Permutaciones y Grupo Simétrico

José Luis Chacón

Introducción

[1] Generalizaciones de la fórmula cuadrática para polinomios cúbicos y cuárticos fueron descubiertos en el siglo XVI, y uno de los mayores problemas matemáticos desde entonces fue encontrar fórmulas análogas para las raíces de polinomios de mayor grado; todos los intentos fracasaron. A mediados del siglo XVIII se entendió que las permutaciones de las raíces de un polinomio $f(x)$ era importante; por ejemplo, se conoció que los coeficientes de $f(x)$ son "funciones simétricas"de sus raíces. En 1770 J.-L. Lagrange usó permutaciones para analizar las fórmulas dadas las raíces de cúbicas y cuárticas, pero no desarrolló completamente esta visión puesto que vio en las permutaciones sólo rearreglos, y no biyecciones que pueden componerse.Composición y permutación aparece en el trabajo de P. Ruffini y de P. Abbati cerca de 1800; en 1815, A.L. Cauchy estableció el cálculo de permutaciones, y este punto de vista fue usado por N.H. Abel en su prueba (1824) de que existen polinomios quínticos para los cuales no existe generalización de la fórmula cuadrática. En 1830, E. Galois inventó los grupos, asociando a cada polinomio un grupo de permutaciones de sus raíces, y probó que existe una fórmula para las raíces si y sólo si el grupo de permutaciones tiene una propiedad especial.

1. Permutaciones

Definición 1 Si X es un conjunto no vacío, una **permutación** de X es una biyección $\alpha : X \to X$. Denotamos el conjunto de todas las permutaciones de X por S_X.

Tiene importancia especial el caso cuando $X = \{1, 2, \ldots, n\}$, aquí escribimos S_n en lugar de S_X. Note que $\mid S_n \mid = n!$, donde $\mid Y \mid$ denota el número de elementos del conjunto Y.

En la época de Lagrange, una permutación de $X = \{1, 2, \ldots, n\}$ era vista como un rearreglo; esto es, como una lista $i_1, i_2, \ldots, i_n$ sin repeticiones de todos los elementos de X. Un rearreglo $i_1, i_2, \ldots, i_n$ define una función $\alpha : X \to X$ por $\alpha(j) = i_j$ para toda $j \in X$. Esta función es una inyección puesto que en la lista no hay repeticiones; es sobreyectiva puesto que todos los elementos de

[1] Es una traducción de una parte del libro *An Introduction to Theory of Groups* de J.J. Rotman y se agregan ejercicios de *Estructuras Algebraicas* de Herstein

X aparecen en la lista. Así cada rearreglo da una biyección. Recíprocamente, cualquier biyección α se puede denotar por dos filas:

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

y la fila inferior es un rearreglo de $\{1, 2, \dots, n\}$. Entonces las dos versiones de permutación, rearreglo y biyección, son equivalentes. La ventaja del nuevo punto de vista es que dos permutaciones de S_X, pueden ser "multiplicadas", por ser la composición de biyecciones una biyección.

Ejercicios 1.1

1.1 La función identidad 1_X sobre un conjunto X es una permutación, y usualmente se denota por 1. Pruebe que $1\alpha = \alpha = \alpha 1$ para cualquier permutación $\alpha \in X$.

1.2 Para cada $\alpha \in S_X$, pruebe que existe $\beta \in S_X$ tal que $\alpha\beta = 1 = \beta\alpha$.

1.3 Para todo $\alpha, \beta, \gamma \in S_X$, pruebe que $\alpha(\beta\gamma) = (\alpha\beta)\gamma$

Problemas 1.2

1. Para $\sigma \in S_n$ definimos la potencia k-ésima de sigma por recurrencia sobre los enteros positivos de esta manera: $\sigma^0 = 1$, $\sigma^{n+1} = \sigma\sigma^n$ y si $n < 0$ se define $\sigma^n = (\sigma^{-1})^{-n}$. Pruebe:

   a) $\sigma^n\sigma^m = \sigma^m\sigma^n$ para enteros n, m.

   b) $\sigma^{n+m} = \sigma^m\sigma^n$ para enteros n, m.

   c) $\sigma^{nm} = (\sigma^n)^m$ para enteros n, m.

2. Si $\sigma \in S_n$, $i \in [n]$, pruebe que existe algún entero positivo k, dependiendo de σ, tal que $\sigma^k(i) = i$

3. Si $\sigma \in S_n$, pruebe que existe algún entero positivo k, dependiendo de σ, tal que $\sigma^k = 1$

4. Pruebe que hay un entero positivo k tal que $\sigma^k = 1$ para toda $\sigma \in S_n$.

5. Si $m < n$, pruebe que existe una aplicación inyectiva $F : S_m \to S_n$ tal que $F(\sigma\gamma) = F(\sigma)F(\gamma)$ para toda σ, $\gamma \in S_m$.

6. Dar dos permutaciones en S_3 que no conmuten.

7. Si $n \geq 3$, pruebe que existen permutaciones α, $\beta \in S_n$ que no conmutan. **Sugerencia.** Para cualquier $n > 3$ verifique que si α y β no conmutan entonces $F(\alpha)$ y $F(\beta)$ no conmutan. F es la función definida dos problemas arriba.

8. Si $\sigma \in S_n$, pruebe que $\sigma = \tau_1\tau_2\cdots\tau_m$ para algunas $\tau_i \in S_n$ tales que $(\tau_i)^2 = 1$. **Sugerencia.** Por inducción sobre el número de elementos que la permutación mueve, es decir, sobre el conjunto $H = \{i|\sigma(i) \neq i\}$. Luego probar que si $\sigma(i) = j$ y τ se obtiene de σ así: $\tau(j) = j$, $\tau(i) = \sigma(j)$ y $\tau(k) = \sigma(k)$ para $k \notin \{i, j\}$ se tiene que $\sigma = \tau(ij)$ donde (ij) es una trasposición (intercambio de los elementos i y j). Además el número de elementos que mueve τ es menor que el número de elementos que mueve σ. Pueden ver la parte inicial de la siguiente sección para informarse de las definiciones.

