El Grupo Simétrico.

Denotamos por $[\![1,n]\!]$, $\forall\, n\in\mathbb{N}$, al conjunto:
$$[\![1,n]\!]=\{1,2,\dots,n\}.$$
y, S_n es el conjunto:
$$\forall n\in\mathbb{N},\quad S_n=\{\sigma:[\![1,n]\!]\to[\![1,n]\!]\mid \sigma \text{ es biyección}\}$$
Si $\sigma\in S_n$, dada por:
$$\forall\, i\in[\![1,n]\!],\ i\mapsto\sigma(i)$$
Expresamos:
$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$$
donde $\{\sigma(1),\sigma(2),\dots,\sigma(n)\}=[\![1,n]\!]$. Tenemos que S_n es grupo con la composición de funciones. Si $\sigma,\theta\in S_n\Rightarrow\sigma\circ\theta\in S_n$.
Por simplicidad, expresamos $\sigma\circ\theta=\sigma\theta$ (por yuxtaposición). Además, la identidad de S_n es:
$$e=id_{[\![1,n]\!]}=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$$
Si $\sigma\in S_n$:
$$\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$$

Ejemplos.

1) Si $\sigma=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ y $\theta=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$, entonces:
$$\sigma\circ\theta=\sigma\theta=\begin{pmatrix}1&2&3&4\\4&2&3&1\\4&1&2&3\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

Def. Sea $n\in\mathbb{N}$ y $\sigma\in S_n$, y $i\in[\![1,n]\!]$. Decimos que **σ mueve a i**, si $\sigma(i)\neq i$. En caso contrario, decimos que **σ deja fijo a i**.
Denotamos por $M_\sigma=\{i\in[\![1,n]\!]\mid\sigma(i)\neq i\}$.

2) En 1), $M_\sigma = \{1,2,3\}$ y $M_\theta = \{1,4\}$. En dicho ejemplo, se observa que $\sigma\theta \neq \theta\sigma$, pues $\sigma\theta(1) = 4$ y $\theta\sigma(1) = 3$.

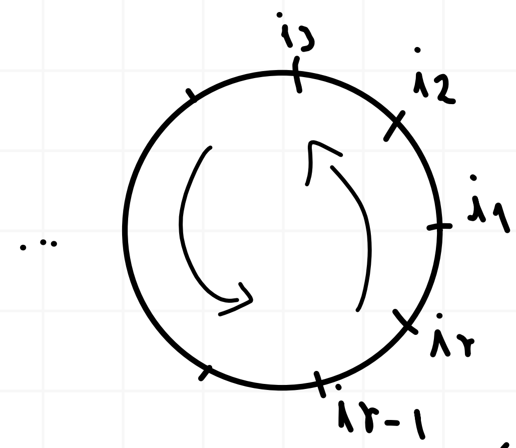
Def. Sea $\sigma \in S_n$ y $r \in [\![1,n]\!]$. Decimos que σ es un <u>r-ciclo</u> si existen $i_1, \dots, i_r \in [\![1,n]\!]$ distintos entre sí, tales que σ está dada como sigue:

$$\forall\, i \in [\![1,n]\!],\ \sigma(i) = \begin{cases} i & \text{si } i \notin \{i_1, i_2, \dots, i_r\}. \\ i_{k+1} & \text{si } i = i_k \text{ con } 1 \leq k < r. \\ i_1 & \text{si } i = i_r. \end{cases}$$

Este r-ciclo lo expresamos como:

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

Donde $M_\sigma = \{i_1, \dots, i_r\}$. Si $r = 1$, entonces $\sigma = e = (1) = (2) = \dots = (n)$. Si $r \geq 2$:



Obs: Si $\sigma = (i_1\ i_2 \dots i_r)$ es un r-ciclo, entonces:

$$\sigma = (i_1 \dots i_r) = (i_2\ i_3 \dots i_r\ i_1)$$
$$= (i_3\ i_4 \dots i_r\ i_1\ i_2) \dots = (i_r\ i_1 \dots i_{r-1})$$

Más aún, tenemos que si $i \in M_\sigma = \{i_1, \dots, i_r\}$:

$$\sigma = (\underset{i_j}{\underset{\parallel}{i}}\ \ \underset{i_{j+1}}{\underset{\parallel}{\sigma(i)}}\ \ \underset{i_{j+2}}{\underset{\parallel}{\sigma^2(i)}}\ \dots\ \underset{i_k}{\underset{\parallel}{\sigma^{r-1}(i)}})$$

Donde $k = j-1$ si $j \neq 1$ y $k = r$ si $j = 1$.

Proposición.

Sea $\sigma \in S_n$ un r-ciclo. Entonces el orden de σ es r.

Dem: Con $r \geq 2$ (el caso $r = 1$ es inmediato).

Si $i \notin M_\sigma \Rightarrow \sigma(i) = i \Rightarrow \sigma^r(i) = i$.

