Capítulo 1

Permutaciones

Para motivar los axiomas de grupo, en este capítulo vamos a considerar solamente grupos de permutaciones, también conocidos como grupos simétricos.

1.0.1. Definición. Sea X un conjunto. Si $f\colon X \to X$ es una biyección, se dice también que f es una **permutación** de los elementos de X. El conjunto de todas las permutaciones de los elementos de X se denota por S_X.

1.0.2. Observación. *La composición de aplicaciones define una operación binaria sobre S_X*

$$\begin{aligned} S_X \times S_X &\to S_X, \\ (g, f) &\mapsto g \circ f \end{aligned}$$

que satisface las siguientes propiedades.

*G1) La operación $\circ$ es **asociativa**: para cualesquiera $f, g, h \in S_X$ tenemos*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

*G2) La aplicación identidad id_X es el **elemento neutro** respecto a $\circ$, es decir*

$$\mathrm{id}_X \circ f = f = f \circ \mathrm{id}_X$$

para todo $f \in S_X$.

*G3) Para toda permutación $f \in S_X$ existe una permutación **inversa** $f^{-1}\colon X \to X$ que satisface*

$$f \circ f^{-1} = \mathrm{id}_X = f^{-1} \circ f.$$

Demostración. Hemos visto estos resultados en el capítulo anterior. La composición de dos permutaciones es también una permutación, y por lo tanto la operación $(g, f) \mapsto g \circ f$ está bien definida. La propiedad G1) significa nada más que la composición de aplicaciones es asociativa. Luego, la propiedad G2) es la composición con la aplicación identidad. Por fin, una aplicación $f\colon X \to X$ es biyectiva si y solamente si existe la aplicación inversa $f^{-1}\colon X \to X$, y esto nos da G3). ■

Las propiedades G1)–G3) significan que S_X es un **grupo**. Es una estructura algebraica que vamos a definir en el siguiente capítulo y estudiar durante todo el semestre.

1.0.3. Observación. *S_X satisface las siguientes propiedades:*

A1) $\mathrm{id}_X(x) = x$ *para todo* $x \in X$.

A2) $(g \circ f)(x) = g(f(x))$ *para todo* $x \in X$ *y* $f, g \in S_X$.

Demostración. A1) es nada más la definición de la aplicación identidad y A2) es la definición de la composición de aplicaciones. ■

Las propiedades A1) y A2) significan que S_X **actúa** sobre X. Las acciones de grupos sobre conjuntos serán de mucha importancia más adelante.

1.0.4. Definición. S_X junto con la operación binaria $\circ$ es el **grupo simétrico** sobre X.

Normalmente para el grupo simétrico el signo de composición $\circ$ no se escribe: "gf" significa "$g \circ f$". Lo vamos a omitir a partir he ahora. Será muy útil pensar en la composición be biyecciones como una especie de multiplicación *no conmutativa* (en general $fg \neq gf$).

1.1 El grupo simétrico S_n

Un caso particular de interés es cuando X es un conjunto finito de n elementos. Podemos suponer que $X = \{1, 2, \ldots, n\}$.

1.1.1. Notación. Para un número natural n, el grupo simétrico sobre $\{1, 2, \ldots, n\}$ se denota por

$$S_n := S_{\{1,2,\ldots,n\}}.$$

1.1.2. Ejemplo. El caso tonto es el de $n = 0$ que corresponde a... las permutaciones del conjunto vacío. Hay una aplicación única $\emptyset \to \emptyset$. Para $n = 1$ tenemos un conjunto de un elemento $\{1\}$ y una aplicación única $\mathrm{id}\colon \{1\} \to \{1\}$. El primer caso no trivial es de $n = 2$. El conjunto $\{1, 2\}$ tiene dos permutaciones: la permutación identidad

$$\mathrm{id}\colon 1 \mapsto 1,\ 2 \mapsto 2$$

y la permutación que intercambia 1 y 2:

$$\sigma\colon 1 \mapsto 2,\ 2 \mapsto 1.$$

Las composiciones de estas permutaciones son

$$\mathrm{id}\,\mathrm{id} = \mathrm{id}, \quad \sigma\,\mathrm{id} = \mathrm{id}\,\sigma = \sigma, \quad \sigma\sigma = \mathrm{id}.$$

▲

1.1.3. Notación. Una permutación $\sigma \in S_n$ puede representarse mediante una tabla donde en la primera fila están los números $i = 1, 2, \ldots, n$ y en la segunda fila están sus imágenes correspondientes $\sigma(i) \in \{1, 2, \ldots, n\}$:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Notamos que el hecho de que σ sea una biyección $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ significa precisamente que los números $\sigma(1), \sigma(2), \ldots, \sigma(n)$ no se repiten.