2. Ciclos

Para distinguir importantes rasgos de permutaciones especiales usaremos una mejor notación.

Definición 2 Si $i \in [n]$ y $\alpha \in S_n$, entonces α **fija** i si $\alpha(i) = i$ y α **mueve** i si $\alpha(i) \neq i$.

Definición 3 Sean $i_1, i_2, \ldots, i_r$ enteros distintos entre 1 y n. Si $\alpha \in S_n$ fija los $n - r$ enteros restantes y si

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

entonces α es un **r-ciclo**; se puede decir que α es un ciclo de **longitud r**. Se denota α por $(i_1\ i_2\ \ldots\ i_r)$.

Cada 1-ciclo fija un elemento de X, y así todos los 1-ciclos son iguales a la identidad. Un 2-ciclo, el cual es simplemente el intercambio de un par de elementos, es denominado **trasposición**.

La multiplicación es fácil cuando se usa la notación cíclica. Por ejemplo, calculemos $\gamma = \alpha\beta$, donde $\alpha = (1\ 2)$ y $\beta = (1\ 3\ 4\ 2\ 5)$. Puesto que la multiplicación es composición de funciones, $\gamma(1) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(3) = 3$; luego $\gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4$ y $\gamma(4) = \alpha(\beta(4)) = \alpha(2) = 1$. Resulta

$$(1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$$

Definición 4 Dos permutaciones $\alpha, \beta \in S_X$ son **disjuntas** si cada x movido por una es fijado por la otra. En símbolos, si $\alpha(x) \neq x$, entonces $\beta(x) = x$ y si $\beta(y) \neq y$ entonces $\alpha(y) = y$ (por supuesto, es posible que existan elementos en X que sean fijos por ambas permutaciones). Una familia de permutaciones $\alpha_1, \alpha_2\ \ldots\ \alpha_m$ es **disjunta** si cada par de ellas es disjunta.

Ejercicios 2.1

1.4 Pruebe que $(i_1\ i_2\ \cdots\ i_{r-1}\ i_r) = (i_2\ i_3\ \cdots\ i_r\ i_1) = (i_3\ i_4\ \cdots\ i_1\ i_2) = \cdots = (i_r\ i_1\ \cdots\ i_{r-2}\ i_{r-1})$. Concluya que hay exactamente r de tales notaciones para cualquier r-ciclo.

1.5 Si $1 \leq r \leq n$, entonces existen $\binom{n}{r}(r-1)!$ r-ciclos en S_n.

1.6 Pruebe la **ley de cancelación** para permutaciones: si $\alpha\beta = \alpha\gamma$, o bien $\beta\alpha = \gamma\alpha$, entonces $\beta = \gamma$.

1.7 Sean $\alpha = (i_1\ i_2\ \cdots\ i_r)$ y $\beta = (j_1\ j_2\ \cdots\ j_s)$. Pruebe que α y β son disjuntos si y sólo si $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \varnothing$.

1.8 Si α y β son permutaciones disjuntas, entonces $\alpha\beta = \beta\alpha$; esto es, α y β **conmutan**.

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

1.10 Si $\alpha, \beta \in S_n$ son disjuntas, pruebe que $(\alpha\beta)^k = \alpha^k\beta^k$ para todo $k \geq 0$

1.11 Muestre que la potencia de un ciclo no es necesariamente un ciclo.

1.12 (i) Sea $\alpha\,(i_0\ i_1\ \cdots\ i_{r-1})$ un r-ciclo. Para cada $j,\ k \geq 0$, pruebe que $\alpha^k(i_j) = i_{k+j}$ si los subíndices se leen modulo r.

(ii) Pruebe que si α es un r-ciclo, entonces $\alpha^r = 1$, pero que $\alpha^k \neq 1$ para todo entero positivo $k < r$.

(iii) Si $\alpha = \beta_1\beta_2\ldots\beta_m$ es un producto de r_i-ciclos β_i, entonces el entero positivo más pequeño l tal que $\alpha^l = 1$ es el mínimo común múltiplo de $\{r_1, r_2, \ldots, r_m\}$.

1.13 (i) Una permutación $\alpha \in S_n$ es **regular** si α no fija puntos y es producto de ciclos disjuntos de la misma longitud o $\alpha = 1$. Pruebe que α es regular si y sólo si es una potencia de un n-ciclo β; esto es, $\alpha = \beta^m$ para algún m.
(Sugerencia:
Si $\alpha = (x_1^1\ x_2^1\ \cdots\ x_k^1)(x_1^2\ x_2^2\ \cdots\ x_k^2)\ldots(x_1^m\ x_2^m\ \cdots\ x_k^m)$, tome $\beta = (x_1^1\, x_1^2\, \ldots\, x_1^m\, x_2^1\, x_2^2\, \ldots\, x_2^k\, \ldots\, x_k^1\, x_k^2\, \ldots\, x_k^m)$.)

(ii) Si α es un n-ciclo, entonces α^k es un producto de $(n,\ k)$ ciclos disjuntos, cada uno de longitud $n/(n,\ k)$. (Recuerde que $(n,\ k)$ denota el máximo común divisor de n y k.)

a) Si p es primo, entonces cualquier potencia de un p-ciclo es o bien un p-ciclo o 1.

1.14 (i) Sea $\alpha = \beta\gamma$ en S_n, donde β y γ son disjuntas. Si β mueve a i, entonces $\alpha^k(i) = \beta^k(i)$ para todo $k \geq 0$.