Si ahora $i \in M_\sigma$, digamos que $i = i_1$ (pues no importa cuál se escoja primero), donde $\sigma = (i_1\ i_2 \dots i_r)$, entonces:

$$\sigma^j(i) = i_{j+1},\ \forall\ 1 \leq j < r.$$

Es decir:

$$\sigma(i) = \sigma(i_1) = i_2$$

$$\sigma^2(i) = \sigma(i_2) = i_3$$

$$\vdots$$

$$\sigma^{r-1}(i) = \sigma(\sigma^{r-2}(i)) = \sigma(i_{r-1}) = i_r$$

$$\Rightarrow \sigma^r(i) = \sigma(i_r) = i_1 = i$$

por tanto, $\sigma^r(i) = i$, $\forall\ i \in [\![1, n]\!]$ y $|\sigma| = r$, pues si $|\sigma| < r$, entonces σ no sería un r-ciclo. En efecto, notemos que si $|\sigma| = k < r$:

$$\sigma^k(i_1) = i_{k+1} \neq i_1, \text{ pues } 1 < k+1 \leq r.$$

Por tanto, $|\sigma| = r$.

Def. Si σ es un r-ciclo con $r \geq 2$, entonces decimos que σ es una *transposición*.

Ejemplo.

1) Sabemos que en S_3 tenemos $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ y $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, entonces $\sigma = (1\ 2)$ y $\pi = (1\ 2\ 3)$, los cuales son elementos que generan a S_3, donde $|\sigma| = 2$, $|\pi| = 3$ y $\pi\sigma = \sigma\pi^2$. Así que $S_3 = \{e, \sigma, \pi, \pi^2, \sigma\pi, \sigma\pi^2\}$.

Def. Sean $\sigma, \theta \in S_n$. Decimos que σ y θ son permutaciones disjuntas ó ajenas si $M_\sigma \cap M_\theta = \emptyset$.

Obs: Supongamos que σ es r-ciclo y θ es s-ciclo. Digamos que $\sigma = (i_1\ i_2 \dots i_r)$ y $\theta = (j_1\ j_2 \dots j_s)$. Entonces σ y θ son disjuntos si y sólo si $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$.

EJEMPLO.

1) Si $\sigma = (1\ 3\ 5)$ y $\pi = (2\ 7\ 4)$, entonces σ y π son disjuntos en S_n, y además:

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 & \dots \end{pmatrix}$$

y

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 & \dots \end{pmatrix}$$

$$\Rightarrow \sigma\pi = \pi\sigma$$

Proposición.

Sean $\sigma, \theta \in S_n$ disjuntos. Entonces, $\sigma\theta = \theta\sigma$.

Dem:

Tenemos que $M_\sigma \cap M_\theta = \emptyset$. Por lo cual,

$$[\![1, n]\!] = M_\sigma \,\dot\cup\, M_\theta \,\dot\cup\, ([\![1, n]\!] \setminus (M_\sigma \cup M_\theta))$$

Sea $i \in [\![1, n]\!]$. Entonces:

a) $i \in [\![1, n]\!] \setminus \{M_\sigma \cup M_\theta\}$, entonces $\sigma(i) = i$ y $\theta(i) = i \Rightarrow \sigma\theta(i) = i = \theta\sigma(i)$.

b) $i \in M_\sigma$: Entonces como $M_\sigma \cap M_\theta = \emptyset \Rightarrow \theta(i) = i$. Luego:

$$(\sigma\theta)(i) = \sigma(\theta(i)) = \sigma(i)$$
$$(\theta\sigma)(i) = \theta(\sigma(i)) = \sigma(i), \text{ pues}$$

Si $\sigma(i)$ es movido por θ, $\sigma(i) \in M_\theta$, pero $\sigma(i) \in M_\sigma$ pues σ mueve a i y, por tanto a $\sigma(i)$. Luego $M_\theta \cap M_\sigma \neq \emptyset$ #c. Por tanto $\theta\sigma(i) = \sigma(i)$. Así:

$$\sigma\theta(i) = \theta\sigma(i)$$

σ mueve a $\sigma(i)$, pues de otra forma si $\sigma(i) \notin M_\sigma$:

$$\Rightarrow \sigma(\sigma(i)) = \sigma(i)$$

$$\Rightarrow \sigma(i) = i \text{ #c.}$$

c) $i \in M_\theta$: Similarmente a b) se cumple el resultado.

Por a), b) y c), $\sigma\theta = \theta\sigma$.

q.e.d.

Obs: Si σ es un r-ciclo, entonces σ^{-1} es un r-ciclo y

$$\sigma^{-1} = (\sigma^{r-1}(i) \ \sigma^{r-2}(i) \ \dots \ \sigma(i) \ i)$$

Donde $i \in M_\sigma$. En efecto, como:

$$\sigma^{-1}\sigma = (\sigma^{r-1}(i) \dots i)(i \ \sigma(i) \dots \sigma^{r-1}(i))$$

Lema.

Sea $n\in\mathbb{N}$. En S_n, si $\sigma,\theta\in S_n$ son dos r-ciclos $\ni$ $\sigma^k(i)=\theta^k(i)$ $\forall k\in\mathbb{N}$, con $i\in M_\sigma$ entonces $\sigma=\theta$.

Dem:

Sea $i\in M_\sigma$, entonces:

$$\begin{aligned}\sigma &= (\sigma(i)\ \sigma^2(i)\ \dots\ \sigma^r(i))\\ &= (\theta(i)\ \theta^2(i)\ \dots\ \theta^r(i))\\ &= \theta\end{aligned}$$

q.e.d.