1.1.4. Ejemplo. Los elementos de S_2 pueden ser representados por las tablas

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

El grupo simétrico S_3 consiste en 6 elementos dados por

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{1.1}$$

Notemos que en general, dos permutaciones $\sigma, \tau \in S_n$ no conmutan; es decir,

$$\sigma\tau \neq \tau\sigma.$$

En el caso de S_3 tenemos

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tag{1.2}$$

mientras que

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{1.3}$$

▲

1.1.5. Observación. *Tenemos*

$$|S_n| = n!$$

Demostración. La base de inducción es $|S_0| = |S_1| = 1$. Luego, supongamos que $|S_{n-1}| = (n-1)!$. Cada elemento $\sigma \in S_{n-1}$ corresponde a una lista sin repeticiones de los números entre 1 y $n-1$:

$$\sigma(1), \sigma(2), \ldots, \sigma(n-1).$$

Todos los elementos de S_n se obtienen poniendo el número n en una posición, y hay precisamente n posibilidades. Entonces,

$$|S_n| = n \cdot |S_{n-1}| = n \cdot (n-1)! = n!$$

■

1.2 Permutaciones cíclicas

1.2.1. Definición. Para $1 \leq k \leq n$ sean $i_1, i_2, i_3, \ldots, i_k$ algunos números distintos entre 1 y n. Definamos una permutación σ por

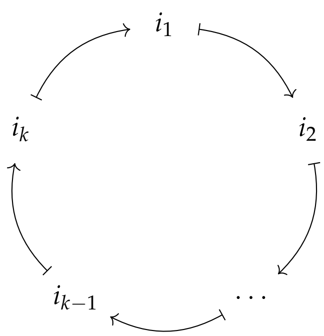
$$\begin{aligned} \sigma(i_1) &:= i_2, \\ \sigma(i_2) &:= i_3, \\ &\vdots, \\ \sigma(i_{k-1}) &:= i_k, \\ \sigma(i_k) &:= i_1 \end{aligned}$$

y

$$\sigma(j) = j \quad \text{para } j \notin \{i_1, i_2, i_3, \ldots, i_k\}.$$

Entonces, se dice que σ es una **permutación cíclica de orden** k o un k**-ciclo** y se escribe

$$\sigma = (i_1\ i_2\ \cdots\ i_{k-1}\ i_k).$$



Note que el orden k es el mínimo número tal que

$$\underbrace{\sigma \cdots \sigma}_{k} = \mathrm{id}.$$

La permutación identidad id se considera como la permutación cíclica de orden 1, ya que esta corresponde a (i) para cualquier $i \in \{1, \ldots, n\}$.

1.2.2. Definición. Los 2-ciclos $\sigma = (i\ j)$ reciben el nombre especial de **transposiciones**.

Note que la transposición $(i\ j)$ intercambia i con j y deja otros elementos intactos.

En un ciclo, los índices en los paréntesis pueden ser *permutados cíclicamente* y el resultado no cambia:

$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$

Por esto normalmente se escoge la presentación $(i_1\ i_2\ \cdots i_{k-1}\ i_k)$ donde i_1 es el número mínimo (en el ejemplo de arriba es $(1\ 2\ 3)$).

1.2.3. Ejemplo. El grupo simétrico S_3 consiste en permutaciones cíclicas; sus elementos, enumerados en (1.1), también pueden ser escritos como

$$\mathrm{id},\ (1\ 2),\ (2\ 3),\ (1\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2).$$

Compilemos la tabla de composición de permutaciones en S_3 en términos de ciclos. Escribamos una tabla de 6×6 indexada por los elementos de S_3 donde en la intersección de la fila σ y la columna τ está $\sigma\tau$:

$\circ$	$\cdots$	τ	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
σ	$\cdots$	$\sigma\tau$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$

Por ejemplo, las fórmulas (1.2) y (1.3) pueden ser escritas como

$$(1\ 2)\,(2\ 3) = (1\ 2\ 3), \quad (2\ 3)\,(1\ 2) = (1\ 3\ 2).$$

Haciendo cálculos similares, se obtiene

$\circ$	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(2 3)	(2 3)	(1 3 2)	id	(1 2 3)	(1 3)	(1 2)
(1 3)	(1 3)	(1 2 3)	(1 3 2)	id	(1 2)	(2 3)
(1 2 3)	(1 2 3)	(1 3)	(1 2)	(2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 3)	(1 2)	id	(1 2 3)