(ii) Sean α y β ciclos en S_n. Si existe i_1 movido por ambas permutaciones y si $\alpha^k(i_1) = \beta^k(i_1)$ para todo entero positivo k, entonces $\alpha = \beta$.

3. Factorización en ciclos disjuntos

Teorema 3.1 Cada permutación $\alpha \in S_n$ es, o bien un ciclo o un producto de ciclos disjuntos.

Prueba. La prueba es por inducción sobre el número k de puntos que son movidos por α. El paso base $k = 0$ es verdadero, porque entonces α es la identidad, el cual es un 1-ciclo. Si $k > 0$, sea i_1 un punto movido por α. Defina $i_2 = \alpha(i_1)$, $i_3 = \alpha(i_2), \ldots, i_{r+1} = \alpha(i_r)$, donde r es el más pequeño entero para el cual $i_{r+1} \in \{i_1, i_2, \ldots, i_r\}$ (la lista $i_1, i_2, i_3, \ldots, i_k$, *dots* no puede continuar por siempre sin repetición ya que hay solamente n posibles valores). Obtenemos que $\alpha(i_r) = i_1$. En caso contrario, $\alpha(i_r) = i_j$ para algún $j \geq 2$; pero $\alpha(i_{j-1}) = i_j$, y esto contradice la hipótesis de que α es una inyección. Sea σ el r-ciclo $(i_1\, i_2 \cdots i_r)$. Si $r = n$ entonces α es el ciclo σ. Si $r < n$ y Y consiste en los $n-r$ puntos restantes, entonces $\alpha(Y) = Y$ y σ fija los puntos de Y. Ahora $\sigma \mid \{i_1, i_2, \ldots, i_r\} = \alpha \mid \{i_1, i_2, \ldots, i_r\}$. Es decir la permutación α restringida al conjunto $\{i_1, i_2, \ldots, i_r\}$ es exactamente el ciclo σ. Si α' es la permutación tal que $\alpha'(Y) = \alpha(Y)$ y la cual fija $\{i_1, i_2, \ldots, i_r\}$ entonces α' y σ son disjuntas, y además $\alpha = \sigma\,\alpha'$. Puesto que α' mueve menos puntos que α, la hipótesis inductiva muestra que α', y por lo tanto α, es producto de ciclos disjuntos. ■

Usualmente se suprimen todos los 1-ciclos, ya que representan los puntos que no son movidos por la permutación. Si todos los ciclos son 1-ciclos entonces la permutación es la identidad. Por otro lado, algunas veces es conveniente mostrar todos los ciclos.

Definición 5 Una **factorización completa** de una permutación α es una factorización de α como producto de ciclos disjuntos los cuales contienen un 1-ciclo(i) por cada i fijado por α.

En una factorización completa de una permutación α, cada i entre 1 y n aparece en exactamente uno de los ciclos.

Teorema 3.2 Sea $\alpha \in S_n$ y sea $\alpha = \beta_1 \ldots \beta_t$ una factorización completa en ciclos disjuntos. Esta factorización es única excepto por el orden en los cuales los factores aparecen.

Prueba. Los ciclos disjuntos conmutan, por el ejercicio 1.8, así el orden de los factores en una factorización completa no se determina de manera única; sin embargo, mostraremos que los factores mismos están determinado de manera única. Puesto que existe exactamente un 1-ciclo por cada i fijado por α, es suficiente probar la unicidad para los ciclos de longitud al menos 2. Suponga que $\alpha = \gamma_1 \ldots \gamma_s$ es una segunda factorización en ciclos disjuntos. Si β_t mueve a i_1, entonces $\beta_t^k(i_1) = \alpha^k(i_1)$ para todo k por el ejercicio 1.14(i). Ahora, algún γ_j debe mover a i_1; puesto que los ciclos disjuntos conmutan, podemos asumir que $\gamma_j = \gamma_s$. Pero $\delta_s^k(i_1) = \alpha^k(i_1)$ para todo k, y por el ejercicio 1.14(ii)

se concluye $\beta_t = \gamma_s$. La ley de cancelación, ejercicio 1.6, da $\beta_1 \dots \beta_{t-1} = \gamma_1 \dots \gamma_{s-1}$, y la prueba es completa por inducción sobre $\max\{s, t\}$. ■

Ejercicios 3.3

1.15 Sea α una permutación de $\{1, 2, \dots, 9\}$ definida por $\alpha(i) = 10 - i$. Escribir α como un producto de ciclos disjuntos.

1.16 Sea p un primo y sea $\alpha \in S_n$. Si $\alpha^p = 1$, entonces, o bien $\alpha = 1$, o α es un p-ciclo, o α es un producto de p-ciclos disjuntos. En particular, si $\alpha^2 = 1$, entonces $\alpha = 1$, α es una trasposición, o α es producto de trasposiciones disjuntas.

1.17 ¿Cuantas $\alpha \in S_n$ existen con $\alpha^2 = 1$? (Sugerencia. $(i\ j) = (j\ i)$, y $(i\ j)(k\ l) = (k\ l)(i\ j)$.)

1.18 Dar un ejemplo de permutaciones $\alpha, \beta, \gamma \in S_5$ con α conmutando con β, con β conmutando con γ, pero α no conmutando con γ.

4. Permutaciones Pares e Impares

Existe otra factorización de permutaciones que es útil.

Teorema 4.1 Toda permutación $\alpha \in S_n$ es un producto de trasposiciones.