Sea $\sigma\in S_n$ arbitrario. Tenemos que la inyección canónica

$$\begin{aligned}\langle\sigma\rangle &\to S_n\\ \theta &\mapsto \theta\end{aligned}$$

es un monomorfismo. Luego, tenemos que $\langle\sigma\rangle$ actúa en $[\![1,n]\!]$ bajo la acción: $\theta\cdot i=\sigma(i)$, $\forall i\in[\![1,n]\!]$ y $\theta\in\langle\sigma\rangle$.

Recordemos que si $i,j\in[\![1,n]\!]$, entonces:

$$i\sim j \iff \exists\,\theta\in\langle\sigma\rangle \ni \theta\cdot i=j$$

La cual es relación de equivalencia sobre $[\![1,n]\!]$. Las clases de equivalencia son sus órbitas. Es decir: si $i\in[\![1,n]\!]$ entonces la órbita de i es:

$$\langle\sigma\rangle\cdot i=\{\theta(i)\mid\theta\in\langle\sigma\rangle\}$$

Si $m=|\sigma|$, entonces:

$$\langle\sigma\rangle\cdot i=\{i,\sigma(i),\dots,\sigma^{m-1}(i)\}$$

Si $\sigma^l(i)=\sigma^t(i)$ con $0\leq t<l\leq m-1$, entonces tenemos que $1\leq l-t\leq m-1$ con $\sigma^{l-t}(i)=i$. Si esto ocurre, i.e $|\langle\sigma\rangle\cdot i|<m$, entonces elegimos

K_0 el mínimo natural tal que $\sigma^{K_0}(i) = i$.

Entonces, tenemos que:

$$\langle\sigma\rangle \cdot i = \{i, \sigma(i), \dots, \sigma^{K_0 - 1}(i)\}$$

donde $|\langle\sigma\rangle \cdot i| = K_0$.

Sean $Y_1, Y_2, \dots, Y_s$ las distintas órbitas de $\langle\sigma\rangle$ en $[\![1, n]\!]$. Así que:

$$[\![1, n]\!] = \bigcup_{t=1}^{s} Y_t$$

Para cada $1 \leq t \leq s$, sea $i_t \in Y_t$ con $|Y_t| = K_t$. Así que:

$$\forall\, 1 \leq t \leq s,\ Y_t = \{i_t, \sigma(i_t), \dots, \sigma^{K_t - 1}(i_t)\}$$

Definimos para cada $1 \leq t \leq s$, el K_t-ciclo:

$$\sigma_t = (i_t\ \ \sigma(i_t)\ \dots\ \sigma^{K_t - 1}(i_t))$$

Afirmamos que:

$$\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$$

En efecto, sea $j \in [\![1, n]\!] \Rightarrow \exists!\ 1 \leq l \leq s \ni j \in Y_l$. Luego como $\sigma_k(j) = j$, $\forall\, k \in \{1, \dots, s\} \setminus \{l\}$, entonces:

$$\begin{aligned}(\sigma_1 \cdot \ldots \cdot \sigma_s)(j) &= \sigma_l(j) \\ &= \sigma_l(\sigma^u(i_l))\end{aligned}$$

Con $0 \leq u \leq K_l - 1$, tal que $j = \sigma^u(i_l)$. Así:

$$\begin{aligned}&= \sigma^{u+1}(i_l) \\ &= \sigma(j)\end{aligned}$$

Por tanto: $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$. En resumen, toda permutación de S_n se expresa como un producto de ciclos disjuntos, por lo cual, podemos suponer que $K_1 \leq K_2 \leq \ldots \leq K_s$.

Esta descomposición se conoce como la estructura cíclica de la permutación.

Es decir, si $\sigma \in S_n$, expresamos la descomposición cíclica de σ como:

$$(\cdot)\ldots(\cdot)(\cdot\cdot)\ldots(\cdot\cdot)(\cdots)\ldots(\cdots)\ldots(\cdot\ldots\cdot)$$

Ejemplo.

1) En S_{10}:

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

Así $Y_1 = \langle\sigma\rangle\cdot 3$, $Y_2 = \langle\sigma\rangle\cdot 5$ y $Y_3 = \langle\sigma\rangle\cdot 1$ con órdenes $k_1 = 1$, $k_2 = 4$ y $k_3 = 5$. Luego $\sigma_1 = (3)$, $\sigma_2 = (5\ 10\ 7\ 6)$ y $\sigma_3 = (1\ 2\ 4\ 8\ 9)$.

Teorema.

Toda permutación de S_n distinta de la identidad, se expresa de manera única salvo orden, como un producto de permutaciones disjuntas.

Dem:

Ejercicio.

Primero, $\sigma \neq e$. Supongu:

$$\underset{k_1}{\sigma_1}\ \underset{k_2}{\sigma_2} \cdots \underset{k_s}{\sigma_s} = \sigma = \underset{l_1}{\theta_1} \cdot \ldots \cdot \underset{l_f}{\theta_f}$$

Veamos sobre σ. Sea $k \in [\![1, s]\!]$. Tenemos 2 casos:

1) σ_k deja a todos fijos, en este caso $\sigma_k = e$ ...

