

Real Bermúdez Jesús M.

June 15, 2003

1.

2.

3.

4. Permutaciones

4.1. El grupo simético

Recordemos que el grupo simético de grado $n \in \mathbb{N}$ es el grupo

$$S_n = \{\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} | \sigma \text{ es biyección}\}$$

con la composición.

Si $\sigma \in S_1$, lo expresamos como:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

y;

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

También sabemos que $|S_n| = n!$.

Sea $\sigma \in S_n \Rightarrow \sigma$ es de orden finito con $|\sigma||S_n| = n!$. Si $|\sigma| = k$ entonces $\langle \sigma \rangle = \{e, \sigma, \sigma^2, \dots, \sigma^{k-1}\}$.

Ejemplo. Sea $\alpha, \in S_3$, donde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

y;

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

y;

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \alpha(\beta(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(2) & \alpha(3) & \alpha(1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Veamos que $\alpha\beta \neq \beta\alpha$ ya que:

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Definición 4.1

Sea $x \in X$ y sea $\sigma \in S_X$. Decimos que σ fija a x si $\sigma(x) = x$ y decimos que σ mueve a x si $\sigma(x) \neq x$.

Definición 4.2

Supongamos que $\sigma \in S_n$ es tal que $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$.

Y supongamos además que σ fija a los restantes $n - r$ enteros en $\{1, \dots, n\}$. Entonces σ se llama un r -ciclo ó ciclo de longitud r . Denotemos a σ por: $\sigma = (i_1 i_2 \dots i_r)$.

Nota

El único 1 - ciclo en S_n es la función identidad.

Definición 4.3

Un 2 - ciclo en S_n se le llama *transposición*.

Ejemplos

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (1 \ 5 \ 3 \ 4 \ 2) \in S_5$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (1 \ 4 \ 5)(2 \ 3)$$

Observaciones

Si $\sigma \in S_n$ es un r -ciclo, entonces $|\sigma| = r$.

Definición 4.4

Dos permutaciones $\alpha, \beta \in S_n$ se dicen disjuntas o ajenas si cada x que es movido por una, es fijado por la otra. Es decir, si $\alpha(x) \neq x$, entonces $\beta(x) = x$ y si $\beta(y) \neq y$, entonces $\alpha(y) = y$. Puede ocurrir que $\alpha(z) = z = \beta(z)$ para algún z .

Una familia de permutaciones $\alpha_1, \dots, \alpha_m$ se dice disjunta, si cada una de ellas son disjuntas.

Por ejemplo, las permutaciones:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} = (1 \ 5 \ 3)$$

y

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2 \ 4)$$

son disjuntas.

Proposición 4.5

1. Si $\alpha, \beta \in S_n$ son disjuntas, entonces $\alpha\beta = \beta\alpha$.
2. Si $\alpha, \beta \in S_n$ son disjuntas y $\alpha\beta = e$, entonces $\alpha = \beta = e$.

Demostración

1) Sea $x \in [1, \dots, n]$

1. Si $\alpha(x) \neq x = \beta(x)$, entonces: $(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$ $(\beta\alpha)(x) = \beta(\alpha(x)) = \beta(x) = x$ Por lo tanto $(\alpha\beta)(x) = (\beta\alpha)(x)$.

2. Supongamos que $\alpha(x) \neq x \Rightarrow \beta(x) = x$. Sea $y \in \alpha(x)$, no tenemos que esto implica que $\alpha(y) \neq y$ (pues α es una función inyectiva).

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = y$$

$$(\beta\alpha)(x) = \beta(\alpha(x)) = \beta(y) = y$$

$$\text{Por lo tanto } (\alpha\beta)(x) = (\beta\alpha)(x)$$

3. Similarmente se demuestra el caso en que $\beta(x) \neq x$.

2) Supongamos que $\alpha \neq e$ entonces existe $x \in \{1, \dots, n\}$ tal que $\alpha(x) \neq x \Rightarrow \beta(x) = x$ sea $y = \alpha(x) \neq x$.