Prueba. Por el teorema 3.1, es suficiente verificarlo para los factores cíclicos, y

$$(1\ 2\ \dots\ r) = (1\ r)(1\ r-1)\dots(1\ 2)$$

■

Cada permutación puede entonces realizarse a través de una sucesión de intercambios. Tal factorización no es tan buena como la factorización en ciclos disjuntos. Primero que todo, las trasposiciones que ocurren no son necesariamente conmutativas: $(1\ 3)(1\ 2) = (1\ 2\ 3)$ y $(1\ 2)(1\ 3) = (1\ 3\ 2)$; segundo, ni los factores, ni el número de factores están únicamente determinados; por ejemplo,

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

¿Existe alguna unicidad en todas estas factorizaciones? Probaremos que la *paridad* del número de factores es igual para todas las factorizaciones de una permutación α: esto es, el número de trasposiciones es siempre par o es siempre impar.

Definición 6 Una permutación $\alpha \in S_n$ es **par** si se puede escribir como un producto de un número par de trasposiciones; en otro caso, α es **impar**.

No sabemos, por el momento, si existen permutaciones impares; no podemos decir que es cuando hay una factorización en un número impar de trasposiciones, puesto que tal vez exista otra factorización como un producto de un número par de trasposiciones. La definición de permutación impar α, después de todo, dice que no existe factorización de α en un número par de trasposiciones.

Lema 4.1 *Si* $k, l \geq 0$, *entonces*

$$(a\ b)(a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l) = (a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_l)$$

y

$$(a\ b)(a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_l) = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l)$$

Prueba. El lado izquierdo envía $a \mapsto c_1 \mapsto c_1$; $c_i \mapsto c_{i+1} \mapsto c_{i+1}$ si $i < k$; $c_k \mapsto b \mapsto a$; $b \mapsto d_1 \mapsto d_1$; $d_j \mapsto d_{j+1} \mapsto d_{j+1}$ si $j < l$; $d_l \mapsto a \mapsto b$. Similar evaluación en el lado derecho muestra que ambas permutaciones son iguales. Para la segunda ecuación, sólo multiplique ambos lados de la primera ecuación por $(a\ b)$ a la izquierda. ■

Definición 7 Si $\alpha \in S_n$ y $\alpha = \beta_1 \ldots \beta_t$ es una factorización completa en ciclos disjuntos, el **signo** de α se define por

$$\mathsf{sgn}(\alpha) = (-1)^{n-t}.$$

De acuerdo al teorema 3.2 sgn esta bien definido. Si τ es una trasposición, entonces mueve dos números, digamos, i y j, y fija cada uno de los otros $n-2$ números; por lo tanto, $t = (n-2)+1 = n-1$, y se sigue

$$\mathrm{sgn}(\tau) = (-1)^{n-(n-1)} = -1$$

Lema 4.2 *Si* $\beta \in S_n$ *y* τ *es una trasposición, entonces*

$$sgn(\tau\beta) = -sgn(\beta).$$

Prueba. Sea $\tau = (a\ b)$ y sea $\beta = \gamma_1 \cdots \gamma_t$ una factorización completa de β en ciclos disjuntos (existe un 1-ciclo por cada i fijado por β, y cada número entre 1 y n ocurre en un único γ). Si a y b ocurren en el mismo γ, digamos en γ_1, entonces $\gamma_1 = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l)$, donde $k \geq 0$ y $l \geq 0$. Por el lema 4.1,

$$\tau\gamma_1 = (a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_l),$$

y así $\tau\beta = (\tau\gamma_1)\gamma_2 \cdots \gamma_t$ es una factorización completa con un ciclo extra ($\tau\gamma_1$ se divide en dos ciclos disjuntos).
Por lo tanto, $\mathrm{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\mathrm{sgn}(\beta)$.
La otra posibilidad es que a y b aparezcan en diferentes ciclos, digamos, $\gamma_1 = (a\ c_1\ \ldots\ c_k)$ y $\gamma_2 = (b\ d_1\ \ldots\ d_l)$ donde $k \geq 0$ y $l \geq 0$. Pero ahora $\tau\beta = (\tau\gamma_1\gamma_2)\gamma_3 \cdots \gamma_t$, y el lema 4.1 nos da

$$\tau\gamma_1\gamma_2 = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l).$$

Por lo tanto, la factorización completa de $\tau\beta$ tiene un ciclo menos de los que tiene β, y entonces $\mathrm{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\mathrm{sgn}(\beta)$. ■

Teorema 4.2 Para todo $\alpha, \beta \in S_n$,

$$\mathsf{sgn}(\alpha\beta) = \mathsf{sgn}(\alpha)\mathsf{sgn}(\beta).$$

Prueba. Supongamos que $\alpha \in S_n$ es dado y que $\alpha = \tau_1 \dots \tau_m$ es una factorización de α en trasposiciones con m minimal. Probaremos, por inducción sobre m, que $\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$ par cualquier $\beta \in S_n$. El paso básico es precisamente el lema 4.2. Si $m > 1$, entonces la factorización $\tau_2 \dots \tau_m$ es también minimal: si $\tau_2 \dots \tau_m = \sigma_1 \dots \sigma_q$ con cada σ_j una trasposición y $q < m-1$, entonces la factorización $\alpha = \tau_1\sigma_1 \dots \sigma_q$ viola la minimalidad de m. Por lo tanto,

$$\begin{aligned}
\mathrm{sgn}(\alpha\beta) &= \mathrm{sgn}(\tau_1 \dots \tau_m\beta) = -\mathrm{sgn}(\tau_2 \dots \tau_m\beta) && \text{lema 4.2} \\
&= -\mathrm{sgn}(\tau_2 \dots \tau_m)\mathrm{sgn}(\beta) && \text{Por hipótesis} \\
&= \mathrm{sgn}(\tau_1 \dots \tau_m)\mathrm{sgn}(\beta) && \text{Por el lema 4.2} \\
&= \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).
\end{aligned}$$

■

Teorema 4.3

(i) Una permutación $\alpha \in S_n$ es par si y sólo si $\mathsf{sgn}(\alpha) = 1$.

