Capítulo

5

Permutaciones

5.1 Introducción

Las permutaciones son el ejemplo de grupo finito que más se utiliza dentro de la teoría de grupos. Su importancia se debe a que todo grupo es isomorfo a un grupo de permutaciones, por un lado, y por otro, el grupo de las permutaciones de las raíces de un polinomio, permite determinar la solubilidad de una ecuación algebráica asociada a él, resultado este que se conoce con el nombre de Teoría de Galois.

El problema de la resolución de ecuaciones algebráicas de grado superior a 4, fue atacado por el matemático Noruego Niels Henrik Abel (1802-1829) quien en 1824 publicó una memoria titulada " *Sobre la Resolución de Ecuaciones Algebráicas*", en donde se da la primera prueba de la imposibilidad de resolver en general la ecuación de grado 5, usando radicales.

Dicho en otras palabras, Abel probó que no existe una fórmula general para resolver ecuaciones de grado mayor que 4.

Anteriormente Carl F. Gauss había resuelto un famoso problema, planteado desde la época de los griegos sobre la posibilidad de construir con regla y compás un polígono regular. Este problema se reduce a resolver la ecuación

$$ax^n + b = 0$$

con a y b enteros, usando raíces.

El matemático francés Evarist Galois (1810-1832) inspirandose en ambos trabajos, se planteó el problema aún más general:

Dar un criterio para solubilidad de la ecuación

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{5.1}$$

por medio de radicales.

Galois obtuvo un método muy interesante, que ha sido uno de los aportes más grandes a la matemáqtica, y en donde el grupo de permutaciones de las raíces del polinomio en (**??**) nos da toda la información necesaria. Este resultado dice "*La ecuación (**??**) es soluble si y sólo si el grupo de permutaciones de las raíces es soluble*".

Al final de este capítulo se da una demostración completa de la simplicidad de los grupos alternantes A_n para $n \geq 5$, lo cual prueba que estos grupos no son solubles y este resultado es así, equivalente a probar que la ecuación (**??**) no se puede resolver por radicales.

5.2 Teorema de Cayley

En 1854 el matemático inglés Arthur Cayley (1824-1895) escribió un artículo titulado "*Notas sobre la teoría de permutaciones*", donde se demuestra uno de los teoremas más importantes de toda la teoría de grupos.

Dicho teorema establece que todo grupo finito es isomorfo a algún grupo de permutaciones. Esto demuestra el poder unificador de la teoría de grupos, al poder condensar en un sólo grupo abstracto, todos los grupos provenientes de las distintas áreas de matemática.

Teorema 5.2.1 *(Cayley) Sea G un grupo finito. Entonces G es isomorfo a un grupo de H, donde H, es un subgrupo de S_n, para algún n.*

Demostración: Consideremos a G como un conjunto solamente y sea $A(G)$ el grupo de aplicaciones biyectivas de G en si mismo. Para cada $g \in G$ se tiene una aplicación

$$\begin{array}{rccc} \phi_g & : & G & \longrightarrow & G \\ & & x & \longrightarrow & xg \end{array}$$

ϕ_g se llama una **traslación a la derecha inducida por** g. Es fácil verificar entonces que ϕ_g define una biyección y por lo tanto $\phi_g \in A(G)$ para todo g en G.

Luego tenemos una función

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & A(G) \\ & & g & \longrightarrow & \phi_g \end{array}$$

Afirmamos que ϕ es un homomorfismo de grupos. En efecto, sean g_1, g_2 en G. Luego

$$\begin{aligned} \phi(g_1 g_2)(x) &= (g_1 g_2)x \\ &= g_1(g_2 x) \\ &= g_1 \phi_{g_2}(x) \\ &= \phi_{g_1}(\phi_{g_2}(x)) \\ &= \phi_{g_1}\phi_{g_2}(x) \end{aligned}$$

Por lo tanto

$$\phi(g_1 g_2) = \phi_{g_1}\phi_{g_2} = \phi(g_1)\phi(g_2)$$

Además ϕ es inyectiva. Supongamos que $\phi(g) = I$. Luego $\phi_g(x) = x$ para todo x en G, y por lo tanto $\phi_g(e) = e$, lo cual implica $ge = e$, de donde $g = e$.