Luego $x = e(x) = (\alpha\beta)x = \alpha(\beta)x = \alpha(\beta(x)) = \alpha(x) = y$. Lo cual es una contradicción.

q.e.d.

Teorema 4.6

Toda permutación de S_n es un ciclo ó es producto de ciclos disjuntos.

Demostración

Sea $\alpha \in S_n$ y sea k el número de puntos movidos por α .

Procedamos por inducción sobre k . Si $k = 1$, entonces α mueve solamente a 1 punto, pero esto sólo es posible si $\alpha = e$ y sabemos que e es un 1-ciclo.

Supongamos ahora que el resultado se cumple para toda permutación que mueve $k - 1$ o menos elementos, con $k > 1$. Puesto que $\alpha \neq e$, sea $i_1 \in \{1, \dots, n\}$ un elemento movido por α .

Definamos $i_2 = \alpha(i_1) \neq i_1$, $i_3 = \alpha(i_2) = \alpha^2(i_1), \dots, i_{r+1} = \alpha(i_r)$, donde r es el menor natural tal que $i_{r+1} \in \{i_1, i_2, \dots, i_r\}$.

Afirmemos que $i_{r+1} = i_1$, pues si $i_{r+1} = i_j$, con $j \in \{2, \dots, r\}$, entonces.

$\alpha(i_{j-1}) = i_j = i_{r+1} = \alpha(i_r) \Rightarrow i_{j-1} = i_r \Rightarrow j-1 = r \Rightarrow j = r+1$. Lo cual es una contradicción.

Por lo tanto $i_{r+1} = i_1 = \alpha(i_r)$.

Consideremos el ciclo $\sigma = (i_1, i_2, \dots, i_r)$ si se tuviese que $r = k$, terminamos, pues se tendría $\sigma = \alpha$ y α sería un k -ciclo. Supongamos que $r < k$. Sea $\{i_1, i_2, \dots, i_r, j_1, j_2, \dots, j_{k-r}\} = A$ el conjunto de puntos que mueve α .

Sea $Y = \{j_1, j_2, \dots, j_{k-r}\}$. Definamos $\alpha' \in S_n$ tal que $\alpha'|_Y = \alpha|_Y$ y α' fija a todo elemento en $\{1, \dots, n\} \setminus Y$.

Notemos que $\alpha = \alpha'\sigma$ y α' y σ son disjuntas.

Puesto que α' mueve $k-r < k$ puntos, por hipótesis de inducción, α' es un ciclo o producto de ciclos disjuntos, digamos $\alpha' = \tau_1\tau_2\dots\tau_s$.

Por lo tanto $\alpha = \tau_1\tau_2\dots\tau_s\sigma$

q.e.d.

Teorema 4.7

La factorización de cualquier permutación $\sigma \in S_n \setminus \{e\}$ como producto de ciclos disjuntos de longitud mayor o igual a 2, es única salvo orden.

Demostración

Sea $\sigma \in S_n$ y supóngase que $\sigma = \beta_1 \cdots \beta_t$ y $\sigma = \psi_1 \cdots \psi_s$, con β_i, ψ_j son ciclos de longitud mayor o igual a 2.

Sea $i_1 \in [1, n]$ tal que $\beta_1(i_1) \neq i_1 \Rightarrow$ existe $\psi_j(i_1) \neq i_1$.

Puesto que los ciclos ψ_1, \dots, ψ_s son disjuntos, entonces conmutan podemos suponer entonces que el ψ_j anterior es ψ_1 .

Lo anterior implica que $\sigma(i_1) = \beta_1(i_1) = \psi_1(i_1) \Rightarrow \sigma^m(i_1) = \beta_1^m(i_1) = \psi_1^m(i_1) \Rightarrow \beta_1$ y ψ_1 son ciclos de la misma longitud, pues son los únicos que mueven al i_1 .