(ii) Una permutación es impar si y sólo si es producto de un número impar de trasposiciones.

Prueba. (i) Hemos visto que $\mathrm{sgn}(\tau) = -1$ para cualquier trasposición τ. Por lo tanto, si $\alpha = \tau_1 \dots \tau_q$ es una factorización de α en trasposiciones, entonces el teorema 4.2 nos da $\mathrm{sgn} = \mathrm{sgn}(\tau_1) \dots \mathrm{sgn}(\tau_q) = (-1)^q$. Así, $\mathrm{sgn}(\alpha) = 1$ si y sólo si q es par. Si α es par, entonces existe una factorización con q par, y así $\mathrm{sgn}(\alpha) = 1$. Recíprocamente, si $1 = \mathrm{sgn}(\alpha) = (-1)^q$, entonces q es par y por lo tanto α es par.

(ii) Si α es impar, entonces no existe factorización en un número par de trasposiciones, y de esta manera debe ser producto de un número impar de ellos. Recíprocamente, si $\alpha = \tau_1 \dots \tau_q$ con q impar, entonces $\mathrm{sgn}(\alpha) = (-1)^q = -1$, α no es par, y por lo tanto es impar. ■

Ejercicios 4.4 1.19 Muestre que un r-ciclo es una permutación par si y sólo si r es impar.

1. Calcule $\mathrm{sgn}(\alpha)$ para $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$.

1.20 Muestre que S_n tiene el mismo número de permutaciones pares como de permutaciones impares.(*Sugerencia*: Si $\tau = (1\ 2)$, considere la función $f : S_n \to S_n$ definida por $f(\alpha) = \tau\alpha$.)

1.21 Sean $\alpha, \beta \in S_n$. Si α y β tienen la misma paridad, entonces $\alpha\beta$ es par; si α y β tienen paridad distinta, entonces $\alpha\beta$ es impar.

5. Paridad (otra perspectiva)

Para S_n, sea $f = \prod_{1\leq i<j\leq n}(x_i - x_j)$ y para $\sigma \in S_n$ definimos $\sigma^*(f)$ así

$$\sigma^*(f) = \prod_{1\leq i<j\leq n}(x_{\sigma(i)} - x_{\sigma(j)})$$

Entonces el polinomio $\sigma^*(f)$ tiene los mismos factores de f, salvo el signo; si $\sigma(i) < \sigma(j)$, entonces $(x_{\sigma(i)} - x_{\sigma(j)})$ es un factor de f y si $\sigma(i) > \sigma(j)$ entonces $-(x_{\sigma(i)} - x_{\sigma(j)}) = (x_{\sigma(j)} - x_{\sigma(i)})$ es un factor de f.

Es fácil verificar que si $\sigma, \tau \in S_n$ entonces $(\sigma\tau)^*(f) = \sigma^*(\tau^*(f))$.

Definición 8 Una permutación $\sigma \in S_n$ se dice par si $\sigma^*(f) = f$.

Procederemos a probar que toda trasposición es impar (no es par); para eso definimos inversión.

Definición 9 Una inversión es una trasposición tal que sus componentes son números consecutivos, es decir, es de la forma $(i\ i+1)$ para $1 \leq i < n$

Tenemos el siguiente resultado

Lema 5.1 *Si τ es una inversión, entonces τ es impar.*

Prueba. Supongamos que $\tau = (k\ k+1)$, entonces el único factor que cambia de signo es $(x_k - x_{k+1})$. Veremos porque es así

$$f = \Big(\prod_{i<j}^{i,j\notin\{k,k+1\}}(x_i - x_j)\Big)\Big(\prod_{i<k}(x_i - x_k)(x_i - x_{k+1}\Big)(x_k - x_{k+1})$$
$$\Big(\prod_{k+1<j}(x_k - x_j)(x_{k+1} - x_j)\Big)$$

Veremos como actúa τ sobre cada grupo de factores observando que si $f = gh$ entonces $\tau^*(f) = \tau^*(g)\tau^*(h)$.
Tenemos entonces

$$\tau^*\Big(\prod_{i<j}^{i,j\notin\{k,k+1\}}(x_i - x_j)\Big) = \Big(\prod_{i<j}^{i,j\notin\{k,k+1\}}(x_i - x_j)\Big)$$

$$\tau^*\Big(\prod_{i<k}(x_i - x_k)(x_i - x_{k+1}\Big) = \Big(\prod_{i<k}(x_i - x_k)(x_i - x_{k+1}\Big)$$

$$\tau^*((x_k - x_{k+1})) = (x_{k+1} - x_k) = -(x_k - x_{k+1})$$

$$\tau^*\Big(\prod_{k+1<j}(x_k - x_j)(x_{k+1} - x_j)\Big) = \Big(\prod_{k+1<j}(x_k - x_j)(x_{k+1} - x_j)\Big)$$

De este modo se tiene que $\tau^*(f) = -f$ para cualquier inversión τ.

Procedemos a probar el siguiente lema que afirma que cualquier trasposición es producto de un número impar de inversiones.