2) σ_k mueve a i.

Hay que proceder por inducción de $1 \leqslant k \leqslant s$.

NO! Proceder por inducción sobre el número s de $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$.

Def. La descomposición única de ciclos disjuntos de una permutación σ, donde $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$, σ_i son r_i-ciclos, $\forall\ i \in [\![1, s]\!]$. $\sigma_1, \ldots, \sigma_s$ son disjuntos con $1 \leqslant r_1 \leqslant r_2 \leqslant \ldots \leqslant r_s$, se dice que es la descomposición cíclica de σ. Su estructura cíclica es:

$$\sigma = \underbrace{(\cdot \ldots \cdot)}_{r_1\text{-puntos}} \cdot \ldots \cdot \underbrace{(\cdot \ldots \cdot)}_{r_s\text{-puntos.}}$$

EJEMPLOS.

1) S_4 no tiene elementos de orden 6. Si $\sigma \in S_4$ con $\sigma \neq e$, entonces las posibles estructuras cíclicas de σ son:

	Orden
$\sigma = (\cdot)(\cdot)(\cdot\ \cdot) \longrightarrow$	2
$\sigma = (\cdot)(\cdot\ \cdot\ \cdot) \longrightarrow$	3
$\sigma = (\cdot\ \cdot)(\cdot\ \cdot) \longrightarrow$	2
$\sigma = (\cdot\ \cdot\ \cdot\ \cdot) \longrightarrow$	4

i.e, todos los elementos de S_4 son de orden 2, 3 ó 4.

Proposición.

Sea $\sigma \in S_n$, $\sigma \neq e$, con descomposición cíclica $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$ con $r_1 \leqslant \cdots \leqslant r_s$. Entonces $|\sigma| = \text{mcm}\{r_1, \ldots, r_s\}$.

Dem:

Sea $|\sigma| = m$ y $r = \text{mcm}\{r_1, \ldots, r_s\}$. Por definición, r:

a) $r_i \mid r$, $\forall\ i \in [\![1, s]\!]$.

b) Si $l \in \mathbb{N}$ m $r_i \mid l$, $\forall\ i \in [\![1, s]\!]$, entonces $r \mid l$.

Puesto que $r_i \mid r$, $\forall\ i \in [\![1, s]\!]$, expresamos a r como: $r = r_i t_i$, $\forall\ i \in [\![1,$

$s]\!]$. Por tanto:

$$\sigma^r = (\sigma_1 \cdot \ldots \cdot \sigma_s)^r = \sigma_1^{r_1 t_1} \cdot \sigma_2^{r_2 t_2} \cdot \ldots \cdot \sigma_s^{r_s t_s}$$
$$= e^{t_1} \cdot e^{t_2} \cdot \ldots \cdot e^{t_s}$$
$$= e$$

$$\Rightarrow m \mid r, \Rightarrow m \leqslant r.$$

Por otro lado, afirmamos que $\sigma_i^m = e$, $\forall i \in [\![1, s]\!]$. Tenemos:

$$e = \sigma^m$$
$$= \sigma_1^m \cdot \ldots \cdot \sigma_s^m$$

Sea $K \in [\![1, n]\!]$, si σ_j mueve a K, con $j \in [\![1, s]\!]$, entonces:

$$\sigma^m(K) = \sigma_j^m(K) = K, \text{ pues } \sigma^m = e$$

por tanto $\sigma_j^m = e$, $\forall j \in [\![1, s]\!]$. Luego, por b):

$$\sigma_i^m = e, \forall i \in [\![1, s]\!] \Rightarrow r_i \mid m, \forall i \in [\![1, s]\!] \Rightarrow m \mid r.$$

Como $r \mid m$ y $m \mid r \Rightarrow m = r$.

q.e.d.

Proposición.

Sea $\sigma \in S_n$, σ un r-ciclo, con $r \geqslant 2$. Entonces, cualquier conjugado de σ es un r-ciclo.

Dem:

Supongamos que $\sigma = (i_1\ i_2 \ldots i_r)$. Afirmamos que $\forall \beta \in S_n$, $\beta \sigma \beta^{-1}$ es un r-ciclo, dado como:

$$\beta \sigma \beta^{-1} = (\beta(i_1) \ldots \beta(i_r))$$

En efecto, notemos que:

$$[\![1, n]\!] = \{\beta(1), \ldots, \beta(n)\}$$

Sea $\beta(i) \in [\![1, n]\!]$, con $1 \leqslant i \leqslant n$. Tenemos 2 casos:

1) $i \notin M_\sigma = \{i_1, \dots, i_r\}$, entonces:

$$\beta \sigma \beta^{-1}(\beta(i)) = \beta\sigma(i) = \beta(i) = \beta(i)$$

Además:

$$(\beta(i_1)\ \beta(i_2) \dots \beta(i_r))(\beta(i)) = \beta(i)$$

$$\therefore \beta\sigma\beta^{-1}(\beta(i)) = (\beta(i_1) \dots \beta(i_r))(\beta(i)).$$