Note que los elementos no se repiten en ninguna columna o fila. No es una coincidencia: en general,

$$\sigma\tau = \sigma\tau' \Rightarrow \tau = \tau'$$

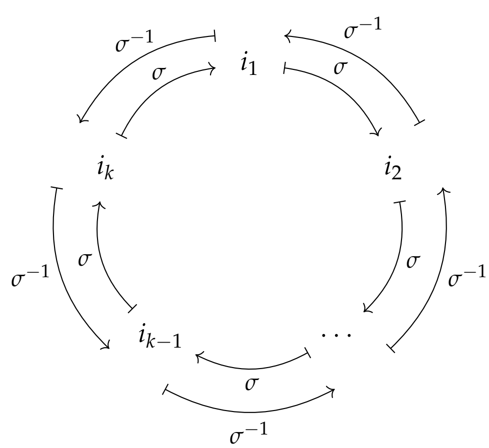
y

$$\sigma\tau = \sigma'\tau \Rightarrow \sigma = \sigma',$$

ya que toda biyección es cancelable por la izquierda y por la derecha. ▲

1.2.4. Observación. *La permutación inversa a un k-ciclo es también un k-ciclo, dado por*

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ i_{k-1}\ \cdots\ i_1) = (i_1\ i_k\ i_{k-1}\ \cdots\ i_2).$$



1.2.5. Definición. Se dice que dos ciclos $\sigma = (i_1\ i_2\ \cdots\ i_k)$ y $\tau = (j_1\ j_2\ \cdots\ j_\ell)$ en S_n son **disjuntos** si $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset$.

1.2.6. Observación. *Dos ciclos disjuntos cualesquiera conmutan entre sí:*

$$\sigma\tau = \tau\sigma.$$

Demostración. En general, si una permutación σ afecta los números $\{i_1, i_2, \ldots, i_k\}$ (es decir, $\sigma(i) = i$ para $i \notin \{i_1, i_2, \ldots, i_k\}$) y τ afecta $\{j_1, j_2, \ldots, j_\ell\}$, está claro que $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset$ implica que $\sigma\tau = \tau\sigma$. ■

No todas las permutaciones son cíclicas. Por ejemplo, la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$$

es una composición de dos ciclos disjuntos:

$$\sigma = (1\;2)\,(3\;4) = (3\;4)\,(1\;2).$$

$$1 \rightleftarrows 2 \qquad\qquad 3 \rightleftarrows 4$$

Sin embargo, tenemos el siguiente resultado.

1.2.7. Proposición. *Toda permutación $\sigma \in S_n$ puede ser escrita como una composición de ciclos disjuntos.*

Demostración. Consideremos la lista máxima

$$i_1 := 1,\; i_2 := \sigma(1),\; i_3 := \sigma(i_2),\; i_4 := \sigma(i_3),\; \ldots,\; i_k := \sigma(i_{k-1})$$

tal que $i_1, i_2, \ldots, i_k$ son números distintos; es decir, terminemos la lista cuando

$$\sigma(i_k) = i_\ell \quad \text{para algún } 1 \le \ell \le k.$$

Ahora si $\ell \ne 1$, tenemos

$$\sigma(i_k) = \sigma(i_{\ell-1}),$$

pero $i_k \ne i_{\ell-1}$ y esto contradice la inyectividad de σ. Entonces, $\ell = 1$, y hemos obtenido un ciclo. (Si $\sigma(1) = 1$, acabamos de encontrar un ciclo de orden 1, pero es conveniente considerarlo como un ciclo legítimo para simplificar el algoritmo.)

Luego podemos considerar el número mínimo j_1 tal que $j_1 \notin \{i_1, \ldots, i_k\}$. De la misma manera, vamos a obtener otro ciclo que empieza por j_1 y que es disjunto con el ciclo $(i_1\; i_2\; \cdots\; i_k)$.

Repitiendo este proceso, encontramos que todos los elementos pertenecen a algún ciclo, y estos ciclos son disjuntos. ∎

1.2.8. Ejemplo. Consideremos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 1 & 3 & 8 & 6 & 5 & 2 & 10 & 9 \end{pmatrix}$$

