# El grupo simétrico y el grupo alternante

Facultad de Ciencias UNAM

# Introducción

En esta sección introducimos y estudiamos a un grupo que jugara un rol crucial en el resto del curso. Cabe recalcar que muchos de los resultados en esta sección no serán ocupados hasta dentro de varias secciones; los presentamos aquí por conveniencia.

# El grupo simétrico $S_X$

## Definición

Supongamos que $X$ es un conjunto no vacío. Si $\sigma : X \to X$ es una biyección, decimos que $\sigma$ es una **permutación de** $X$. Al conjunto de todas las permutaciones de $X$ lo denotamos por $S_X$.

Claramente, $S_X$ forma un grupo con la operación dada por la composición usual de funciones. En lo que sigue, siempre consideramos a $S_X$ de esta manera.

El caso $X = \{1, \ldots, n\}$ es importante y por eso, denotamos $S_n := S_{\{1,\ldots,n\}}$.

Por un argumento básico de combinatoria, es fácil ver que

$$|S_n| = n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1.$$

# Permutación = reacomodo

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Un reacomodo de $X = \{1, 2, \ldots, n\}$ es una lista ordenada $i_1, i_2, \ldots, i_n$ de todos los elementos de $\{1, 2, \ldots, n\}$ que no tiene elementos repetidos.

Dado un reacomodo de $X = \{1, 2, \ldots, n\}$, digamos $i_1, i_2, \ldots, i_n$, definimos $\alpha : X \to X$ por $\alpha(j) = i_j$ para toda $j \in X$. Entonces $\alpha$ es inyectiva[1] y suprayectiva[2] Por lo tanto, $\alpha$ es biyectiva y *todo reacomodo induce una permutación*.

Conversamente, cualquier permutación $\alpha \in S_n$ puede ser denotada por

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

y la fila de abajo es un reacomodo de $\{1, 2, \ldots, n\}$. Por lo tanto, también *toda permutación induce un reacomodo*.

En resumen, los conceptos de permutación y reacomodo son "equivalentes". Ambas perspectivas tienen sus ventajas. Por ejemplo, hay una forma muy natural de operar permutaciones (composición de funciones).

---

[1]Un reacomodo es una de elementos que no tiene elementos repetidos.

[2]Un reacomodo es una lista ordenada de todos los elementos de $X$.

# $l$-ciclos

## Definición

Supongamos que $n \in \mathbb{Z}_{\geq 2}$ y que $i_1, \ldots, i_l \in \{1, \ldots, n\}$ son números distintos. Denotamos por $(i_1 i_2 \cdots i_l)$ al elemento de $S_n$ que satisface

$$
\begin{aligned}
i_1 &\mapsto i_2 \\
i_2 &\mapsto i_3 \\
&\vdots \\
i_{l-1} &\mapsto i_l \\
i_l &\mapsto i_1 \\
i &\mapsto i \text{ si } i \notin \{i_1, \ldots, i_l\}
\end{aligned}
$$

Mas aun, para cualesquiera $i_1, \ldots, i_l \in \{1, \ldots, n\}$ números distintos, decimos que $(i_1 i_2 \cdots i_l)$ es un **$l$-ciclo** o que $(i_1 i_2 \cdots i_l)$ es un **ciclo de longitud** $l$. Finalmente, si $\sigma$ es un 2-ciclo[3], entonces decimos que $\sigma$ es una **transposición**.

[3] Es decir, $\sigma$ simplemente intercambia un par de elementos.

# Observación

- Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Si $i_1, \ldots, i_l \in \{1, \ldots, n\}$ son números distintos, entonces

$$(i_1 i_2 \cdots i_{l-1} i_l) = (i_2 i_3 \cdots i_l i_1) = \cdots = (i_l i_1 \cdots i_{l-2} i_{l-1}).$$

- Cuando usemos esta notación, es importante tener cuidado con la forma en la que "multiplicamos" o mas precisamente, "componemos". Por ejemplo,

$$(345)(123)(12) = (1453).$$

# $\sigma$ fija/mueve a $x$

**Definición**

Supongamos que $X$ es un conjunto no vacío, que $x \in X$, y que $\sigma \in S_X$. Decimos que $\sigma$ **fija a** $x$ si $\sigma(x) = x$ y decimos que $\sigma$ **mueve a** $x$ si $\sigma(x) \neq x$.