Si tomamos H la imagen de ϕ, en $A(G)$, entonces se tiene que

$$G \approx H$$

Observación: El teorema de Cayley, si bien es muy importante desde el punto de vista teórico, no tiene mucha aplicación práctica, pues el grupo $A(G)$ es inmenso comparando con G. Por ejemplo, si el orden de G es 20, entonces $A(G)$ tiene orden 20! ¿Cómo hacemos para hallar este pequeño grupo de orden 20 dentro de un grupo de orden 2432902008176640000?

5.3 Descomposición Cíclica

Sea S un conjunto finito de n elementos. Estudiaremos en detalle **el grupo de permutaciones de** S, el cual se denota por $A(S)$.

Sea $S = \{x_1, \ldots, x_n\}$ entonces si θ es una permutación de S podemos representarla en la forma

$$\theta = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix},$$

donde $\theta x_1 = x_{i_1}, \theta x_2 = x_{i_2}, \ldots, etc.$

Podemos simplificar esta notación, eliminado las x, para obtener

$$\theta = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

Así pues una permutación del conjunto S, se puede representar, sin ambigüedad, por una permutación del conjunto $\{1, 2, \ldots, n\}$. El conjunto de estas prmutaciones se denota por S_n y se llama **Grupo Simétrico de grado** n.

Observación: Cuando se tienen dos permutaciones θ y τ en S_n, el producto $\theta\tau$ se interpreta de la forma siguiente:

$$\theta\tau(m) = \tau(\theta(m)),$$

para todo $m \in \{1, 2, \ldots, n\}$.

Es decir, convenimos en "leer" el producto de permutaciones de izquierda a derecha. Otros autores lo hacen en sentido contrario, pero en todo este trabajo usamos siempre la misma convención.

Por ejemplo si θ, τ en S_6 son de la forma

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix}$$

Entonces

$$\theta\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$$

$$\tau\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$$

Nótese que

$$\theta\tau \neq \theta\tau.$$

y por lo tanto S_n no es abeliano, para $n > 2$.

Definición 5.3.1 *Sea $\theta \in S_n$ y m un elemento del conjunto*

$$\{1, 2, \ldots, n\}.$$

Diremos que la permutación θ:

1) **Mueve** *a m si $\theta(m) \neq m$*

2) **Fija** *a m si $\theta(m) = m$.*

Observación: El conjunto de los elementos de $\{1, 2, \ldots, n\}$ que son movidos por una permutación σ, se denota por A_σ y se llama **el soporte de la permutación**.

Por ejemplo, si σ y θ son las dos permutaciones dadas con anterioridad, tendremos:

$$A_\sigma = \{1, 2, 3\} \text{ y } A_\theta = \{1, 2, 3, 4\}$$

Definición 5.3.2 *Dos premutaciones σ y θ_1 se dicen* **permutaciones disjuntas**, *si $A_\sigma \cap A_\theta = \phi$.*

Ejemplo: 1 En S_6 consideremos las permutaciones

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

y

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

entonces θ y σ son disjuntas.

Teorema 5.3.1 *Sean θ_1 y θ_2 permutaciones disjuntas en S_n. Entonces ellas conmutan, es decir*

$$\theta_1\theta_2 = \theta_2\theta_1.$$

Demostración: Sea $m \in \{1, 2, \ldots, n\}$ y consideremos las tres posibilidades:

1) θ_1 y θ_2 fijan a m.

2) θ_2 mueve a m.

3) θ_1 mueve a m.

1) En este caso se tiene

$$\theta_1\theta_2(m) = m = \theta_2\theta_1(m)$$

luego ellas conmutan.

2) Supongamos $\theta_1(m) = m$ y $\theta_2(m) = k$ con $k \neq m$. Entonces $\theta_1(k) = k$, pues θ_2 mueve a k.

