Por ejemplo, en los casos del cubo de Rubik modificado y del puzle de la introducción, ambos son transitivos.

Vemos que las órbitas y estabilizadores son herramientas interesantes para obtener información de grupos de permutaciones. Vamos a ver cómo iterar los procedimientos anteriores de manera provechosa. Para eso, será conveniente definir el estabilizador de varios puntos a la vez:

$$G_{x_1 x_2 \dots x_k} = \cap_j G_{x_j}.$$

4. Resolviendo el puzle

Queríamos ver si $m = (1423)(56)$ está en

$$G = \langle r, s\rangle = \langle (13456), (132)\rangle \leq S_6.$$

Vemos que G es transitivo, por lo que $6 \mid |G|$. Además, por el orden de s vemos que $5 \mid |G|$, luego $30 \mid |G|$.

Por otra parte, podemos fijarnos en que r y s son permutaciones pares, por lo que en realidad $G = A_6$. Eso quiere decir que $30 \mid |G| \mid 3 * 4 * 30$ y que no va a tener trasposiciones.

Lo más sencillo que hay después de las trasposiciones son los 3-ciclos. Así, vamos a buscar 3-ciclos en G. Como s es un 3-ciclo, podemos generar más conjugando con potencias de r:

$$rsr^{-1} = (342) \qquad r^2sr^{-2} = (452).$$

Así, vemos que G_{65} es transitivo como subgrupo de $(S_6)_{65} \cong S_4$, por lo que $4 \mid |G_{65}|$, y como tiene elementos de orden 3 vemos que $3*4 \mid |G_{65}|$, y como sólo tiene permutaciones pares $G_{65} \leq (A_6)_{65} \cong A_4$, luego por tamaños $G_{65} = A_4$ y $|G_{65}| = 12$.

De igual forma vemos que G_6 es transitivo en $(S_6)_6$, luego $5 = |\mathrm{Orb}_{G_6}(5)| = |G_6/G_{65}|$, por lo que $|G_6| = 5 * 12 = 60$, luego de nuevo por tamaño $G_6 = (A_6)_6 \cong A_5$. Finalmente $|G/G_6| = |\mathrm{Orb}_G(6)| = 6$, luego de nuevo $G = A_6$.

Así, hemos demostrado que $G = A_6$, y como m es par, debe pertenecer a G. Pero además veamos que nuestro método sirve para ver como escribir m con r y s. Hemos visto que

$$G_{654} = \langle (123)\rangle \qquad G_{65} = \langle (132), (342)\rangle \qquad G_6 = \langle (132), (342), (452)\rangle.$$

Así, buscamos en G un elemento que actue sobre el 6 igual que m, es decir $6 \mid 5$. Por ejemplo $r^{-1} = (65431)$. Así, tenemos que m y r^{-1} están en la misma clase de G/G_6, luego $m_6 = (r^{-1})^{-1}m$ está en G_6, es decir, fija 6. Tenemos que

$$m_6 = rm = (13456)(1423)(56) = (15)(24) \in G_6.$$

Ahora, buscamos un elemento de los que generan G_6 que actue sobre 5 igual que m_6, es decir $5 \mapsto 1$. Tenemos por ejemplo $(132)(452)$. Así, como antes,

$$m_{65} = [(132)(452)]^{-1}m_6 = (254)(231)(15)(24) = (143) \in G_{65}.$$

El siguiente paso sería

$$m_{654} = (342)m_{65} = (342)(143) = (123) \in G_{654}$$

y por último

$$m_{6543} = [(132)^2]^{-1}m_{654} = e.$$

Deshaciendo los pasos vemos que

$$m = r^{-1}(132)(452)(342)^{-1}(132)^2$$

y como tenemos que $(132) = s$, $(452) = r^2sr^{-2}$ y $(342) = rsr^{-1}$, vemos que

$$m = r^{-1}sr^2sr^{-2}rs^{-1}r^{-1}s^2.$$