Por otro lado se tiene que $\psi_1^r(i_1) = i_{1+r}$ y $\beta_1^{i_1} = i_{1+r} = \beta_1(i_r) = \psi_1(i_r) \Rightarrow \psi_1 = \beta_1$ en $\{i_1, i_2, \dots, i_m\}$ y como ψ_1 y β_1 dejan fijos a todos los elementos de $\{1, \dots, n\} \setminus \{i_1, \dots, i_m\}$, concluimos que $\psi_1 = \beta_1$.

De $\sigma = \beta_1 \cdots \beta_t = \psi_1 \cdots \psi_s \Rightarrow \beta_2 \cdots \beta_t = \psi_2 \cdots \psi_s$.

Continuando con el mismo razonamiento, vamos cancelando los ciclos iguales y si $s > t$, entonces: $e = \psi_{t+1} \cdots \psi_s \Rightarrow \psi_{t+1} = \dots = \psi_s = e$. Lo que es una contradicción.

Por lo tanto $s = t$.

q.e.d.

Corolario 1

el orden de $\sigma \in S_n$ es igual al mínimo común múltiplo de los órdenes de sus ciclos.

Corolario 2

Toda permutación $\sigma \in S_n$ puede representarse (no de manera única) como producto de transposiciones.

Demostración

Es suficiente probar que todo ciclo es producto de transposiciones.

$$(i_1 \ i_2 \ \dots \ i_r) = (i_1 \ i_r) \dots (i_1 \ i_4) (i_1 \ i_3) (i_1 \ i_2)$$

q.e.d.

Ejemplos

$$\begin{aligned} (15 \ 32) &= (1 \ 2)(1 \ 3)(1 \ 5) \\ &= (2 \ 3)(2 \ 5)(2 \ 1) \\ &= (1 \ 2)(2 \ 3)(1 \ 2)(3 \ 1)(3 \ 5)(2 \ 3)(1 \ 2) \end{aligned}$$

Definición 4.8

Sea $\theta \in S_n$, θ se dice *par* (respectivamente *impar*) si θ se escribe como producto de una cantidad par (impar) de transposiciones.

Definición 4.9

El *signo* de una permutación se define como sigue:

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

Sea $\varphi : S_n \rightarrow \{1, -1\} = C_2$ dada por:

$$\varphi(\theta) = \begin{cases} +1 & \text{si } \theta \text{ es par} \\ -1 & \text{si } \theta \text{ es impar} \end{cases}$$

φ es epimorfismo. Pues $\varphi(e) = 1$ y $\varphi((12)) = -1$, por lo que φ es suprayectiva.

φ es homomorfismo. Considerando diferentes casos. (σ y θ par ó σ par, θ impar ó σ y θ impares), se demuestra que en efecto, φ es un homomorfismo.

$$\begin{aligned} N_\varphi &= \{\sigma \in S_n \mid \varphi(\sigma) = 1\} \\ &= \{\sigma \in S_n \mid \sigma \text{ es par}\} \triangleleft S_n \end{aligned}$$

Además $S_n/N_\varphi \cong C_2 \Rightarrow |S_n|/|N_\varphi| = 2$, entonces $|N_\varphi| = \frac{1}{2}|S_n|$. Esto nos dice que la mitad de los elementos de S_n son permutaciones pares.

Al subgrupo normal N_φ se llama *el grupo alternante* y se denota por A_n .

Definición 4.10

EL *grupo alternante* de grado n , denotado por A_n , es el grupo de S_n que consiste de todas las permutaciones pares.

Proposición 4.11

Sea $n \geq 3$. Entonces A_n está generado por los 3 – *ciclos*.

Demostración

Basta demostrar que el producto de dos transposiciones es producto de 3 – *ciclos*.

$$(a \ b) (c \ d) = (b \ c \ a) (c \ d \ b)$$

q.e.d.

Teorema 4.12

Sea $n > 2$. Entonces A_n es el único subgrupo de S_n de índice 2.