Luego

$$\theta_1\theta_2(m) = \theta_2(m) = k$$
$$\theta_2\theta_1(m) = \theta_1(k) = k$$

es decir

$$\theta_1\theta_2(m) = \theta_2\theta_1(m)$$

3) Si $\theta_1(m) = t$, con $t \neq m$, se tiene que $\theta_2(m) = m$.

Además $\theta_2(t) = t$, pues θ_1 mueve a t. Luego

$$\theta_1\theta_2(m) = \theta_2(t) = t$$
$$\theta_2\theta_1(m) = \theta_1(m) = t$$

esto es

$$\theta_1\theta_2(m) = \theta_2\theta_1(m)$$

Por lo tanto hemos probado que

$$\theta_1\theta_2 = \theta_2\theta_1$$

♠

Definición 5.3.3 *Una permutación $\theta \in S_n$ se llama* **un ciclo**, *si existen elementos s_1, $s_2, \ldots s_k$ en el conjunto $\{1, 2, \ldots, s\}$ tales que*

1. *Se tienen las relaciones $\theta(s_1) = s_2$, $\theta(s_2) = s_3 \ldots \theta(s_{k-1}) = s_k$ y $\theta(s_k) = s_1$.*
2. *La permutación θ deja fijo a todos los elementos de $\{1, 2, \ldots, n\}$ distintos de los s_i.*

Para expresar la permutación anterior, se usa la notación cíclica.

$$\theta = (s_1, s_2, \ldots, s_k)$$

Definición 5.3.4 *El entero k en la definición de arriba, se llama* **la longitud de la permutación**

Ejemplo: 1 La permuatción $\sigma \in S_7$ dada por

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

es un ciclo, ella se denota por $\sigma = (1,\ 5,\ 7,\ 2)$

Definición 5.3.5 *Sea θ una permutación de S_n y $s \in \{1, 2, \ldots, n\}$, entonces el conjunto*

$$\theta_s = \{s, \theta(s), \theta^2(s), \ldots\}$$

se llama la **órbita de** *s bajo la permutación θ.*

Lema 5.3.1 *Para todo $s \in \{1, 2, \ldots, n\}$ existe un entero positivo k, el cual depende de s. tal que*

$$\theta_s = \{s, \theta(s), \ldots, \theta^{k-1}(s)\}.$$

Demostración: Nótese que el conjunto

$$s, \theta(s), \theta^2(s), \ldots, \theta^n(s), \ldots$$

es finito.

Luego debe haber repeticiones entre estos elementos y por lo tanto existen subíndices i, j con $i < j$ tales que

$$\theta^i(s) = \theta^j(s)$$

es decir,

$$\theta^{i-j}(s) = s$$

Luego si, se toma $t = i - j$ y por lo tanto se cumple

$$\theta^t(s) = s$$

Sea

$$k = \min\{t \mid \theta^t(s)\}$$

Afirmamos que los elementos $s, \theta(s), \ldots, \theta^{k-1}(s)$ son todos distintos. En efecto, si hay una repetición, digamos para $h < \ell$, con $0 \leq h < k$ y $0 \leq \ell < k$

$$\theta^h(s) = \theta^\ell(s)$$

entonces

$$\theta^{\ell-h}(s) = s, \quad \text{y} \;\; 0 \leq \ell - h < k$$

Esto contradice la minimalidad de k y por lo tanto $\theta^h(s)$ y $\theta^\ell(s)$ son distintos.

Por otro lado, si n es cualquier entero positivo, se tiene

$$n = p \cdot k + r, \quad \text{con} \;\; 0 \leq r < k$$

y por lo tanto

$$\begin{aligned} \theta^n(s) &= \theta^{p\cdot k+r}(s) \\ &= \theta^r(\theta^{p\cdot k}(s)) \\ &= \theta^r(s) \end{aligned}$$

Con esto se da fin a la prueba.

♠

Observación: Si θ es una permutación en S_n, entonces la relación en s

$$s_1 \sim s_2 \iff s_1 = \theta^i(s_2),$$

para algún i entero, es de equivalencia.

Además cada clase de equivalencia es una órbita de la permutación. El conjunto $\{1, 2, \ldots, n\}$ queda así dividido en la unión de órbitas disjuntas.