Empezando por 1, tenemos una sucesión

$$1 \mapsto 4 \mapsto 3 \mapsto 1$$

Esto nos da un ciclo $(1\;4\;3)$. Nos quedan los números $2, 5, 6, 7, 8, 9, 10$. Empezando por 2, se obtiene

$$2 \mapsto 7 \mapsto 5 \mapsto 8 \mapsto 2$$

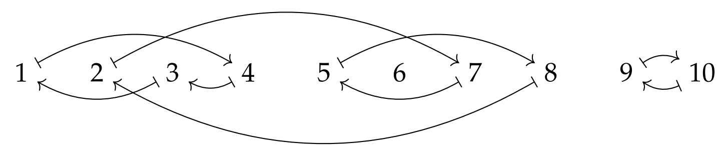
y otro ciclo es $(2\;7\;5\;8)$. Luego, 6 es un punto fijo: tenemos $\sigma(6) = 6$ y un ciclo (6). Nos quedan 9 y 10:

$$9 \mapsto 10 \mapsto 9$$

lo que nos da una transposición $(9\;10)$. Entonces, la descomposición en ciclos disjuntos es dada por

$$\sigma = (1\;4\;3)\,(2\;7\;5\;8)\,(9\;10)$$

(el ciclo (6) no cambia nada y se omite, como todos los ciclos de orden 1).



▲

1.2.9. Definición. Para $\sigma \in S_n$, consideremos su descomposición en ciclos disjuntos. La sucesión de órdenes de estos ciclos se llama el **tipo de ciclo** de σ.

Todos los tipos de ciclo posibles en S_n corresponden a las particiones de n en una suma de números positivos. Por ejemplo, para $n = 4$ tenemos las siguientes opciones.

$$\begin{aligned}
1+1+1+1 &\quad\leftrightarrow\quad (\bullet)\,(\bullet)\,(\bullet)\,(\bullet) = \mathrm{id} \\
1+1+2 &\quad\leftrightarrow\quad (\bullet)\,(\bullet)\,(\bullet\,\bullet) = (\bullet\,\bullet) \\
2+2 &\quad\leftrightarrow\quad (\bullet\,\bullet)\,(\bullet\,\bullet) \\
1+3 &\quad\leftrightarrow\quad (\bullet)\,(\bullet\;\bullet\;\bullet) = (\bullet\;\bullet\;\bullet) \\
4 &\quad\leftrightarrow\quad (\bullet\;\bullet\;\bullet\;\bullet)
\end{aligned}$$

El número de particiones de n se denota por $p(n)$ y se llama la **función de particiones**. La tabla de abajo presenta algunos valores de $p(n)$. Sus propiedades se estudian extensivamente en combinatoria y teoría de números.

n:	1	2	3	4	5	6	7	8	9	10
$p(n)$:	1	2	3	5	7	11	15	22	30	42
n:	11	12	13	14	15	16	17	18	19	20
$p(n)$:	56	77	101	135	176	231	297	385	490	627

1.2.10. Ejemplo. Con un poco de cuidado para no olvidar ninguna permutación y no escribirla dos veces, encontramos la lista completa de las permutaciones en S_4:

$$\begin{gathered}
\mathrm{id}, \\
(1\,2),\quad (1\,3),\quad (1\,4),\quad (2\,3),\quad (2\,4),\quad (3\,4), \\
(1\,2\,3),\quad (1\,2\,4),\quad (1\,3\,2),\quad (1\,3\,4),\quad (1\,4\,2),\quad (1\,4\,3),\quad (2\,3\,4),\quad (2\,4\,3), \\
(1\,2)\,(3\,4),\quad (1\,3)\,(2\,4),\quad (1\,4)\,(2\,3), \\
(1\,2\,3\,4),\quad (1\,2\,4\,3),\quad (1\,3\,2\,4),\quad (1\,3\,4\,2),\quad (1\,4\,2\,3),\quad (1\,4\,3\,2).
\end{gathered}$$

Para comprobar, calculemos el número de elementos:

$$1 + 6 + 8 + 3 + 6 = 24 = 4!$$

▲

1.2.11. Proposición. *En S_n hay*

$$\frac{n!}{\prod_\ell M_\ell! \cdot \ell^{M_\ell}}$$

permutaciones con la descomposición en ciclos disjuntos de la forma

$$\sigma = \underbrace{(\bullet)\cdots(\bullet)}_{M_1 \textit{ puntos fijos}}\ \underbrace{(\bullet\ \bullet)\cdots(\bullet\ \bullet)}_{M_2 \textit{ transposiciones}}\ \underbrace{(\bullet\ \bullet\ \bullet)\cdots(\bullet\ \bullet\ \bullet)}_{M_3 \textit{ ciclos de orden } 3}\cdots \tag{1.4}$$

(aquí $M_1 + M_2 \cdot 2 + M_3 \cdot 3 + \cdots = n$).