Demostración

Sea $H \geq S_n$ tal que $[S_n : H] = 2 \Rightarrow |H| = |A_n|$. Basta demostrar que $A_n \subset H$ y con esto haremos que todos los 3 – *ciclos* estén contenidos en H .

Notemos que $\forall \sigma \in S_n$, se tiene que $\sigma^2 \in H$.

Sea τ un 3 – *ciclo*, entonces $|\tau| = 3 \Rightarrow \tau^4 = \tau$ ya que $\tau^4 = (\tau^2)^2 \in H$ y $(\tau^2)^2 = \tau \in H$.

q.e.d.

Observaciones

1. El signo de una transposición es -1.
2. El signo de un r – *ciclo* es $(-1)^{r-1}$

$$(i_1 \ i_2 \ \dots \ i_r) = \frac{(i_1 \ i_r) \dots (i_1 \ i_3) (i_1 \ i_2)}{r-1}$$

$$3. \quad (1 \ 2 \ 3 \ \dots \ m)^{-1} = (m \ m-1 \ \dots \ 3 \ 2 \ 1)$$

Definición 4.13

Se dice que los elementos de $\alpha, \beta \in S_n$ tienen la misma estructura en ciclos, si para cada $r \leq n$, el número de r -ciclos en α es igual al número de r -ciclos en β .

Definición 4.14

Si G es un grupo, la relación “ x es un conjugado de y en G ” es una relación de equivalencia en G ; las clases de equivalencia son llamadas *clases conjugadas*.

Como un ejemplo, Si G es el grupo multiplicativo de todas las matrices no singulares de $n \times n$ sobre un campo, entonces 2 matrices quedan en la misma clase de conjugación si y sólo si ellas son similares.

Ahora, x e y son de la misma clase de conjugación si existe un elemento $a \in G$ con $y = axa^{-1} = x^a$. Existe entonces un isomorfismo $\gamma : G \rightarrow G$ (llamada, conjugación por a) con $y = \gamma(x)$. Se sigue que todos los elementos en la misma clase de conjugación tienen el mismo orden. Una consecuencia interesante es que, para cualesquiera dos elementos $a, b \in G$, ab y ba tienen el mismo orden.

Un elemento $x \in G$ es el solo residente de su clase de conjugación si $x = axa^{-1} \ \forall a \in G$, es decir, x conmuta con todo elemento en G . En un grupo Abelian, por lo tanto, las clases de conjugación no son de mucho interés.

Definición 4.14

El *centro* de G , denotado por $Z(G)$, es el conjunto de todas las $x \in G$ que conmutan con todo elemento de G .

Teorema 4.15

Sean $\alpha, \beta \in S_n$, entonces α, β son conjugados si y sólo si tienen la misma estructura en ciclos.

Demostración

\Rightarrow) Supongamos que α es un r -ciclo, digamos $\alpha = (\alpha_1 \ \alpha_2 \ \alpha_3 \ \dots \ \alpha_r) \in S_n$ y sea $\tau \in S_n$.
Escribamos $\tau(\alpha_i) = b_i$ con $i = 1, \dots, r$ $b_i \neq b_j$.
Notemos que $b_i \neq b_j$ si $i \neq j$, y escribamos $b_1 = b_{r+1}$.

$$\begin{aligned} \tau\alpha\tau^{-1}(b_i) &= \tau\alpha(\alpha_i) \\ &= \tau(\alpha_{i+1}) \\ &= b_{i+1} \end{aligned}$$

Se demuestra que $\tau\alpha\tau^{-1}$ deja fijo a todo elemento de $\{1, 2, \dots, n\} \setminus \{b_1, \dots, b_r\}$. Luego

$$\begin{aligned} \tau\alpha\tau^{-1} &= (b_1 \ b_2 \ b_3 \ \dots \ b_r) \\ &= (\tau(\alpha_1) \ \tau(\alpha_2) \ \dots \ \tau(\alpha_r)) \end{aligned} \tag{1}$$

Pasemos al caso más general; es decir, supongamos que $\alpha \in S_n$ es una permutación en ciclos disjuntos es: $\alpha = \alpha_1\alpha_2\dots\alpha_t$.
Dado $\tau \in S_n$

$$\tau\alpha\tau^{-1} = \tau\alpha_1\tau^{-1}\tau\alpha_2\tau^{-1}\tau\dots\tau^{-1}\tau\alpha_t\tau^{-1}$$

Por lo anterior $c \setminus \tau\alpha_i\tau^{-1}$ es un ciclo de la misma longitud que α_i .