Cada órbita de θ origina la permutación

$$\Big(s, \theta(s), \ldots, \theta^{\ell-1}(s)\Big)$$

Este tipo de permutación se llama un **ciclo**.

Ejemplo: Consideremos la permutación

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

Entonces las distintas órbitas son

$$\begin{aligned} \theta_1 &= \{1, 3, 8\} \\ \theta_2 &= \{2, 4, 5, 9\} \\ \theta_6 &= \{6, 7\} \end{aligned}$$

y los ciclos correspondientes vienen dados por:

$$\begin{aligned} c_1 &= (1, 3, 8) \\ c_2 &= (2, 4, 5, 9) \\ c_3 &= (6, 7) \end{aligned}$$

Teorema 5.3.2 *Toda permutación se escribe como un producto de ciclos disjuntos.*

Demostración: Descomponer el conjunto $\{1, 2, \ldots, n\}$ en la unión disjuntas de sus órbitas. Luego formar los ciclos $c_1, \ldots, c_t$.

Afirmamos que

$$\theta = c_1 \cdots c_t$$

En efecto, sea $s \in \{1, 2, \ldots, n\}$. Entonces s aparece en sólo uno de los ciclos, digamos c_i, luego

$$\begin{aligned} c_1 \cdots c_t(s) &= c_1 \cdots c_i(s) \\ &= c_1 \cdots c_{i-1}(\theta(s)) \\ &= \theta(s) \end{aligned}$$

♠

Definición 5.3.6 *Un ciclo de longitud 2 se llama una* **transposición**.

Nota: Si θ es el ciclo $\theta = (s_1, \ldots, s_t)$, entonces se demuestra la fórmula:

$$\theta = (s_1, s_2)(s_1, s_3) \cdots (s_1, s_t) \tag{5.2}$$

Teorema 5.3.3 *Toda permutación se puede escribir como un producto de transposiciones.*

Demostración: Hemos probado que toda permutación se escribe como un producto de ciclos. Si ahora usamos la fórmula (**??**), para descomponer cada ciclo como un producto de transposiciones, se obtiene el resultado deseado.

♠

Ejemplo: La permutación θ del ejemplo anterior, puede ser descompuesta en ciclos:

$$\begin{aligned} \theta &= (1,3,8)(2,4,5,9)(6,7) \\ &= (1,3)(1,8)(2,4)(2,5)(2,9)(6,7) \end{aligned}$$

Ejercicios

1) Sean θ y τ las permutaciones en S_8 dadas por

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

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

Hallar

a) $\theta\tau$

b) $\tau\theta$

c) $\tau^{-1}\theta^{-1}$

d) $\theta^3\tau^3$

e) $\theta\tau\theta^{-1}$

2) Sea A el conjunto de permutaciones en S_6 que conmutan con la permutación $\theta = (1, 2, 4)$. Probar que A es un subgrupo de S_6. ¿Cuál es el orden de A?

3) Probar que el orden de un ciclo en S_n es igual a su longitud.

4) Probar la fórmula en S_n

$$(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$$

5) Sea $\theta \in S_n$. Sean a, b en $\{1, 2, \ldots, n\}$ y diremos que a y b están relacionados si

$$a = \theta^t(b)$$

para algún $t \in \mathbb{Z}$. Probar que ésta relación es de equivalencia en $\{1, 2, \ldots, n\}$.

6) Calcule el número de órbitas de $\theta = (3, 5, 7)$ en S_9.

7) Sean θ_1 y θ_2 dos ciclos disjuntos de ordenes m y n con $(m, n) = 1$. Probar que el orden de $\theta_1\theta_2$ es mn.

8) Sean $\theta_1, \ldots, \theta_s$ ciclos disjuntos de ordenes $m_1, \ldots, m_s$ ¿Cuál es el orden de $\theta_1 \ldots, \theta_s$?.

9) Sea $G = D_n$ el grupo diédrico de grado n. Hallar la representación de este grupo como un grupo de permutaciones en S_n.