2) $i \in \{i_1, i_2, \dots, i_{r-1}\}$: Suponemos $i = i_j$ con $j \in [\![1, r-1]\!]$,

$$\beta\sigma\beta^{-1}(\beta(i)) = \beta\sigma(i_j) = \beta(i_{j+1})$$

y:

$$(\beta(i_1) \dots \beta(i_r))(\beta(i_j)) = \beta(i_{j+1})$$

$$\therefore \beta\sigma\beta^{-1}(\beta(i)) = (\beta(i_1) \dots \beta(i_r))(\beta(i_j))$$

3) $i = i_r$, entonces:

$$\beta\sigma\beta^{-1}(\beta(i_r)) = \beta\sigma(i_r) = \beta(i_1)$$

$$(\beta(i_1) \dots \beta(i_r))(\beta(i_r)) = \beta(i_1)$$

$$\therefore \beta\sigma\beta^{-1}(\beta(i_r)) = (\beta(i_1) \dots \beta(i_r))(\beta(i_r))$$

por 1)-3), $\beta\sigma\beta^{-1}$ es un r-ciclo.

q.e.d.

Ejemplo.

1) Sea $\sigma = (5\ 1\ 4\ 3\ 2)$ y $\beta = (1\ 2)(3\ 4)$

$$\Rightarrow \beta\sigma\beta^{-1} = (\beta(5)\ \beta(1)\ \beta(4)\ \beta(3)\ \beta(2)) = (5\ 2\ 3\ 4\ 1)$$

Si C es la clase de conjugación de un r-ciclo σ, entonces $C = \{\beta\sigma\beta^{-1} \mid \beta \in S_n\}$

Proposición.

En las condiciones del párrafo anterior, tenemos que C es la clase de conjugación de σ constituida de todos los r-ciclos.

Dem:

Sea $\theta \in S_n$ un r-ciclo arbitrario, digamos:

$$\theta = (j_1 \; j_2 \ldots j_r)$$

tenemos que $\sigma = (i_1 \; i_2 \ldots i_r)$. Claramente todos los elementos de C son r-ciclos. Probaremos entonces que $\exists \, \beta \in S_n \ni \theta = \beta \sigma \beta^{-1}$.

Sea $\beta : [\![1,n]\!] \to [\![1,n]\!]$ dada por:

$$\forall \, i \in [\![1,n]\!], \; \beta(i) = \begin{cases} j_k & \text{si } i = i_k \text{ para algún } k \in [\![1,r]\!] \\ l(i) & \end{cases}$$

Donde $l : [\![1,n]\!] \setminus \{i_1, i_2, \ldots, i_r\} \to [\![1,n]\!] \setminus \{j_1, \ldots, j_r\}$ es una biyección arbitraria. Claramente $\beta \in S_n$, así:

$$\beta \sigma \beta^{-1} = (\beta(i_1) \; \beta(i_2) \ldots \beta(i_r)) = (j_1 \; j_2 \ldots j_r) = \theta$$

$\Rightarrow \theta \in C$, así C es el conjunto de todos los r-ciclos.

q.e.d.

Obs:

1) Si $\sigma = e \Rightarrow C(\sigma) = C(e) = \{e\}$.

2) Sabemos que si σ es un r-ciclo, entonces:

$$|C(\sigma)| = \frac{|S_n|}{|N_{S_n}(\sigma)|}$$

donde $N_{S_n}(\sigma) = \{\beta \in S_n \mid \beta \sigma \beta^{-1} = \sigma\}$. Notemos que el l de la función se puede construir de $(n-r)!$, como $\beta(i_k) = i_k$, $\forall \, k \in [\![1,r]\!]$, entonces $|N_{S_n}(\sigma)| = (n-r)!$, tomando los r-ciclos con una única representación. Por tanto:

$$|C(\sigma)| = \frac{n!}{(n-r)!} \quad \left(= \frac{n!}{r(n-r)!} \checkmark \text{ según el prof.} \right)$$

3) La cantidad de transposiciones es:

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

Teorema.

Sean $\sigma, \theta \in S_n$ arbitrarios. Entonces σ y θ tienen la misma estructura cíclica $\Leftrightarrow$ σ y θ tienen la misma estructura cíclica.

Dem:

$\Rightarrow$) Supóngase que σ y θ son conjugados, $\exists$ $\beta \in S_n$ $\ni$ $\beta\sigma\beta^{-1} = \theta$. Expresamos a σ en su descomposición cíclica:

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_s$$

Cada σ_i es un r_i-ciclo con $1 \leq r_1 \leq \ldots \leq r_s \leq n$. Entonces:

$$\begin{aligned} \Rightarrow \theta &= \beta\sigma\beta^{-1} \\ &= \beta\sigma_1\sigma_2\ldots\sigma_s\beta^{-1} \\ &= (\beta\sigma_1\beta^{-1})(\beta\sigma_2\beta^{-1})\cdot\ldots\cdot(\beta\sigma_s\beta^{-1}) \end{aligned}$$

con $\sigma_i = (j_{i_1}\ j_{i_2}\ \ldots\ j_{ir_i})$, $\forall\ i \in [\![1, s]\!]$, entonces:

$$\beta\sigma_i\beta^{-1} = (\beta(j_{i_1})\ \beta(j_{i_2}) \ldots \beta(j_{ir_i}))$$

por ser β biyección, entonces $M_{\beta\sigma_i\beta^{-1}} \cap M_{\beta\sigma_j\beta^{-1}} = \emptyset$, $\forall\ i, j \in [\![1, s]\!]$ luego $\beta\sigma_i\beta^{-1}$ es un r_i-ciclo. Por tanto, al ser r_i-ciclos disjuntos, la descomposición anterior es la misma que la de θ. i.e σ y θ tienen la misma descomposición cíclica.