Por lo tanto $\tau\alpha\tau^{-1}$ tiene la misma estructura en ciclos que α .

\Leftarrow) Recíprocamente, sean $\sigma, \rho \in S_n$ con la misma estructura en ciclos, digamos

$$\sigma = (a_1 \ a_2 \ \dots \ a_{i_1}) (b_1 \ b_2 \ \dots \ b_{i_2}) \dots (n_1 \ n_2 \ \dots \ n_{i_n})$$

y

$$\rho = (z_1 \ z_2 \ \dots \ z_{i_1}) (y_1 \ y_2 \ \dots \ y_{i_2}) \dots (n'_1 \ n'_2 \ \dots \ n'_{i_n})$$

En donde los ciclos aparecen en orden creciente en cada una de las permutaciones e incluimos los ciclos de orden 1.
Definiendo $\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ como:

$$\tau(a_j) = z_j$$

$$\begin{aligned}\tau(b_j) &= y_j \\ &\vdots \\ \tau(n_j) &= n'_j\end{aligned}$$

Se verifica que $\tau\sigma\tau^{-1} = \rho$ ya que:

$$\tau\sigma\tau^{-1}(z_j) = \tau\sigma(a_j) = \tau(a_{j+1}) = z_{j+1} = \rho(z_j).$$

Por lo tanto si σ y ρ tienen la misma estructura cíclica entonces σ y ρ son conjugados.

q.e.d.

Proposición 4.16

Sea $1 \leq k < n$. Entonces el número de k -ciclos en S_n es: $\frac{1}{k}n(n-1) \cdot \dots \cdot (n-k+1)$

Demostración

Tomemos un subconjunto $A \subset \{1, 2, \dots, n\}$ con k elementos.

Dado i_1 , hay $k-1$ formas de enviar i_1 a otro valor. Una vez fijo i_2 tal que $i_1 \rightarrow i_2$, hay $k-2$ formas posibles de elegir i_3 tal que $i_2 \rightarrow i_3$ continuando de esta forma, vemos que dado el conjunto A , se pueden construir $(k-1)!$ diferentes k -ciclos.

Además se tienen $\binom{n}{k}$ subconjuntos de $\{1, \dots, n\}$ con k elementos.

Así, el número de k -ciclos es:

$$\binom{n}{k} (k-1)! = \frac{n!}{k!(n-k)!} (k-1)! = \frac{1}{k} n(n-1) \cdot \dots \cdot (n-k+1)$$

q.e.d.

Ejemplo

El número de 3-ciclos en S_4 es: $\frac{1}{3}(3)(2) = 8$.

Con lo anterior mostremos que el recíproco del teorema de Lagrange no es cierto, es decir, existen grupos finitos y $k \in \mathbb{N}$ tales que $k \mid |G|$ pero G no contiene subgrupos de orden k .

Teorema 4.17

A_4 no contiene subgrupos de orden 6.

Demostración

Supongamos que existe $H < A_4$ tal que $|H| = 6 \Rightarrow [A_4 : H] = 2$.

Luego $\forall \sigma \in A_4, \sigma^2 \in H$. Si $\sigma \in A_4$ es un 3-ciclo, entonces $\sigma^3 = 1 \Rightarrow \sigma = \sigma^4 = (\sigma^2)^2 \in H$.

Es decir, H contiene a todos los 3-ciclos, lo cual es una contradicción, pues en A_4 hay 8 3-ciclos.

q.e.d.