5.4 Grupo Alternante

Definición 5.4.1 *Una permutación θ en S_n se llama* **permutación par** *si se puede descomponer como un número par de transposiciones.*

Si una permutación se descompone como un número impar de transposiciones, entonces diremos que es **impar.**

Una permutación no puede ser par e impar a la vez, como veremos a continuación:

Teorema 5.4.1 *Sea $\theta \in S_n$ una permutación. Entonces θ no puede ser descompuesta como un producto de un número par de transposiciones e impar de transposiciones simultáneamente.*

Demostración: La prueba la dividimos en dos casos:

Caso I: Si $\theta = I$ la permutación identidad. Entonces afirmamos que θ sólo puede ser descompuesta como un número par de transposiciones.

En efecto, si

$$I = \alpha_1 \cdots \alpha_k \tag{5.3}$$

donde cada α_i es una transposición, probaremos que k debe ser par.

Sea s un entero en el conjunto $\{1, 2, \ldots, n\}$ tal que s es movido por algunas de las transposiciones en (**??**) y supongamos que α_j es la primera transposición que mueve a m. Entonces, debe ser $j < k$, pues si la última transposición mueve a m, y ninguna de las anteriores lo hace, el producto en (**??**) no es la identidad.

Sea $\alpha_j = (m, x)$, donde $x \in \{1, 2, \ldots, n\}$. Entonces tenemos dos posibilidades para la siguiente permutación a la derecha α_j, la cual denotamos por α_{j+1}.

1) Si α_{j+1} mueve a m, entonces el producto $\alpha_j\alpha_{j+1}$ se reduce a algunos de los siguientes casos:

$$\alpha_j\alpha_{j+1} = (x, m)(x, m) = I$$
$$\alpha_j\alpha_{j+1} = (x, m)(y, m) = (x, y)(x, m)$$

2) Si α_{j+1} no mueve a m, entonces el producto $\alpha_j\alpha_{j+1}$ se expresa de alguna de las dos formas

$$\alpha_j\alpha_{j+1} = (x,m)(y,z) = (y,z)(x,m)$$
$$\alpha_j\alpha_{j+1} = (x,m)(x,y) = (x,y)(y,m)$$

En conclusión se tiene que α_{j+1} es la primera transposición que mueve a m o bien m desaparece en (**??**), eliminando dos transposiciones. Continuando este proceso se pueden cancelar todas las transposiciones en (**??**), hasta tener la identidad en ambos lados. Luego k debe ser par.

Caso II: Sea θ una permutación cualquiera en S_n y consideremos dos posibles descomposiciones de esta, como producto de transposiciones

$$\theta = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_t$$

Luego

$$\begin{aligned} \theta\theta^{-1} &= \alpha_1 \cdots \alpha_k(\beta_1 \cdots \beta_t)^{-1} \\ &= \alpha_1 \cdots \alpha_k\beta_t^{-1} \cdots \beta_1^{-1} \\ &= \alpha_1 \cdots \alpha_k\beta_t \cdots \beta_1 \end{aligned}$$

pues β_i es una transposición, y por lo tanto

$$\beta_i^{-1} = \beta_i.$$

luego se tiene

$$I = \alpha_1 \cdots \alpha_k\beta_t \cdots \beta_1,$$

y usando el primer caso se concluye que $\alpha + t$ debe ser par. Luego α y t deben ser ambos pares o impares.

Definición 5.4.2 *Una permutación θ en S_n, se dice* **par** *(respectivamente* **impar***) si θ se puede expresar como el producto de un número par (respectivamente impar) de transposiciones.*

El producto de dos permutaciones pares es de nuevo una permutación par. Además si θ es par, su inverso θ^{-1} es también una permutación par.

Luego el conjunto de las permutaciones pares de S_n, es un grupo el cual se denomina **Grupo Alternante de grado n** y se denota por A_n.

Teorema 5.4.2 *El grupo alternante A_n, es un subgrupo normal de S_n y tiene orden*

$$\circ(A_n) = n!/2$$

Demostración: Sea U el grupo formado por 1 y -1 bajo el producto de los números enteros. Consideremos la aplicación

$$\varphi : S_n \longrightarrow U$$

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

Entonces se puede verificar fácilmente que φ es un homomorfismo de grupos, el cual es sobre. ¿Quién es el Kernel de φ?