Por ejemplo,

- Usando la pura definición, es fácil ver que todo 1-ciclo fija a todo elemento de $S_n$. Equivalentemente, el único 1-ciclo es la identidad.
- Supongamos que $(i_1 i_2 \cdots i_l) \in S_n$ es un $l$-ciclo con $n \geq 2$. Entonces
  - $(i_1 i_2 \cdots i_l)$ mueve a $i_1, i_2, \ldots, i_l$ y
  - $(i_1 i_2 \cdots i_l)$ fija a los $n - l$ elementos de $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_l\}$.

# Permutaciones disjuntas

## Definición

Supongamos que $X$ es un conjunto no vacío. Dos permutaciones $\alpha, \beta \in S_X$ son **disjuntas** si todo $x$ movido por una es fijado por la otra. Específicamente,

$$\alpha(x) \neq x \implies \beta(x) = x \quad \text{y} \quad \beta(x) \neq x \implies \alpha(x) = x.$$

También, decimos que $\alpha_1, \ldots, \alpha_m \in S_n$ son **disjuntas** si $\alpha_i$ y $\alpha_j$ son disjuntas para toda $i, j \in \{1, \ldots, m\}$ distintos.

Considera $A = \{x \in X \mid \alpha \text{ mueve a } x\}$ y $B = \{x \in X \mid \beta \text{ mueve a } x\}$. Es fácil verificar que $\alpha$ y $\beta$ son permutaciones disjuntas si y solo si $A$ y $B$ son conjuntos disjuntos.

Por ejemplo, si $i_1, \ldots, i_l \in \{1, \ldots, n\}$ son números distintos y $j_1, \ldots, j_m \in \{1, \ldots, n\}$ también son números distintos, entonces $(i_1 i_2 \cdots i_l)$ y $(j_1 j_2 \cdots j_m)$ son disjuntas si y solo si $\{i_1, \ldots, i_l\} \cap \{j_1, \ldots, j_m\} = \emptyset$.

# Las permutaciones disjuntas conmutan

**Proposición 1**

Supongamos que $X$ es un conjunto no vacío. Si $\alpha, \beta \in S_X$ son disjuntas, entonces $\alpha\beta = \beta\alpha$.

*Demostración.* Supongamos que $x \in X$. Como $\alpha$ y $\beta$ son disjuntas, no puede suceder que $\alpha(x) \neq x$ y $\beta(x) \neq x$. Por lo tanto, tenemos tres casos:

1. $\alpha(x) \neq x$ y $\beta(x) = x$.
2. $\beta(x) \neq x$ y $\alpha(x) = x$.
3. $\alpha(x) = x$ y $\beta(x) = x$.

Como el tercer caso es trivial y el segundo caso es análogo al primero, solo veamos el primer caso: Como $\alpha$ es inyectiva, la primera ecuación implica que $\alpha(\alpha(x)) \neq \alpha(x)$. Es decir, $\alpha$ mueve a $\alpha(x)$ y por lo tanto (como $\alpha$ y $\beta$ son disjuntas), $\beta$ fija a $\alpha(x)$. Finalmente,

$$\begin{aligned} \alpha(\beta(x)) &= \alpha(x) && \text{(pues } \beta(x) = x\text{)} \\ &= \beta(\alpha(x)). && \text{(pues } \beta \text{ fija a } \alpha(x)\text{)} \end{aligned}$$

# Comentario

En lo que sigue, demostraremos que toda permutación $\alpha \in S_n$ es un ciclo o un producto de ciclos disjuntos. Antes de ver el caso general, veamos como factorizar a

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix} \in S_9$$

en ciclos disjuntos.