Lema 5.2 *Sea* $(k,\ t)$ *una trasposición tal que* $n \geq t > k+1 \geq 1$, *y sea* $j \geq 1$ *tal que* $t = k + j$ *entonces*

$$(k,\ k+j) = \Big(\prod_{r=1}^{j-1}(k+j+1-r,\ k+j-r)\Big)(k,\ k+1)\Big(\prod_{r=1}^{j-1}(k+r+1,\ k+r)\Big)$$

Prueba. Haremos una prueba por inducción sobre $2 \leq j \leq n-k$. Si $j = 2$ se tiene que

$$\begin{aligned}&\Big(\prod_{r=1}^{1}(k+3-r,\ k+2-r)\Big)(k,\ k+1)\Big(\prod_{r=1}^{1}(k+r+1,\ k+r)\Big) = \\ &= (k+2,\ k+1)(k,\ k+1)(k+2,\ k+1) = (k,\ k+2)\end{aligned}$$

Supongamos que la ecuación vale para $j < n-k$, entonces desarrollamos la ecuación para $j+1$. Trabajamos con la expresión

$$\prod_{r=1}^{j}(k+j+2-r,\ k+j+1-r)$$

Hacemos un cambio de variable $s = r-1$ y separamos el primer término

$$\begin{aligned}&\prod_{r=1}^{j}(k+j+2-r,\ k+j+1-r) = \\ &= \prod_{s=0}^{j-1}(k+j+2-(s+1),\ k+j+1-(s+1)) = \prod_{s=0}^{j-1}(k+j+1-s,\ k+j-s) \\ &= (k+j+1,\ k+j)\prod_{s=1}^{j-1}(k+j+1-s,\ k+j-s) \\ &= (k+j+1,\ k+j)\prod_{r=1}^{j-1}(k+j+1-r,\ k+j-r)\end{aligned}$$

Aplicamos esta identidad en la siguiente expresión

$$\Big(\prod_{r=1}^{j}(k+j+2-r,\ k+j+1-r)\Big)(k,\ k+1)\Big(\prod_{r=1}^{j}(k+r+1,\ k+r)\Big) =$$
$$= (k+j+1,\ k+j)\Big(\prod_{r=1}^{j-1}(k+j+1-r,\ k+j-r)\Big)(k,\ k+1)$$
$$\Big(\prod_{r=1}^{j-1}(k+r+1,\ k+r)\Big)(k+j+1,\ k+j)$$

Por hipótesis inductiva se tiene

$$\Big(\prod_{r=1}^{j-1}(k+j+1-r,\ k+j-r)\Big)(k,\ k+1)\Big(\prod_{r=1}^{j-1}(k+r+1,\ k+r)\Big) = (k,\ k+j)$$

Luego, sustituyendo esta ecuación en la expresión anterior se tiene

$$\Big(\prod_{r=1}^{j}(k+j+2-r,\ k+j+1-r)\Big)(k,\ k+1)\Big(\prod_{r=1}^{j}(k+r+1,\ k+r)\Big) =$$
$$= (k+j+1,\ k+j)(k,\ k+j)(k+j+1,\ k+j) = (k,\ k+j+1)$$

Esto culmina la prueba.

De este modo tenemos que cualquier trasposición es producto de un número impar de inversiones. Tenemos el siguiente resultado

Teorema 5.1 Las trasposiciones son permutaciones impares

6. Ejercicios

1. Sea $\phi = (a_1\ \cdots\ a_r)$, un ciclo de longitud r en S_n y sea $\psi \in S_n$ una permutación cualquiera, entonces $\psi\phi\psi^{-1} = (\psi(a_1), \ldots, \psi(a_n))$
2. Las permutaciones (1 2) y (1 2 3 $\cdots$ n) generan a S_n
3. Si p es primo y ϕ es un p-ciclo, entonces para todo $1 \leq k < p$ se tiene que ϕ^k es un p ciclo.
4. Si p es primo entonces cualquier trasposición y p-ciclo de S_p genera a S_p.
5. El producto de dos trasposiciones es un 3-ciclo o producto de dos 3-ciclos.
6. Para $n \geq 3$ el grupo A_n es generado por los 3-ciclos.
7. Demuestre que todo elemento de A_n es un producto de ciclos de orden n

8. A_n para $n \geq 3$ es generado por ciclos de la forma

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

9. Si $N \lhd\ A_n$ y N contiene un 3-ciclo, entonces $N = A_n$

10. Sea $n \geq 5$ y $(e) \neq H \lhd\ A_n$, entonces H tiene un ciclo de longitud 3.

Solución.

1. Supongamos que $\psi(k) \notin \{\psi(a_1), \ldots, \psi(a_n))$, entonces $(\psi\phi\psi^{-1})(\psi(k)) = \psi(k)$.
   Si $\psi(k) = \psi(a_i)$ con $1 \leq i < r$, entonces $(\psi\phi\psi^{-1})(\psi(a_i) = \psi(a_{i+1})$, y $(\psi\phi\psi^{-1})(\psi(n)) = \psi(1)$

2. Por lo anterior, siendo $\phi = (1\ 2)$ y $\psi = ((1\ 2\ 3 \cdots\ n)$ se tiene que $\psi^k\phi\psi^{-k} = (\psi^k(1)\ \psi^k(2))$, y esto es $(k\ k+1)$ si $1 \leq k < r$ y $(1\ n)$ si $k = n$. Tenemos que las trasposiciones $(1\ 2)$, $(2\ 3)$, $(3\ 4), \ldots, (n\ (n-1)$, $(1\ n)$ son generadas. Además $(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$ y de este modo $(1\ 3)$, es generada; procedemos por inducción, observando que $(1\ k)(k\ k{+}1)(1\ k) = (1\ k+1)$; de este modo se tiene que todas las trasposiciones $(1,\ k)$ son generadas. Puesto que $(1\ r)(1\ k)(1\ r) = (r\ k)$ tenemos que todas las trasposiciones son generadas y como toda permutación es producto de trasposiciones tenemos que es generado S_n.