Tenemos que $\ker \varphi$ son exactamente aquellas permutaciones pares, esto es el grupo A_n. Además por el primer teorema de los isomorfismos, obtenemos

$$S_n/\ker \varphi = S_n/A_n \approx U,$$

luego

$$\circ(S_n/A_n) = \circ(U) = 2$$

pero

$$\circ(S_n/A_n) \quad = \quad \frac{\circ(S_n)}{\circ(A_n)} = \frac{n!}{\circ(A_n)}$$

y de esto se concluye

$$\circ(A_n) = \frac{n!}{2}$$

♠

5.5 Simplicidad de A_n $(n \geq 5)$

En esta sección se demuestra uno de los hechos más resaltantes sobre el grupo de permutaciones, como lo es la simplicidad del grupo alternante A_n, para $n \geq 5$.

Este resultado tiene profundas y sorprendentes concecuencias cuando se considera el grupo de permutaciones de las raíces de un polinomio de grado mayor o igual a 5 sobre los racionales. La simplicidad de A_n en este contexto implica la imposibilidad de obtener dichas raíces usando radicales.

Sin embargo no podemos estudiar con detalle esta aplicación. Para la misma se requieren algunos conocimientos de la teoría de cuerpos que no están a nuestro alcance en este momento.

Definición 5.5.1 *Un grupo G se dice* **simple** *si no posee subgrupos normales diferentes de los triviales.*

Lema 5.5.1 *Sean $\varphi = (1,2)$ y $\psi = (1,2,\ldots,n)$. Entonces S_n es generado por estas dos permutaciones.*

Demostración: La prueba se hará en varios pasos:

1) Demostraremos que φ, ψ generan todas los transposiciones

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

2) Probaremos que esas transposiciones generan todas las transposiciones.

3) Luego cada $\sigma \in S_n$ al ser generada por un producto de transposiciones, es generada por φ y ψ.

Iniciamos la demostración calculando algunos valores de $\psi^{-n}\varphi\psi^n$.

$$\begin{aligned} \psi^{-1}\varphi\psi(1) &= (n)\varphi\psi \\ &= (n)\psi \\ &= 1 \end{aligned}$$

$$\begin{aligned} \psi^{-1}\varphi\psi(2) &= (1)\varphi\psi \\ &= (2)\psi \\ &= 3 \end{aligned}$$

$$\begin{aligned} \psi^{-1}\varphi\psi(3) &= (2)\varphi\psi \\ &= (1)\psi \\ &= 2 \end{aligned}$$

Si $3 < s \leq n$

$$\begin{aligned} \psi^{-1}\varphi\psi(s) &= (s-1)\varphi\psi \\ &= (s-1)\psi \\ &= s \end{aligned}$$

Luego hemos probado

$$\begin{aligned} \psi^{-1}\varphi\psi(1) &= (2,3) \\ &= (\psi(1), \psi(2)) \end{aligned}$$

En general, probaremos la fórmula

$$\psi^{-k}\varphi\psi^k = (\psi^k(1), \psi^k(2)) \tag{5.4}$$

Es más, si φ es cualquier ciclo $\varphi = (a_1, \ldots, a_s)$. Entonces se tiene

$$\psi^{-k}\varphi\psi^k = (\psi^k(a_1), \ldots \psi^k(a_s)) \tag{5.5}$$

para todo k, $1 \leq k \leq n$.

Para probar (**??**), notemos en primer lugar que

$$\begin{aligned}(\psi^k(1))\psi^{-k}\varphi\psi^k &= (1)\varphi\psi^k \\ &= 2\psi^k \\ &= \psi^k(2),\end{aligned}$$

y además

$$\begin{aligned}(\psi^k(2))\psi^{-k}\varphi\psi^k &= (2)\varphi\psi^k \\ &= 1\psi^k \\ &= \psi^k(1)\end{aligned}$$