Como $\alpha(1) = 6$, entonces $\alpha$ empieza con "(16". Como $\alpha(6) = 3$, entonces $\alpha$ continua con "(163". Como $\alpha(3) = 1$, el paréntesis se cierra y $\alpha$ continua con "(163)". El entero mas chico que no ha aparecido es 2. Por lo tanto, $\alpha$ continua con "(163)(2". Como $\alpha(2) = 4$, entonces $\alpha$ continua con "(163)(24". Continuando de esta manera, eventualmente llegamos a la siguiente factorización de $\alpha$ en ciclos disjuntos

$$\alpha = (163)(24)(5)(789)$$

# Toda permutación en $S_n$ es un ciclo o un producto de ciclos disjuntos

**Teorema 2**

Toda permutación en $S_n$ es un ciclo o un producto de ciclos disjuntos.

*Demostración.* Antes de empezar, un poquito de notación. Dado $\sigma \in S_n$, sea

$$F_\sigma := \left\{x \in \{1, \ldots, n\} \mid \sigma \text{ fija a } x\right\}.$$

Ahora si, supongamos que $\alpha \in S_n$. Procedemos por inducción sobre $|F_\alpha|$.

*Paso base*: $|F_\alpha| = 0$.

Entonces $\alpha$ es la identidad y por lo tanto, $\alpha$ es un 1-ciclo.

*Paso inductivo*: Supongamos que $|F_\alpha| = n > 0$ y que toda $\sigma \in S_n$ con $|F_\sigma| < n$ es un ciclo o un producto de ciclos disjuntos.

Como $|F_\alpha| = n > 0$, entonces $F_\alpha \neq \emptyset$ y por lo tanto, existe algún $i_1 \in F_\alpha$. Definimos

$$i_2 \coloneqq \alpha(i_1),\ i_3 \coloneqq \alpha(i_2),\ \ldots,\ i_r = \alpha(i_{r-1})$$

donde $r$ es el menor entero para el cual $\alpha(i_r) \in \{i_1, \ldots, i_r\}$ (la lista $i_1, i_2, \ldots, i_k, \ldots$ no puede continuar para siempre sin repeticiones porque solo toma $n$ distintos valores).

Veamos que $\alpha(i_r) = i_1$.

De lo contrario, como (por definición) $\alpha(i_r) \in \{i_1, \ldots, i_r\}$, entonces $\alpha(i_r) = i_j$ para alguna $j \in \{2, \ldots, r\}$. Pero $i_j = \alpha(i_{j-1})$ y por lo tanto $\alpha(i_r) = \alpha(i_{j-1})$. Como $\alpha$ es inyectiva, lo anterior implica que $i_r = i_{j-1}$, lo cual contradice la hipótesis "$r$ es el menor entero para el cual $\alpha(i_r) \in \{i_1, \ldots, i_r\}$".

Usando la notación que usamos en el comentario anterior, acabamos de demostrar que "$\alpha$ empieza con $(i_1 i_2 \ldots i_r)$".

Ahora bien, denotemos $\sigma \coloneqq (i_1 i_2 \ldots, i_r)$. Si $r = n$, entonces $\alpha$ es igual al ciclo $\sigma$ y no hay nada mas que probar. Por eso, supongamos que $r < n$. Sea $\alpha' : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tal que

$$\alpha'(x) = \begin{cases} \alpha(x) & \text{si } x \notin \{i_1, \ldots, i_r\} \\ x & \text{si } x \in \{i_1, \ldots, i_r\} \end{cases}$$

Usando la pura definición, es fácil ver

1. que $\alpha' \in S_n$,
2. que $|F_{\alpha'}| < |F_\alpha|$
3. que $\alpha$ y $\sigma$ son permutaciones disjuntas, y
4. que $\alpha = \sigma\alpha'$.