Proposición 4.18

1. Si $n \geq 3$, entonces $Z(S_n) = \{e\}$. En particular $S_n \cong \text{Int}(S_n)$.
2. Si $n \geq 4$, entonces $Z(A_n) = \{e\}$ y por tanto $A_n \cong \text{Int}(A_n)$.
3. Si $n \geq 3$, $N \triangleleft A_n$ y N contiene un 3-ciclo entonces $N = A_n$.

Demostración

1) Sea $\sigma \in S_n$ y sea $\sigma = \sigma_1\sigma_2 \dots \sigma_r$ su descomposición como producto de ciclos disjuntos. Supongamos que escribimos los ciclos $\sigma_1, \dots, \sigma_r$ en orden decreciente.

Supongamos que $\sigma_1 = (i_1 \ i_2 \ \dots \ i_m), m \geq 3$.

Entonces $\sigma (i_1 \ i_2) (i_1) = (i_1 \ i_2 \ \dots \ i_m)$
 $\sigma_{i_2 \dots i_r} (i_1 \ i_2) (i_1) = i_3$ y $(i_1 \ i_2) \sigma(i_1) = i_1$
 Por lo tanto $\sigma \notin Z(S_n)$.

Si $\sigma_1, \dots, \sigma_r$ son transposiciones disjuntas supongamos que $\sigma_1 = (i_1 \ i_2)$ y tomemos $i_3 \notin \{i_1, i_2\}$.
 Entonces $(i_1 \ i_2) \sigma_2 \sigma_3 \dots \sigma_r (i_1 \ i_3) (i_3) = \sigma (i_1 \ i_3) = i_2$

$$\begin{aligned} (i_1 \ i_3) \sigma(i_3) &= (i_1 \ i_3) (i_1 \ i_2) \sigma_2 \dots \sigma_r (i_3) \\ &= \begin{cases} \sigma \neq i_2 & \sigma \neq i_3 & \sigma \neq i_1 \\ i_1 \end{cases} \end{aligned}$$

2) Es análoga a la anterior.

3) Sea $\sigma \in N$ el 3 - ciclo que se menciona. Por ser $N \triangleleft A_n \ \forall \tau \in A_n, \tau \sigma \tau^{-1} \in N$ y los conjugados de σ son 3 - ciclos. Luego N contiene a todos los 3 - ciclos. Por lo tanto $N = A_n$.

q.e.d.

Veremos que A_n es simple cuando $n \geq 5$. Ya que el 4-grupo V contiene todas las permutaciones en S_4 de una estructura cíclica dada, V es un subgrupo normal de S_4 , por tanto, A_4 no es simple. Examinemos S_5 y A_5 .

Estructura Cíclica	S_5 Número	Orden	Paridad
(1)	1	1	Par
(12)	$10 = (5 \times 4)/2$	2	Impar
(123)	$20 = (5 \times 4 \times 3)/3$	3	Par
(1234)	$30 = (5 \times 4 \times 3 \times 2)/4$	4	Impar
(12345)	$24 = 5!/5$	5	Par
(12)(34)	$15 = \frac{1}{2} \left(\frac{5 \times 4}{2} \times \frac{3 \times 2}{2} \right)$	2	Par
(123)(45)	$20 = \frac{5 \times 4 \times 3}{3} \times \frac{2 \times 1}{2}$	6	Impar
	$120 = 5!$		

Estructura Cíclica	A_5 Número	Orden	Paridad
(1)	1	1	Par
(123)	20	3	Par
(12345)	24	5	Par
(12)(34)	15	2	Par
	60		

Teorema 4.19

Si $n \geq 5$, A_n es simple.

Demostración

Sea $H \triangleleft A_n, H \neq \{e\}$. Sea $\alpha \in H \setminus \{e\}$ y sea $\alpha = \alpha_1 \alpha_2 \dots \alpha_k$ su descomposición como ciclos disjuntos. Supongamos además que los ciclos $\alpha_1, \dots, \alpha_k$ están escritos en orden decreciente.