Por otro lado, sea $t \neq \psi^k(1), \psi^k(2)$, entonces como ψ^k es biyectiva, existe $x \neq 2, 1$ tal que

$$t = \psi^k(x)$$

luego

$$\begin{aligned}(t)\psi^{-k}\varphi\psi^k &= (\psi^k(x))(\psi^{-k}\varphi\psi^k) \\ &= (x)\varphi\psi^k \\ &= (x)\psi^k \\ &= \psi^k(x) \\ &= t\end{aligned}$$

Luego el elementos t no es movido por esa permutación y por lo tanto

$$\psi^{-k}\varphi\psi^k = (\psi^k(1), \psi^k(2))$$

De esta forma las permutaciones φ, ψ generan todas las transposiciones

$$(1,2)(2,3)(3,4)\cdots(n-1,n)$$

¿Como generamos una permutación del tipo $(1, a)$ con $2 \leq a \leq n$?

Simplemente usamos la fórmula de recurrencia

$$(1, a-1)(a-1, a)(1, a-1) = (1, a). \tag{5.6}$$

2) Si (a, b) es cualquier transposición, entonces

$$(1, a)(1, b)(1, a) = (a, b)$$

Luego (a, b) es generado por φ, ψ.

3) Si θ es cualquier permutación, entonces

$$\theta = \theta_1 \cdots \theta_t$$

donde cada θ_i es una transposición. Con esto se da fin a la prueba.

♠

Lema 5.5.2 *Probar que para $n \geq 3$, el grupo generado por los $3-$ciclos es A_n.*

Demostración: Sea H =subgrupo de S_n generado por los $3-$ciclos. Como cada $3-$ciclo es de la forma:

$$(a, b, c) = (a, b)(a, c),$$

se tiene que

$$H \subseteq A_n$$

Luego si $\theta \in A_n$, entonces θ es producto de un número par de transposiciones.

Si demostramos que el producto de dos transposiciones es un $3-$ciclo o producto de $3-$ciclos estará listo.

Tenemos dos casos a considerar

1) $(a, b)(a, c) = (a, b, c)$.

2) $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, b, c)(c, a, d)$.

Por lo tanto los 3-ciclos generan al grupo alternante A_n.

♠

Lema 5.5.3 *A_n, $n \geq 3$ esta generado por $3-$ciclos de la forma*

$$(1,2,3)(1,2,4)\cdots(1,2,n).$$

Demostración: Basta probar que todo ciclo de la forma (a,b,c) esta generado por un producto de los anteriores o sus inversos.

En primer lugar

$$(1,2,b)^{-1}(1,2,c)(1,2,b) = (\psi(1),\psi(2),\psi(c)) \tag{5.7}$$

donde $\psi = (1,2,b)$

luego

$$\begin{aligned}(1,2,b)^{-1}(1,2,c)(1,2,b) &= (2,b,c)\\ (2,b,c)(2,b,a)(2,b,c)^{-1} &= (\psi(2),\psi(b),\psi(a))\end{aligned}$$

donde $\psi = (2,b,c)$

Luego

$$(1,2,b)^{-1}(1,2,c)(1,2,b) = (b,c,a) = (a,b,c)$$

De esta forma obtenemos el $3-$ciclo buscado.

♠

Lema 5.5.4 *Sea N un subgrupo normal de A_n, $(n \geq 3)$. Si N contiene un $3-$ciclo (a,b,c), entonces*

$$N = A_n.$$

Demostración:

$$\begin{aligned}(1,2,a)^{-1}(a,b,c)(1,2,a) &= (\psi(a),\psi(b),\psi(c))\\ &= (1,b,c) \in N\end{aligned}$$

con $\psi = (1, 2, a)$

Sea $\lambda = (b, 2)(c, k) \in A_n$

$$\begin{aligned} \lambda^{-1}(1, b, c)\lambda &= (\lambda(1), \lambda(b), \lambda(c)) \\ &= (1, 2, k) \in N \end{aligned}$$

Luego N contiene todos los 3−ciclos

$$(1, 2, 3)(1, 2, 4) \cdots (1, 2, n)$$

y por lo tanto

$$N = S_n$$

♠

Teorema 5.5.1 *A_n, $(n \geq s)$ es simple.*

Demostración: Sea $N \neq \{e\}$ un subgrupo normal de A_n. Será suficiente con probar que N contiene 3−ciclo.