Demostración. Hay $n!$ posibilidades de colocar los números $\{1,\ldots,n\}$ en lugar de $\bullet$ en (1.4). En cada serie de M_ℓ ciclos de longitud ℓ, podemos escribir los ciclos en otro orden, y el resultado no cambia, así que hay que dividir $n!$ por $\prod_\ell M_\ell!$. También para cada ciclo de longitud ℓ, hay ℓ modos equivalentes de escribirlo permutando los índices cíclicamente. Por esto hay que dividir todo por $\prod_\ell \ell^{M_\ell}$. ■

1.2.12. Ejemplo. Si nos interesan los k-ciclos en S_n (donde $1 \le k \le n$), tenemos

$$M_1 = (n-k), \quad M_2 = \cdots = M_{k-1} = 0, \quad M_k = 1, \quad M_{k+1} = M_{k+2} = \cdots = 0$$

y la fórmula nos da

$$\frac{n!}{(n-k)!\cdot k}.$$

En particular, hay

$$\frac{n\,(n-1)}{2} = \binom{n}{2}$$

transposiciones. ▲

1.2.13. Ejemplo. En S_5 tenemos

- la permutación identidad id,
- $10 = \frac{5!}{3!\cdot 2}$ transposiciones $(\bullet\ \bullet)$,
- $20 = \frac{5!}{2!\cdot 3}$ ciclos $(\bullet\ \bullet\ \bullet)$,
- $30 = \frac{5!}{4}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet)$,
- $24 = \frac{5!}{5}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$,
- $15 = \frac{5!}{2!\cdot 2^2}$ permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet)$,
- $20 = \frac{5!}{2\cdot 3}$ permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet\ \bullet)$.

▲

1.2.14. Definición. Para $\sigma, \tau \in S_n$ la permutación $\tau\sigma\tau^{-1} \in S_n$ se llama la **conjugación de σ por τ**.

1.2.15. Observación. *Para dos permutaciones $\sigma, \tau \in S_n$, si*

$$\sigma\colon i \mapsto j,$$

entonces

$$\tau\sigma\tau^{-1}\colon \tau(i) \mapsto \tau(j).$$

Demostración.

$$\tau\sigma\tau^{-1}(\tau(i)) = (\tau\sigma\tau^{-1}\tau)(i) = (\tau\sigma)(i) = \tau(j).$$

■

1.2.16. Corolario. *Si*

$$\sigma = (i_1\, i_2\, \cdots\, i_k)$$

es un k-ciclo, entonces para toda permutación $\tau \in S_n$, la conjugación de σ por τ es también un k-ciclo dado por

$$\tau\,(i_1\, i_2\, \cdots\, i_k)\,\tau^{-1} = (\tau(i_1)\; \tau(i_2)\; \cdots\; \tau(i_k)).$$

En general, la conjugación no cambia el tipo de ciclo de una permutación. Dos permutaciones $\sigma, \sigma' \in S_n$ son conjugadas ($\sigma' = \tau\sigma\tau^{-1}$ para alguna permutación $\tau \in S_n$) si y solamente si tienen el mismo tipo de ciclo.

Demostración. Todo esto está claro de la observación precedente: la conjugación nada más cambia la numeración de nuestros elementos $\{1, 2, \ldots, n\}$. Para una permutación

$$\sigma = (\bullet\ \bullet\ \cdots\ \bullet)\,(\bullet\ \bullet\ \cdots\ \bullet)\cdots(\bullet\ \bullet\ \cdots\ \bullet)$$

la conjugación por τ nos da

$$\tau\sigma\tau^{-1} = \tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}\,\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}\cdots\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1},$$

y aquí para cada k-ciclo $(\bullet\ \bullet\ \cdots\ \bullet)$ en la descomposición su conjugado $\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}$ es también un k-ciclo. Si al principio los ciclos son disjuntos, los conjugados son también disjuntos, puesto que τ es una biyección.

Ahora si σ y σ' son dos permutaciones que tienen el mismo tipo de ciclo, esto significa que son idénticas salvo renumeración de los elementos $\{1, 2, \ldots, n\}$. Esta renumeración se realiza por cierta permutación $\tau \in S_n$ y $\sigma' = \tau\sigma\tau^{-1}$. ■

1.3 Signo y el grupo alternante A_n

1.3.1. Definición. Para una permutación $\sigma \in S_n$ cuando para algunos $i < j$ se tiene $\sigma(i) > \sigma(j)$, se dice que hay una **inversión**. El número

$$\operatorname{sgn}\sigma := (-1)^{\#\text{de inversiones}}$$

se llama el **signo** de σ. Se dice que σ es **par** si $\operatorname{sgn}\sigma = +1$ e **impar** si $\operatorname{sgn}\sigma = -1$.