$\Leftarrow$) Supongamos que σ y θ tienen la misma estructura cíclica, digamos:

$$\sigma = \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_s.$$
$$\theta = \theta_1\theta_2 \cdot \ldots \cdot \theta_s.$$

Donde cada σ_i y θ_i es un r_i-ciclo, con $1 \leq r_1 \leq r_2 \leq \ldots \leq r_s \leq n$. Podemos expresar: $\forall\ i \in [\![1, s]\!]$:

$$\sigma_i = (j_{i_1}\ j_{i_2}\ \dots\ j_{ir_i}),\ y$$
$$\theta_i = (K_{i_1}\ K_{i2}\ \dots\ K_{ir_i})$$

Notemos que:

$$\{ j_{it} \mid 1 \leq t \leq r_i,\ i \in [\![1,s]\!] \} = \{ K_{it} \mid 1 \leq t \leq r_i,\ i \in [\![1,s]\!] \}$$

Definimos $\beta \in S_n$, como:

$$\beta(j_{it}) = K_{it},\ \forall\ 1 \leq t \leq r_i,\ i \in [\![1,s]\!].$$

Entonces

$$\begin{aligned} \beta\sigma\beta^{-1} &= (\beta\sigma_1\beta^{-1}) \cdot \dots \cdot (\beta\sigma_s\beta^{-1}) \\ &= \cdots (\beta(j_{i_1})\ \beta(j_{i2})\ \dots\ \beta(j_{ir_i})) \cdots \\ &= \cdots (K_{i1}\ K_{i2}\ \dots\ K_{ir_i}) \cdots \\ &= \theta_1 \cdot \dots \cdot \theta_s = \theta \end{aligned}$$

por tanto, θ y σ son conjugados.

q.e.d.

Corolario.

Si $\sigma \in S_n$ y C es la clase de conjugación de σ, entonces:

$$\theta \in C \iff \theta \text{ tiene la misma estructura cíclica de } \sigma.$$

Dem:

Es inmediato de lo anterior.

q.e.d.

Si $\sigma \in S_n$, determinar $|C(\sigma)|$. $\sigma = \sigma_1 \cdot \dots \cdot \sigma_s$ con $1 \leq r_1 \leq \dots \leq r_s \leq n$.

Sol. $|C(\sigma)| = \dfrac{n!}{1^{\alpha_1} \cdot \alpha_1! \cdot 2^{\alpha_2} \cdot \alpha_2! \cdot \dots \cdot n^{\alpha_n} \cdot \alpha_n!}$ $\quad \alpha_i$ número de i-ciclos.

Obs: Los r-ciclos de S_n generan a S_n (con $r \in [\![1, n]\!]$). Más aún, S_n es generado por el conjunto de transposiciones.

Proposición.

Las transposiciones generan a S_n, i.e toda permutación es un producto de transposiciones.

Dem:

Sea $\sigma \in S_n$ y $\sigma = \sigma_1 \sigma_2 \dots \sigma_s$ con $1 \leq r_1 \leq r_2 \leq \dots \leq r_s$ su descomposición cíclica. Para probar que σ es descomposición de transposiciones, basta probar que σ_i con $r_i \geq 3$ es producto de transposiciones con $i \in [\![1, s]\!]$ (si $r_i = 1$, $\sigma_i = e$ y $r_i = 2 \Rightarrow \sigma_i$ es transposición).
En efecto, sea $i \in [\![1, s]\!]$ $\ni$ $r_i \geq 3$. Si

$$\sigma_i = (i_1 \; i_2 \; \dots \; i_{r_i})$$

tenemos que:

$$\sigma_i = (i_1 \; i_{r_i})(i_1 \; i_{r_i - 1}) \cdots (i_1 \; i_2)$$

(se verifica de manera inmediata). Luego σ_i es producto de transposiciones y, por ende, σ lo es.

q.e.d.

Corolario.

Las transposiciones de la forma $(1 \; i)$ con $2 \leq i \leq n$, generan a S_n.

Dem:

Como en la prop. anterior, basta probar ahora que toda transposición de la forma $(i \; j)$ con $i, j \in [\![1, n]\!]$ es producto de transposiciones de la forma $(1 \; t)$ con $t \geq 2$. En efecto:

$$(i\ j) = (1\ j)(1\ i)(1\ j)$$

Con $i \neq j$, $i, j \neq 1$. Claramente $i \mapsto j$, $j \mapsto i$ y $1 \mapsto 1$.

q.e.d.

Corolario.

El conjunto de transposiciones de la forma $(i\ i+1)$, con $i \in [\![1, n-1]\!]$, generan a S_n.