Sea $\alpha_1 = (a_1 \ a_2 \ \dots \ a_m)$.

1. Supongamos que $m > 3$ y sea $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}$. Notemos que $\alpha_2, \dots, \alpha_k$ permutan con σ . Entonces:

$$\begin{aligned}\sigma\alpha\sigma^{-1} &= \sigma\alpha_1\alpha_2\dots\alpha_k\sigma^{-1} \\ &= \sigma\alpha\sigma^{-1}\alpha_2\dots\alpha_k\sigma^{-1} \\ &= \sigma\begin{pmatrix} a_1 & a_2\dots a_m \end{pmatrix}\sigma^{-1}\alpha_2\alpha_3\dots\alpha_k \\ &= (\sigma(a_1) \ \sigma(a_2)\dots\sigma(a_m))\alpha_2\dots\alpha_k \\ &= \begin{pmatrix} a_2 & a_3 & a_1 & a_4 & a_5\dots a_m \end{pmatrix}\alpha_2\dots\alpha_k \in H\end{aligned}\tag{1}$$

$$\begin{aligned}\alpha^{-1}\sigma\alpha\sigma^{-1} &= \alpha_k^{-1}\dots\alpha_3^{-1}\alpha_2^{-1}\begin{pmatrix} a_m & a_{m-1}\dots a_1 \end{pmatrix}\begin{pmatrix} a_2 & a_3 & a_1 & a_4 & a_5\dots a_m \end{pmatrix}\alpha_2\dots\alpha_k \\ &= \begin{pmatrix} a_1 & a_3 & a_m \end{pmatrix} \in H.\end{aligned}\tag{1}$$

Por 3) de la proposición anterior, se concluye que $H = A_n$.

2. Supongamos que $m = 3$

a) Supongamos que también es un 3 - ciclo. Entonces $\alpha_1 = \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}$ y $\alpha_2 = \begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix}$. Tomemos $\sigma = \begin{pmatrix} a_2 & a_3 b_1 \end{pmatrix}$.

Notemos que σ conmuta con $\alpha_3\dots\alpha_k$,

$$\begin{aligned}\sigma\alpha\sigma^{-1} &= \sigma\alpha_1\sigma^{-1}\sigma\alpha_2\sigma^{-1}\sigma\alpha_3\dots\alpha_k\sigma^{-1} \\ &= (\sigma(a_1)\sigma(a_2)\sigma(a_3))(\sigma(b_1)\sigma(b_2)\sigma(b_3))\alpha_3\dots\alpha_k \\ &= \begin{pmatrix} a_1 & a_3 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 & b_3 \end{pmatrix}\alpha_3\dots\alpha_k \in H\end{aligned}\tag{1}$$

$$\begin{aligned}\Rightarrow \alpha^{-1}\sigma\alpha\sigma^{-1} &= \alpha_k^{-1}\dots\alpha_3^{-1}\begin{pmatrix} b_3 & b_2 & b_1 \end{pmatrix}\begin{pmatrix} a_3 & a_2 & a_1 \end{pmatrix}\begin{pmatrix} a_1 & a_3 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 & b_3 \end{pmatrix}\alpha_3\dots\alpha_k \\ &= \begin{pmatrix} b_3 & b_2 & b_1 \end{pmatrix}\begin{pmatrix} a_3 & a_2 & a_1 \end{pmatrix}\begin{pmatrix} a_1 & a_3 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 & b_3 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 & b_1 & a_3 & b_3 \end{pmatrix} \in H\end{aligned}\tag{1}$$

Por el caso anterior $H = A_n$

b) Supongamos que $\alpha_2, \dots, \alpha_k$ son transposiciones.

Sea $\alpha_1 = \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}$

$$\begin{aligned}\alpha &= \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}\alpha_2\alpha_3\dots\alpha_k \in H \\ \alpha^2 &= \begin{pmatrix} a_1 & a_3 & a_2 \end{pmatrix} \in H\end{aligned}$$

Por lo tanto $H = A_n$.