3. Veremos inicialmente que si ψ es un n-ciclo, entonces para todo k tal que $(n, k) = 1$ se tiene que ψ^k es un n-ciclo. Si $\psi = (i_1\ i_2\ i_3 \cdots i_n)$ debemos probar que $\psi^{rk}(i_1)$ debe recorrer todos los valores i_s con $s = 1, 2, \ldots, n$, es decir, para todo $s \in [n]$ existe $r \in [n]$ tal que $\psi^{rk}(i_1) = i_s$; sabemos que $\psi^{rk}(i_1) = i_{[1+rk]}$ donde $[1 + rk]$ es el resto módulo n; en consecuencia debemos probar que la ecuación $kx+1 \equiv s(n)$ tiene solución para todo $s \in [n]$. Puesto que $(k, n) = 1$ se tiene que existen t, m tales que $mk + tn = 1$, entonces $s{-}1 = km(s{-}1){+}nt(s{-}1)$ y en consecuencia $km(s{-}1) \equiv s{-}1(n)$. Quedo demostrado.

   En particular, si p es primo se tiene $(k, p) = 1$ para todo $1 \leq k < p$, y por lo previo ψ^k es un p-ciclo siempre que ψ sea un p-ciclo.

4. Sea $\psi = (r\ t)$ una trasposición y $\phi = (i_1\ i_2\ \cdots i_p)$ un p-ciclo, como estamos en S_p el p ciclo contiene todos los números en $[p]$, por lo tanto, podemos suponer, sin perder generalidad, que $i_1 = r$. Entonces $\psi = (i_1\ i_s)$ para algún $1 \leq s \leq p$; puesto que p es primo tenemos que ϕ^{s-1} es un p-ciclo y tiene la forma $\phi^{s-1} = (\imath_1\ i_s\ \cdots)$ de manera que renombrando las variables tenemos el p-ciclo $\sigma = (j_1\ j_2\ j_3\ \cdots j_p)$ y la trasposición $\psi = (j_1\ j_2)$. Aplicamos $\sigma^{k-1}\psi(\sigma^{k-1})^{-1} = (j_k\ j_{k+1})$ para $1 \leq k < p$ y generamos todos las trasposiciones que tienen la forma $(j_k\ j_{k+1})$. Por último generamos todas las trasposiciones posibles de esta manera: sea

$(u\ v)$ una trasposición, entonces existen $1 \leq r < s \leq p$ tales que $(u\ v) = (i_s\ i_r)$, sea n tal que $s = r + n$. Procedemos por inducción: puesto que

$$(i_r\ i_{r+1})(i_{r+1}\ i_{r+2})(i_r\ i_{r+1}) = (i_r\ i_{r+2})$$

tenemos la base inductiva. Supongamos que hemos generado la trasposición $(i_r\ i_{r+k})$, entonces

$$(i_{r+k}\ i_{r+k+1})(i_r\ i_{r+k})(i_{r+k}\ i_{r+k+1}) = (i_r\ i_{r+k+1})$$

Luego es posible generar $(i_r\ i_s)$ para todo $1 \leq r < s \leq p$ y estas son todas las posibles trasposiciones y por lo tanto se genera S_p.

5. El producto de dos trasposiciones disjuntas $(a\ b)(c\ d)$ es

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

Si el producto es de la forma $(a\ b)(a\ c)$ entonces

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

La identidad se puede expresar $(a\ b\ c)(a\ c\ b)$

6. Según la prueba anterior todo elemento de A_n es un 3-ciclo o producto de 3-ciclos, pues todo elemento de A_n tiene una descomposición en un número par de trasposiciones. Recíprocamente todo 3-ciclo se encuentra en A_n pues $(a\ b\ c) = (a\ c)(a\ b)$.

7. Basta notar que el producto entre $\phi = (i_1\ i_2\ i_3\ i_4 \cdots\ i_n)$ y la permutación σ que se obtiene de ϕ invirtiendo el orden de los elementos del tercer lugar en adelante, es decir, $\sigma = (i_1\ i_2\ i_n\ i_{n-1} \cdots\ \imath_4\ i_3)$ resulta $(i_1\ i_3\ i_2)$. Formalmente σ se define así:

$$\sigma(i_k) = \begin{cases} i_2, & \text{si} \quad k = 1 \\ i_n, & \text{si} \quad k = 2 \\ i_1, & \text{si} \quad k = 3 \\ i_{k-1}, & \text{si} \quad 4 \leq k \leq n \end{cases}$$

De este modo el producto de dos n-ciclos adecuados generan un 3-ciclo determinado y por lo tanto todo A_n.

8. Basta probar que todo 3-ciclo $(a\ b\ c)$ es generado por los dados o sus inversos (observe que $(1\ 2\ k)^{-1} = (1\ 2\ k)^2$).

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

La validez de la ecuación previa nos da el resultado esperado. Los cálculos se facilitan usando el resultado del ejercicio 1.

9. Sea $(a\ b\ c) \in N$ entonces la normalidad de N sobre A_n garantiza

$$\sigma(a\ b\ c)\sigma^{-1} \in N$$

para toda $\sigma \in A_n$ Veremos varios casos:

Primer caso. $(a\ b\ c) = (1\ 2\ c)$, si $n = 4$ podemos suponer que $c = 3$ luego $(1,2,3)^{-1} \in N$ y así $(1\ 3\ 2) \in N$ y por la normalidad se tiene $(3\ 4)(1\ 3)(1\ 3\ 2)((3\ 4)(1\ 3))^{-1} = (1\ 2\ 4) \in N$ y así tenemos que $(1\ 2\ 3), (1\ 2\ 4) \in N$.

Si $n > 4$ elegimos $k, r \notin \{1, 2, c\}$ y se verifica

$$(c\ r\ k)(1\ 2\ c)(c\ r\ k)^{-1} = (1\ 2\ r)$$

y

$$(c\ k\ r)(1\ 2\ c)(c\ k\ r)^{-1} = (1\ 2\ k)$$

y se cumple $(1\ 2\ k) \in N$ para todo $k \notin \{1, 2\}$

Segundo caso. $(a\ b\ c) = (2\ 1\ c)$, entonces $(2\ 1\ c)^{-1} = (1\ 2\ c) \in N$ y estamos en el caso anterior.