Juntando lo anterior con la hipótesis de inducción, obtenemos lo deseado. $\square$

# Todo $l$-ciclo puede ser escrito como el producto de $l-1$ transposiciones

**Lema 3**

Supongamos que $n \in \mathbb{Z}_{\geq 2}$ y que $i_1, \ldots, i_l \in \{1, \ldots, n\}$ son números distintos con $l \geq 2$. Entonces

$$(i_1 i_2 \cdots i_l) = (i_1 i_l)(i_1 i_{l-1}) \cdots (i_1 i_3)(i_1 i_2).$$

*Demostración.* Procediendo por inducción sobre $l$ y usando la igualdad

$$(i_1 i_2 \cdots i_l) = (i_1 i_l)(i_1 i_2 \cdots i_{l-1})$$

obtenemos lo deseado. □

# Toda permutación es un producto de transposiciones y la paridad del numero de factores es invariante

## Lema 4

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Entonces

1. Todo $\alpha \in S_n$ puede ser escrita como el producto de transposiciones.
2. Si $\sigma_1, \ldots, \sigma_s, \tau_1, \ldots, \tau_t \in S_n$ son transposiciones tales que

$$\sigma_1 \sigma_2 \cdots \sigma_s = \tau_1 \tau_2 \cdots \tau_t$$

entonces

$$s \text{ es par} \iff t \text{ es par} \quad \text{y} \quad s \text{ es impar} \iff t \text{ es impar.} \tag{1}$$

La demostración de (1) es consecuencia inmediata de los dos resultados anteriores: (i) toda permutación es un ciclo o un producto de ciclos disjuntos y (ii) todo ciclo puede ser escrito como el producto de transposiciones.
La demostración de (2) es bastante mas complicada y como los métodos usados en esta no son particularmente relevantes para el resto del curso, la omitimos.

# La paridad y el signo de una permutación

En resumen, el lema anterior nos dice (i) que toda permutación puede ser escrita como un producto de transposiciones y (ii) que la paridad del numero de factores de cualquier factorización en transposiciones es invariante. Esta invarianza nos permite hacer la siguiente definición.

## Definición

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Decimos que una permutación $\sigma \in S_n$ es **par** si es el producto de un numero par de transposiciones y análogamente, decimos que es **impar** si es el producto de un numero impar de transposiciones.

La existencia de la factorización en transposiciones implica que toda permutación es par ó impar. Para cada $\sigma \in S_n$ definimos el **signo de** $\sigma$ por

$$\operatorname{sgn}(\sigma) := \begin{cases} +1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

En el lema 3 demostramos que todo $l$-ciclo puede ser escrito como el producto de $l-1$ transposiciones. Por lo tanto, un $l$-ciclo es par si y solo si $l-1$ es par.

# $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$

## Proposición 5

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Si $\alpha, \beta \in S_n$, entonces

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$$

En particular, si consideramos a $\{+1, -1\}$ como un subgrupo multiplicativo de $\mathbb{Z}$, entonces la función $\alpha \mapsto \operatorname{sgn}(\alpha)$ define un homomorfismo de grupos.

La demostración de la igualdad es por casos sobre la paridad de $\alpha$ y $\beta$. También es util recordar (i) que la suma de dos números pares es un numero par, (ii) que la suma de dos números impares es par, y (iii) que la suma de un numero par con un numero impar es un numero impar. La demostración de que $\alpha \mapsto \operatorname{sgn}(\alpha)$ es un homomorfismo es muy sencilla y se la dejamos al lector.

# El grupo alternante $A_n$

## Definición

Para cada $n \in \mathbb{Z}_{\geq 2}$, definimos el **grupo alternante** $A_n$ como el subgrupo de $S_n$ que consiste de todas las permutaciones pares de $S_n$.

Notemos que $A_n$ es el kernel de el homomorfismo $\alpha \mapsto \operatorname{sgn}(\alpha)$ y por lo tanto, $A_n$ es un subgrupo normal de $S_n$ (recuerda que el kernel de un homomorfismo siempre es un subgrupo normal).

Por otro lado, notemos que si $\sigma \in S_n$, entonces

$$\sigma A_n = \{\sigma\alpha \mid \alpha \in A_n\} = \begin{cases} A_n & \text{si } \sigma \text{ es par} \\ S_n \setminus A_n & \text{si } \sigma \text{ es impar} \end{cases}$$

y por lo tanto,

$$[S_n : A_n] = |S_n/A_n| = 2.$$

## $S_3$ y $A_3$

El lector podrá fácilmente verificar (por eliminación) que

$$S_3 = \big\{e, (12), (13), (23), (123), (132)\big\}$$

y por lo tanto, como $(123) = (12)(23)$ y $(132) = (13)(32)$, entonces

$$A_3 = \big\{e, (123), (132)\big\}\,.$$

Por otro lado, se puede demostrar que

$$S_3,\ A_3,\ \big\langle(12)\big\rangle,\ \big\langle(13)\big\rangle,\ \big\langle(23)\big\rangle,\ \{e\}$$

son todos los subgrupos de $S_3$.