Dem:

Como en el caso anterior, basta probar que $\forall\, t \geq 2$, $(1\ t)$ es producto de transposiciones de la forma $(i\ i+1)$. En efecto, como:

$$(1\ 2) = (1\ 2)$$
$$(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$$
$$(1\ 4) = (3\ 4)(1\ 3)(3\ 4)$$
$$\vdots$$
$$(1\ n) = (n-1\ n)(1\ n-1)(n-1\ n)$$

q.e.d.

Def. Sea $\sigma \in S_n$. Se define el **signo de σ** como:

$$\operatorname{Sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^K$$

donde $K = \left|\{(i, j) \mid 1 \leq i < j \leq n \text{ y } \sigma(j) - \sigma(i) < 0\}\right|$.

EJEMPLO:

1) En S_6, tome $\sigma = (1\ 3)(2\ 6\ 5)$, entonces:

$$\operatorname{Sgn}(\sigma) = \frac{\sigma(2)-\sigma(1)}{1} \cdot \frac{\sigma(3)-\sigma(1)}{2} \cdot \frac{\sigma(4)-\sigma(1)}{3} \cdot \frac{\sigma(5)-\sigma(1)}{4} \cdot \frac{\sigma(6)-\sigma(1)}{5}$$
$$\cdot \frac{\sigma(3)-\sigma(2)}{1} \cdot \frac{\sigma(4)-\sigma(2)}{2} \cdot \frac{\sigma(5)-\sigma(2)}{3} \cdot \frac{\sigma(6)-\sigma(2)}{4}$$
$$\cdot \frac{\sigma(4)-\sigma(3)}{1} \cdot \frac{\sigma(5)-\sigma(3)}{2} \cdot \frac{\sigma(6)-\sigma(3)}{3}$$

$$\cdot \frac{\sigma(5)-\sigma(4)}{1} \cdot \frac{\sigma(6)-\sigma(4)}{2}$$
$$\cdot \frac{\sigma(6)-\sigma(5)}{1}$$
$$= 1\cdot(-1)\cdot 1\cdot(-1)\cdot 1\cdot(-1)\cdot(-1)(-1)(-1)\cdot 1\cdot 1\cdot 1\cdot$$
$$(-1)\cdot 1\cdot 1$$
$$=(-1)^7 = -1.$$

Obs:

1) $sgn(e)=1$, pues $K=0$.

2) Si $\sigma, \pi \in S_n$, entonces:
$$sgn(\sigma\pi) = sgn(\sigma)\, sgn(\pi)$$
En efecto, pues:
$$sgn(\sigma\pi) = \prod_{1\leq i<j\leq n} \frac{\sigma\pi(j)-\sigma\pi(i)}{j-i}$$
$$= \prod_{1\leq i<j\leq n} \frac{\sigma(\pi(j))-\sigma(\pi(i))}{\pi(j)-\pi(i)} \cdot \frac{\pi(j)-\pi(i)}{j-i}$$
$$= \left(\prod_{1\leq i<j\leq n} \frac{\sigma(\pi(j))-\sigma(\pi(i))}{\pi(j)-\pi(i)}\right)\cdot\left(\prod_{1\leq i<j\leq n} \frac{\pi(j)-\pi(i)}{j-i}\right)$$
$$= sgn(\sigma)\, sgn(\pi).$$

3) Si $\sigma, \pi \in S_n$ son conjugados, entonces: $sgn(\sigma) = sgn(\pi)$, pues
$$\sigma = \theta\pi\theta^{-1}, \text{ con } \theta \in S_n$$
$$\Rightarrow sgn(\sigma) = sgn(\theta)\, sgn(\pi)\, sgn(\theta^{-1})$$
Como $sgn(e)=1 \Rightarrow 1 = sgn(\theta\theta^{-1}) = sgn(\theta)\cdot sgn(\theta^{-1}) \Rightarrow sgn(\theta) = sgn(\theta^{-1})$.
$$\Rightarrow sgn(\sigma) = sgn(\pi)$$

4) $sgn(1\ 2) = (-1)^k$, donde $K=-1 \Rightarrow sgn(1\ 2) = -1$. Por tanto, toda transposición es de signo -1.

Def. Una permutación de S_n se dice que es par, si $sgn(\sigma)=1$; caso contrario, decimos que es impar.

Proposición

Considerando a $\{-1,1\} < \mathbb{Q}^*$, tenemos que: $\forall\, n \geq 2$, $sgn: S_n \to \{-1,1\}$ es un epimorfismo. Por lo cual $S_n/_{Ker(Sgn)} \cong \{-1,1\}$. En particular: $\left| S_n/_{Ker(Sgn)} \right| = 2$.

Dem:

Notemos que:

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \operatorname{Sgn}(\sigma) = 1\}$$
$$= \{\sigma \in S_n \mid \sigma \text{ es par}\} \trianglelefteq S_n$$

Def. Se define el grupo alternante A_n, de S_n, como:

$$A_n := \operatorname{Ker}(\operatorname{sgn}).$$

Notemos que $A_n \trianglelefteq S_n$, $\forall n \in \mathbb{N}$. Así que $S_n/A_n \cong \{-1, 1\}$ y $|S_n/A_n| = 2 \Rightarrow |A_n| = \frac{n!}{2}$.