1.3.2. Ejemplo. Para S_3 tenemos

permutación	inversiones	signo	
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	no hay	$+1$	(par)
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$3>2$	-1	(impar)
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$3>2, 3>1, 2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$2>1, 3>1$	$+1$	(par)
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$3>1, 3>2$	$+1$	(par)

▲

1.3.3. Digresión. El signo de permutación aparece en la famosa fórmula para el determinante de una matriz $A = (x_{ij})_{1 \le i,j \le n}$:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot x_{1,\sigma(1)}\, x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}. \tag{1.5}$$

Por ejemplo, en S_2 tenemos dos permutaciones: la permutación identidad de signo $+1$ y la transposición $(1\ 2)$ de signo -1. Esto nos da

$$\det \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = x_{11}\, x_{22} - x_{12}\, x_{21}.$$

Sin embargo, la expresión (1.5) es horrible y no explica el significado geométrico del determinante, ni sirve para hacer cálculos prácticos (¡la suma es sobre $n!$ términos!).

1.3.4. Observación. *Todo k-ciclo es una composición de $k-1$ transposiciones:*

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)\,(i_2\ i_3)\,(i_3\ i_4) \cdots (i_{k-1}\ i_k).$$

1.3.5. Corolario. *Toda permutación $\sigma \in S_n$ es una composición de transposiciones (no necesariamente disjuntas).*

Demostración. Sigue de la descomposición de permutaciones en ciclos disjuntos (1.2.7) y luego descomposición de cada ciclo en transposiciones (1.3.4). ∎

El último resultado es muy natural: intuitivamente debe de ser claro que para permutar n elementos de cualquier modo, es suficiente hacer una sucesión de intercambios por pares. De hecho, se puede hacer una sucesión de intercambios de elementos adyacentes.

1.3.6. Observación. *Toda transposición $(a\ b)$ con $b - a = k$ puede ser escrita como una composición de $2k-1$ transposiciones de la forma $(i\ i+1)$.*

1.3.7. Ejemplo. Tenemos

$$(1\ 4) = (1\ 2)\,(2\ 3)\,(3\ 4)\,(2\ 3)\,(1\ 2).$$

1	2	3	4
2	1	3	4
2	3	1	4
2	3	4	1
2	4	3	1
4	2	3	1

▲

Demostración de 1.3.6. La idea debe de ser clara a partir del ejemplo de arriba. Para formalizar la demostración, usamos la inducción sobre k. La base de inducción es el caso de $k = 1$ y el paso inductivo resulta de la fórmula

$$(a\ b) = (a\ a+1)\,(a+1\ b)\,(a\ a+1).$$

∎

El mismo argumento formulado en otras palabras: a partir de $(b-1\ b)$ se puede hacer una sucesión de $k-1$ conjugaciones

$$\begin{aligned}(b-2\ b-1)\,(b-1\ b)\,(b-2\ b-1) &= (b-2\ b),\\ (b-3\ b-2)\,(b-2\ b)\,(b-3\ b-2) &= (b-3\ b),\\ (b-4\ b-3)\,(b-3\ b)\,(b-4\ b-3) &= (b-4\ b),\\ &\cdots\end{aligned}$$

hasta que se obtenga $(a\ b)$.

1.3.8. Corolario. *Todo elemento de S_n puede ser expresado como un producto de transposiciones*

$$(1\,2),\ (2\,3),\ (3\,4),\ \ldots,\ (n-1\ n).$$

Demostración. Sigue de 1.3.5 y 1.3.6. ■

1.3.9. Observación. *Transposiciones cambian la paridad: si τ es una transposición y $\sigma \in S_n$ es cualquier permutación, entonces*

$$\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}\sigma.$$

Demostración. Está claro que cuando σ es de la forma $(i\ i+1)$, el signo cambia al opuesto. Luego, hemos visto en 1.3.6 que toda transposición $(a\ b)$ es una composición de $2k-1$ transposiciones de esta forma, donde $k = b-a$. El número $2k-1$ es impar. ■

Como hemos visto en el ejemplo 1.3.2, en S_3 hay 3 pares y 3 impares permutaciones. Esto no es una coincidencia.