3. Finalmente supongamos que $\alpha_1\dots\alpha_k$ son transposiciones disjuntas.

Supongamos que $\alpha_1 = \begin{pmatrix} a_1 & a_2 \end{pmatrix}$ y $\alpha_2 = \begin{pmatrix} b_1 & b_2 \end{pmatrix}$.

Sea $\sigma = \begin{pmatrix} a_2 & b_1 & b_2 \end{pmatrix}$ entonces:

$$\begin{aligned}\sigma\alpha\sigma^{-1} &= \sigma\alpha_1\sigma^{-1}\sigma\alpha_2\sigma^{-1}\sigma\alpha_3\dots\alpha_k\sigma^{-1} \\ &= (\sigma(a_1)\sigma(a_2))(\sigma(b_1)\sigma(b_2))\alpha_3\dots\alpha_k \\ &= \begin{pmatrix} a_1 & b_1 \end{pmatrix}\begin{pmatrix} b_2 & a_2 \end{pmatrix}\alpha_3\dots\alpha_k \in H.\end{aligned}\tag{1}$$

$$\begin{aligned}\alpha^{-1}\sigma\alpha\sigma^{-1} &= \alpha_k^{-1}\dots\alpha_3^{-1}\begin{pmatrix} b_1 & b_2 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} a & b_1 \end{pmatrix}\begin{pmatrix} b_2 & a_2 \end{pmatrix}\alpha_3\dots\alpha_k \\ &= \begin{pmatrix} b_1 & b_2 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \end{pmatrix}\begin{pmatrix} b_2 & a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & b_2 \end{pmatrix}\begin{pmatrix} a_2 & b_1 \end{pmatrix} = \beta \in H.\end{aligned}\tag{1}$$

Sea $b \notin \{1, a_2, b_1, b_2\}$ ($n \geq 5$).

Sea $\gamma = \begin{pmatrix} a_1 & b_2 & b \end{pmatrix}$ entonces:

$$\begin{aligned}\gamma\beta\gamma^{-1} &= (\gamma(a_1)\gamma(b_2))(\gamma(a_2)\gamma(b_1)) \\ &= \begin{pmatrix} b_2 & b \end{pmatrix}\begin{pmatrix} a_2 & b_1 \end{pmatrix} \in H.\end{aligned}\tag{1}$$

$$\begin{aligned}\beta^{-1}\gamma\beta\gamma^{-1} &= \begin{pmatrix} a_1 & b_2 \end{pmatrix}\begin{pmatrix} a_2 & b_1 \end{pmatrix}\begin{pmatrix} b_2 & b \end{pmatrix}\begin{pmatrix} a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & b_2 & b \end{pmatrix} \in H \Rightarrow H = A_n\end{aligned}\tag{1}$$

q.e.d.

Teorema 4.20 (Cayley, 1878)

Todo grupo G es isomorfo a un subgrupo de S_G . En particular, todo grupo finito de orden n es isomorfo a un subgrupo de S_n .

Demostración

Para cada $a \in G$, definimos $L_a : G \rightarrow G$ por $L_a(x) = ax$ (L_a es la translación por la izquierda de a). Vemos que L_a tiene una correspondencia 1-1, así que $L_a \in S_G$. La función λ manda a a en L_a ésta es una función de G a S_G .

Pedimos que λ sea uno-uno y un homomorfismo. Si $a \neq b$ son elementos de G , entonces $L_a(1) = a \neq b = L_b(1)$, así que $L_a \neq L_b$ y $\lambda(a) \neq \lambda(b)$, por tanto, λ es uno-uno. Finalmente consideremos $\lambda(ab)L_{ab}$ y $\lambda(a)\lambda(b) = L_aL_b$. Mostremos que éstas permutaciones son las mismas, debemos mostrar que ellas asignan los mismos valores a cada $x \in G$. Pero $L_{ab} = (ab)x$, y $L_aL_b(x) = L_a(bx) = a(bx)$ y esto es lo mismo por asociatividad.

q.e.d.