# Comentario

Finalizamos esta sección con 2 resultados que serán muy útiles.

## Proposición 6

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Si $(i_1 i_2 \cdots i_l) \in S_n$ es un $l$-ciclo y $\theta \in S_n$ es cualquier permutación, entonces

$$\theta(i_1 i_2 \cdots i_l)\theta^{-1} = \big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)\,.$$

*Demostración.* Primero notemos que para toda $j \in \{1, \ldots, l-1\}$ tenemos que

$$\begin{aligned}\left(\theta(i_1 i_2 \cdots i_l)\theta^{-1}\right)\left(\theta(i_j)\right) = \theta\left((i_1 i_2 \cdots i_l)(i_j)\right) &= \theta(i_{j+1}) \\ &= \big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)\left(\theta(i_j)\right)\end{aligned}$$

y análogamente,

$$\left(\theta(i_1 i_2 \cdots i_l)\theta^{-1}\right)\left(\theta(i_l)\right) = \big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)\left(\theta(i_l)\right)$$

Por lo tanto, $\theta(i_1 i_2 \cdots i_l)\theta^{-1}$ y $\big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)$ coinciden en toda $\theta(i_j)$.

Para concluir, notemos que los elementos fijados por $\big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)$ son precisamente los elementos de

$$\{1,\ldots,n\}\setminus\{\theta(i_1),\theta(i_2),\cdots,\theta(i_l)\}. \tag{2}$$

El lector podrá verificar que los elementos fijados por $\theta(i_1 i_2\cdots i_l)\theta^{-1}$ también son precisamente los elementos de (2). Como $\theta(i_1 i_2\cdots i_l)\theta^{-1}$ y $\big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)$ coinciden en toda $\theta(i_j)$, lo anterior implica la igualdad deseada:

$$\theta(i_1 i_2\cdots i_l)\theta^{-1} = \big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)\,.$$

□

# Un par de curiosas igualdades

**Lema 7**

Supongamos que $n \in \mathbb{Z}_{\geq 3}$ y que $i, j, k \in \{1, \ldots, n\}$. Entonces

- $(ijk) = (ij)(ik)$.
- $(ij)(kl) = (ijk)(jkl)$.

La demostración es muy sencilla y por eso se la dejamos al lector.

# $A_n$ es generado por los 3-ciclos si $n \geq 3$

## Proposición 8

Si $n \in \mathbb{Z}_{\geq 3}$, entonces $A_n$ es generado por los 3-ciclos, es decir,

$$A_n = \left\langle \{(ijk) \mid i, j, k \in \{1, \ldots, n\}\} \right\rangle .$$

*Demostración.*

$\supset$) Si $\sigma \in \left\langle \{(ijk) \mid i, j, k \in \{1, \ldots, n\}\} \right\rangle$, entonces $\sigma$ es de la forma

$$(i_1 j_1 k_1)(i_2 j_2 k_2) \cdots (i_m j_m k_m). \tag{3}$$

Usando la igualdad $(ijk) = (ij)(ik)$ es fácil ver que podemos reescribir (3) como un producto de $2m$ transposiciones y por lo tanto, $\sigma \in A_n$.

$\subset$) Supongamos que $\sigma \in A_n$. Por definición, existe $m \in \mathbb{Z}$ par y $\sigma_1, \ldots, \sigma_m$ transposiciones tales que

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_{m-1} \sigma_m. \tag{4}$$

Usando la igualdad $(ij)(kl) = (ijk)(jkl)$ y el hecho de que $m$ es par, es fácil ver que podemos reescribir el lado derecho de (4) como un producto de 3-ciclos.