1.3.10. Corolario. *Para $n \geq 2$ el número de permutaciones pares en S_n es igual al número de permutaciones impares.*

Demostración. Consideremos la aplicación

$$\begin{aligned}\phi\colon S_n &\to S_n,\\ \sigma &\mapsto (1\,2)\,\sigma.\end{aligned}$$

Es una biyección (de hecho $\phi\circ\phi = \mathrm{id}$) que según 1.3.9 aplica toda permutación par a una permutación impar y viceversa. ■

1.3.11. Corolario. *La paridad de una permutación σ es precisamente la paridad de la longitud de alguna descomposición en transposiciones: si*

$$\sigma = \tau_k\cdots\tau_1,$$

para algunas transposiciones τ_i, entonces

$$\operatorname{sgn}\sigma = (-1)^k.$$

1.3.12. Corolario. *Para dos diferentes descomposiciones en transposiciones*

$$\sigma = \tau_k\cdots\tau_1 = \tau'_\ell\cdots\tau'_1$$

los números k y ℓ necesariamente tienen la misma paridad: $k \equiv \ell \pmod 2$.

1.3.13. Digresión. A veces 1.3.11 se toma por la *definición* del signo, pero luego hay que demostrar que esta fórmula tiene sentido; es decir deducir 1.3.12 sin usar el signo. He aquí una breve explicación en términos del tipo de ciclo de σ, que es evidentemente un invariante de σ, a diferencia de la longitud de una descomposición en transposiciones. Para toda transposición $\tau = (i\ j)$ hay dos posibilidades.

1) i y j pertenecen al mismo ciclo. En este caso en $\tau\sigma$ este ciclo se descompone en dos.

2) i y j pertenecen a diferentes ciclos (posiblemente de orden 1). Entonces se ve que en $\tau\sigma$ estos dos ciclos se unen en uno.

En ambos casos el número de ciclos disjuntos cambia su paridad para $\tau\sigma$. Ahora si tenemos

$$\sigma = \tau_k \cdots \tau_1 = \tau'_\ell \cdots \tau'_1,$$

entonces se ve que los números k y ℓ deben tener la misma paridad.

1.3.14. Observación. *Para dos permutaciones $\sigma, \tau \in S_n$ se tiene*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

Demostración. Está claro de la interpretación del signo en 1.3.11. ∎

1.3.15. Corolario. *Tenemos*

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}\sigma.$$

Demostración.

$$\operatorname{sgn}\sigma \cdot \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\mathrm{id}) = +1.$$

∎

1.3.16. Definición. Al conjunto de las permutaciones pares en S_n lo llamamos **grupo alternante** y lo denotamos por A_n:

$$A_n := \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\} \subset S_n.$$

Tenemos las siguientes propiedades:

- $\mathrm{id} \in A_n$ (puesto que $\operatorname{sgn}(\mathrm{id}) = +1$),
- si $\sigma, \tau \in A_n$, entonces $\sigma\tau \in A_n$ (véase 1.3.14),
- si $\sigma \in A_n$, entonces $\sigma^{-1} \in A_n$ (véase 1.3.15).
- conjugando las permutaciones de A_n por las permutaciones de S_n, se obtienen también permutaciones de A_n: para todo $\sigma \in A_n$ y $\tau \in S_n$ tenemos $\tau\sigma\tau^{-1} \in A_n$.

  (De hecho, $\operatorname{sgn}(\tau\sigma\tau^{-1}) = \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma \cdot \operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}\sigma$.)

Además, hemos calculado en 1.3.10 que

$$|A_n| = |S_n|/2 = n!/2.$$

1.3.17. Ejemplo.

$$A_2 = \{\mathrm{id}\},$$
$$A_3 = \{\mathrm{id},\ (1\ 2\ 3),\ (1\ 3\ 2)\}.$$

En S_4 las permutaciones son de la forma

$$\mathrm{id},\quad (\bullet\,\bullet),\quad (\bullet\ \bullet\ \bullet),\quad (\bullet\,\bullet)\,(\bullet\,\bullet),\quad (\bullet\ \bullet\ \ \bullet\ \bullet).$$

Luego, todas las transpocisiones son impares. Los 3-ciclos son pares, ya que son productos de dos transposiciones:

$$(i\ j\ k) = (i\ j)\,(j\ k).$$

Los 4-ciclos con impares, siendo productos de 3 transposiciones:

$$(i\ j\ k\ \ell) = (i\ j)\,(j\ k)\,(k\ \ell).$$

Entonces, los elementos de A_4 son

$$\mathrm{id},$$
$$(1\,2\,3),\quad (1\,2\,4),\quad (1\,3\,2),\quad (1\,3\,4),\quad (1\,4\,2),\quad (1\,4\,3),\quad (2\,3\,4),\quad (2\,4\,3),$$
$$(1\,2)\,(3\,4),\quad (1\,3)\,(2\,4),\quad (1\,4)\,(2\,3).$$

De hecho, en la lista de arriba tenemos $1+8+3 = 12 = 4!/2$ permutaciones. ▲

1.4 Ejercicios

Ejercicio 1.1. *Encuentre la descomposición en ciclos disjuntos para la permutación*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 5 & 1 & 4 & 2 & 3 & 10 & 8 & 9 \end{pmatrix} \in S_{10}$$

y su signo.