Sea $\theta \in N$ tal que θ fija el mayor número de elementos del conjunto $\{1, 2, \ldots, n\}$.

Afirmamos que θ es un 3−ciclo. Si θ no es un 3−ciclo, entonces θ mueve más de 3 elementos, luego podemos suponer

1) $\theta = (1, 2, 3, \ldots)$
o bien

2) $\theta = (1, 2)(3, 4) \cdots$

En el primer caso θ mueve 2 elementos más, digamos 4 y 5, pues si $\theta = (1, 2, 3, 4)$ entonces θ es impar.

Sea $\tau = (3, 4, 5) \in A_n$ y hagamos

$$\theta_1 = \tau\theta\tau^{-1} \in N$$

Si θ es como en 1) entonces

$$\theta_1 = (1, 2, 4, 5, \ldots)$$

Si θ es como en 2) entonces

$$\theta_1 = (1, 2)(4, 5) \cdots$$

Luego

$$\theta_1 \neq \theta$$

y por lo tanto

$$\theta_2 = \tau\theta\tau^{-1}\theta^{-1} \neq e$$

Si θ fija un número s de elementos, con $s > 5$, entonces θ_2 fija dicho número. Además, si θ es como en 1)

$$\begin{aligned} \theta_2(1) &= (1)\tau\theta\tau^{-1}\theta^{-1} \\ &= (1)\theta\tau^{-1}\theta \\ &= (2)\tau^{-1}\theta^{-1} \\ &= 2(\theta^{-1}) \\ &= 1 \end{aligned}$$

Luego θ mueve 1,2,3,4,5 y θ_2 fija 1. Por lo tanto θ_2 tiene más elementos fijos que θ, lo cual es una contradicción.

Si θ es como en 2)

$$\begin{aligned} \theta_2(1) &= (1)\tau\theta\tau^{-1}\theta^{-1} \\ &= (1)\theta\tau^{-1}\theta^{-1} \\ &= (1) \end{aligned}$$

$$\begin{aligned} \theta_2(2) &= (2)\tau\theta\tau^{-1}\theta^{-1} \\ &= (2)\theta\tau^{-1}\theta^{-1} \\ &= (2) \end{aligned}$$

Luego θ fija más elementos que θ lo cual es nuevamente una contradicción.

♠

Ejercicios

1) Determine cuales de las siguientes permutaciones en S_8 son pares y cuales son impares.

a) $(1,2,3)(5,2)$

b) $(4,5,6,7)(1,2)$

c) $(1,2,3,4)(7,8)$

d) $(2,8,7,6,4,5)$

e) $(2,4,5)(3,8,1)$

f) $(1,8,7)(2,5,4,3,6)$

2) Sean θ y τ las permutaciones en S_6 dadas por $\theta = (1,2,3)(4,5)$ $\tau = (1,5,7,4)$

Calcular

a) $\theta^{-1}\tau\theta$

b) $\theta^{-k}\tau\theta^k$, para $2 \leq k \leq 6$.

3) Hallar la descomposición en ciclos de

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 1 & 4 & 6 & 5 & 12 & 11 & 9 & 8 & 2 & 7 & 3 \end{pmatrix}$$

4) Determine si la permutación anterior es par.

5) Demuestre que el producto de dos ciclos disjuntos en S_n es conmutativo.

6) Sea $\theta = (a_1, \ldots, a_t)$ un ciclo de S_n y $\psi \in S_n$. Probar la fórmula

$$\psi^{-1}\theta\psi = (\psi(a_1), \ldots, \psi(a_t)).$$

7) Probar la fórmula (**??**)

8) Probar la fórmula (**??**)

9) Probar la fórmula (**??**)

10) Dos permutaciones θ y τ en S_n se dicen **conjugadas**, si existe otra permutación σ en S_n tal que

$$\theta = \sigma\tau\sigma^{-1}.$$

Halle todos los conjugados de la permutación $(1, 2, 3)$ en S_5.

11) Demuestre que si dos ciclos son conjugados, entonces tiene la misma longitud.