Obs:

1) El producto de 2 permutaciones pares (resp. impares), es par.
2) El producto de una permutación par con una impar es impar.
3) Una permutación σ es par (resp. impar) si y sólo si σ se expresa como un número par (resp. impar) de transposiciones multiplicándose.
4) Un r-ciclo es par (resp. impar) si y sólo si r es impar (resp. par).

Proposición:

$$A_n = \langle \sigma^2 \mid \sigma \in S_n \rangle.$$

Dem:

Si $\sigma \in S_n \Rightarrow \sigma^2 \in A_n$. Por tanto $\langle \sigma^2 \mid \sigma \in S_n \rangle \subseteq A_n$. Para la recíproca basta probar que el producto de 2 tansposiciones pertenece a $\langle \sigma^2 \mid \sigma \in S_n \rangle$. Sean $\sigma, \theta \in S_n$ dos transposiciones:

(i) $\sigma\theta = (i\ j)(k\ l)$ m $|\{i, j, k, l\}| = 4$.

$$(i\ j)(k\ l) = (l\ i\ j)^2 (i\ k\ l)^2$$

(ii) $\sigma\theta = (i\ j)(j\ l)$ m $|\{i, j, l\}| = 3$.

$$(i\ j)(j\ l) = (i\ l\ j)^2$$

Por tanto, si $\sigma \in A_n$, entonces $\sigma = \sigma_1 \sigma_2 \dots \sigma_{2m}$, con $m \in \mathbb{N}$. Como es un número par, lo podemos agrupar de dos en dos, con σ_i transposición. Por lo anterior, σ es producto de cuadrados de elementos de S_n.

q.e.d.

Corolario.

A_n es generado por los 3-ciclos.

Dem:

Notemos que todo 3-ciclo es permutación par, elemento de A_n. Luego, la afirmación se sigue de la demostración de la proposición anterior.

q.e.d.

Corolario.

A_n es generado por los 3-ciclos de la forma $(a\ b\ x)$, donde a, b son fijos distintos y $x \in [\![1, n]\!] \setminus \{a, b\}$.

Dem:

Por el corolario anterior, basta expresar cada 3-ciclo de la forma $(i\ j\ k)$ como un producto de ciclos de la forma $(a\ b\ x)$.

a) $a, b \in \{i, j, k\}$, entonces:

$$(i\ j\ k) \begin{cases} (a\ b\ l) = (a\ b\ l) \\ (a\ l\ b) = (a\ b\ l)^2 \\ (l\ a\ b) = (a\ b\ l) \\ (b\ a\ l) = (a\ b\ l)^2 \\ (b\ l\ a) = (a\ b\ l) \\ (l\ b\ a) = (a\ b\ l)^2 \end{cases}$$

, donde $l \in \{i, j, k\} \setminus \{a, b\}$.

(b) $a \in \{i, j, k\}$ y $b \notin \{i, j, k\}$. Entonces:

Mismo para

$$(i\ j\ k) = (a\ i\ j)$$
$$= (a\ b\ j)^2 (a\ b\ i)(a\ b\ j)$$

(c) $a \notin \{i, j, k\}$ y $b \in \{i, j, k\}$:

$$(i\ j\ k) = (b\ i\ j)$$
$$= (a\ b\ j)(a\ b\ i)^2 (a\ b\ j)^2$$

(d) $a, b \notin \{i, j, k\}$:

$$(i\ j\ k) = (a\ b\ i)(a\ b\ k)(a\ b\ j)^2 (a\ b\ k^2)(a\ b\ i)$$

q.e.d.

Proposición.

Si $H < S_n$, entonces $H \leq A_n$ ó $[H : H \cap A_n] = 2$.

Dem:

Supongamos que $H \not\leq A_n$. Tenemos que $sgn : S_n \to \{-1, 1\}$ es epimorfismo, así $f = sgn|_H : H \to \{-1, 1\}$ sigue siendo epimorfismo, donde $Ker(f) = \{\sigma \in H \mid \sigma \in A_n\} = H \cap A_n$. Por el P.T.I: $H/H \cap A_n \cong \{-1, 1\}$. Luego: $[H : H \cap A_n] = 2$.

q.e.d.

Proposición.

Sean $n \geq 3$, $N \triangleleft S_n$ tal que $N \neq S_n$. Si N contiene un 3-ciclo, entonces $N = A_n$.

Dem:

Sea $(a\ b\ c) \in N$ un 3-ciclo. Afirmamos que todo 3-ciclo $(i\ j\ k) \in N$. En efecto, existe $\theta \in S_n$ m $(i\ j\ k) = \theta (a\ b\ c) \theta^{-1} \in N$. Luego $A_n = \langle (i\ j\ k) \mid (i\ j\ k)$ es 3-ciclo$\rangle \leq N \neq S_n$. Luego:

$$\Rightarrow 2 = [S_n : A_n] = \underbrace{[S_n : N]}_{\neq 1} [N : A_n]$$

$$\Rightarrow [N : A_n] = 1$$

$$\Rightarrow N = A_n .$$

q.e.d.