Ejercicio 1.2. *Calcule la descomposición en ciclos disjuntos del producto de ciclos*

$$(1\,2)\,(2\,5\,3)\,(1\,5\,7\,3\,2\,6\,4)\,(4\,7\,6) \in S_7$$

y su signo.

Ejercicio 1.3. *Demuestre la fórmula para el signo de un k-ciclo:*

$$\operatorname{sgn}(i_1\ i_2\ \cdots\ i_k) = (-1)^{k-1}.$$

En general, si $\sigma \in S_n$ afecta m elementos (en el sentido de que $\sigma(i) \neq i$ para m números i) y tiene una descomposición en s ciclos disjuntos, entonces

$$\operatorname{sgn}\sigma = (-1)^{m-s}.$$

Por ejemplo,

$$\sigma = (1\,2)\,(3\,6\,4)\,(5\,11\,8)$$

afecta $1,2,3,4,5,6,8,11$, entonces $m = 8$, y en la expresión de arriba hay $s = 3$ ciclos disjuntos. Entonces, $\operatorname{sgn}\sigma = (-1)^{8-3} = -1$.

Ojo: según nuestra terminología, el último ejercicio nos dice que una permutación cíclica de orden par k es impar (tiene signo -1) y viceversa.

Para realizar cualquier permutación, se puede fijar algún elemento y cada vez hacer intercambios solo con este.

Ejercicio 1.4. *Fijemos algún elemento de $\{1,\ldots,n\}$, por ejemplo 1. Demuestre que toda transposición $(i\ j)$ puede ser escrita como una composición de transposiciones de la forma $(1\ k)$. Deduzca que toda permutación $\sigma \in S_n$ para $n \geq 2$ es un producto de transposiciones*

$$(1\,2),\ (1\,3),\ \ldots,\ (1\,n).$$

De hecho, para expresar cualquier permutación, es suficiente usar una sola transposición, un n-ciclo y su inverso.

Ejercicio 1.5. *Demuestre que todo elemento de S_n puede ser expresado como un producto de*

$$(1\,2),\ (1\,2\ \cdots\ n),\ (1\,2\ \cdots\ n)^{-1}.$$

Indicación: use que los elementos de S_n se expresan como productos de transposiciones de la forma $(i\ i+1)$ y la fórmula $\sigma\,(i_1\ i_2\ \cdots\ i_k)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$.

En los siguientes ejercicios vamos a demostrar un resultado similar para los grupos alternantes.

Ejercicio 1.6. *Sean i, j, k, ℓ números distintos. Verifique las relaciones para la composición de transposiciones*

$$\begin{aligned}(i\ j)\,(j\ k) &= (i\ j\ k),\\ (i\ j)\,(k\ \ell) &= (i\ j\ k)\,(j\ k\ \ell).\end{aligned}$$

Deduzca que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de orden 3.

Ejercicio 1.7. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(1\ i\ j)$.*
Indicación: use el ejercicio 1.6.

Ejercicio 1.8. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(1\ 2\ i)$.*
Indicación: use el ejercicio 1.7.

Ejercicio 1.9. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(i\ i+1\ i+2)$.*
Indicación: note que es un análogo de la descomposición de los elementos de S_n mediante las transposiciones de la forma $(i\ i+1)$. Para $i > 3$ demuestre la identidad

$$(1\ 2\ i) = (1\ 2\ i-2)\,(1\ 2\ i-1)\,(i-2\ i-1\ i)\,(1\ 2\ i-2)\,(1\ 2\ i-1)$$

Luego, proceda por inducción sobre i y use el ejercicio 1.8.

Ejercicio 1.10. *Demuestre que para $n \geq 3$ todo elemento de A_n puede ser escrito como el producto de*

- $(1\ 2\ 3)$, $(2\ 3\ \cdots\ n)$, $(2\ 3\ \cdots\ n)^{-1}$, *si n es par;*
- $(1\ 2\ 3)$, $(1\ 2\ \cdots\ n)$, $(1\ 2\ \cdots\ n)^{-1}$, *si n es impar.*

Indicación: use la fórmula $\sigma\,(i_1\ i_2\ \cdots\ i_k)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$ y el ejercicio 1.9.

La moraleja de los ejercicios de arriba: aunque S_n y A_n tienen muchos elementos, estos se expresan en términos de solamente dos de ellos (y sus inversos).