Tercer caso. Supongamos que $(a\ b\ c) = (1\ b\ c)$ con $b, c \notin \{2\}$, se tiene que $(1\ c\ b) \in N$ y

$$(b\ 2)(c\ 2)(1\ b\ c)((c\ 2)(b\ 2))^{-1} = (1\ 2\ c) \in N$$

$$(c\ 2)(b\ 2)(1\ c\ b)((b\ 2)(c\ 2))^{-1} = (1\ 2\ b) \in N$$

Para $k \notin \{1, 2, b, c\}$

$$(b\ 2)(c\ k)(1\ b\ c)((c\ k)(b\ 2))^{-1} = (1\ 2\ k) \in N$$

Cuarto caso. Si $(a\ b\ c) = (2\ b\ c)$ con $b, c \notin \{1\}$ entonces

$$(1\ c)(1\ b)(2\ b\ c)((1\ c)(1\ b))^{-1} = (1\ 2\ c) \in N$$

Siendo $(2\ c\ b) \in N$ se tiene

$$(1\ b)(1\ c)(2\ c\ b)((1\ b)(1\ c))^{-1} = (1\ 2\ b) \in N$$

Sea $k \notin \{1, 2, b, c\}$ entonces

$$(1\ c)(b\ k)(2\ b\ c)((1\ c)(b\ k))^{-1} = (1\ 2\ k) \in N$$

Quinto caso. Sea $(a\ b\ c)$ con $a, b, c \notin \{1, 2\}$ tenemos

$$(2\ b)(1\ a)(a\ b\ c)((2\ b)(1\ a))^{-1} = (1\ 2\ c) \in N$$

$$(2\ a)(1\ c)(a\ b\ c)((2\ a)(1\ c))^{-1} = (1\ 2\ b) \in N$$
$$(2\ c)(1\ b)(a\ b\ c)((2\ c)(1\ b))^{-1} = (1\ 2\ a) \in N$$

Si $n > 5$ sea $k \notin \{1, 2, a, b, c\}$ y $r \notin \{1, 2, c, k\}$, entonces

$$(c\ k)(r\ k)(1\ 2\ c)((c\ k)(r\ k))^{-1} = (1\ 2\ k) \in N$$

Hemos probado que si N es subgrupo normal de A_n que contiene un 3-ciclo $(a\ b\ c)$ entonces contiene todos los 3-ciclos $(1\ 2\ k)$ para todo $k \in [n] \setminus \{1, 2\}$ y por el problema anterior se tiene que N contiene todos los 3-ciclos y por el problema 4 es todo A_n

10. Sea $e \neq \theta \in H$ y $\theta = \theta_1\theta_2 \cdots \theta_k$ una descomposición de θ en ciclos y sea θ_1 uno de los ciclos de mayor longitud (esto es siempre posible porque ciclos disjuntos conmutan). Veremos tres casos: que el ciclo tenga longitud mayor que 3, que tenga longitud igual a 3, y que todos tengan longitud 2.

Supongamos que $\theta_1 = (i_1\ i_2\ \cdots\ i_n)$ con $n > 3$, entonces

$$\theta_1^{-1}(i_1\ i_2\ i_3)\theta_1(i_1\ i_2\ i_3)^{-1} = \theta_1^{-1}(i_2\ i_3\ i_1\ i_4\ i_5 \cdots i_n)$$

es fácil verificar que $\theta_1^{-1}(i_2\ i_3\ i_1\ i_4\ i_5 \cdots i_n) = (i_1\ i_3\ i_n)$. En consecuencia, por ser H un subgrupo normal de A_n, se tiene que

$$\theta^{-1}(i_1\ i_2\ i_3)\theta(i_1\ i_2\ i_3)^{-1} \in H$$

Ahora

$$\theta^{-1}(i_1\ i_2\ i_3)\theta(i_1\ i_2\ i_3)^{-1} = \theta_1^{-1}(i_1\ i_2\ i_3)\theta_1(i_1\ i_2\ i_3)^{-1}$$

Esto se debe a que $\theta^{-1} = \theta_1^{-1}\theta_2^{-1} \cdots \theta_n^{-1}$ por ser $\theta_i\theta_j = \theta_j\theta_i$ y por ser

$$(i_1\ i_2\ i_3)\theta(i_1\ i_2\ i_3)^{-1} = (i_1\ i_2\ i_3)\theta_1(i_1\ i_2\ i_3)^{-1}\theta_2 \cdots \theta_n$$

ya que $(i_1\ i_2\ i_3)\theta_j = \theta_j(i_1\ i_2\ i_3)$ para $2 \leq j \leq n$. De este modo se tiene que $(i_1\ i_2\ i_n) \in H$

El caso en que el ciclo de mayor longitud es mayor que 3 esta demostrado. Veremos a continuación el caso en el que el ciclo de mayor longitud es 3.

Supongamos que $\theta_1 = (i_1\ i_2\ i_3)$. Si hay al menos otro de longitud 3 entonces

$$\theta = (i_1\ i_2\ i_3)(i_4\ i_5\ i_6)\theta_3 \cdots \theta_k$$

Por ser H subgrupo normal de A_n, se tiene que

$$(i_1\ i_2\ i_4)\theta(i_1\ i_4\ i_2)\theta^{-1} \in H$$

Desarrollando la expresión

$$\begin{aligned}&(i_1\ i_2\ i_4)\theta(i_1\ i_4\ i_2)\theta^{-1} = \\ &= (i_1\ i_2\ i_4)(i_1\ i_2\ i_3)(i_4\ i_5\ i_6)(i_1\ i_4\ i_2)(i_1\ i_3\ i_2)(i_4\ i_6\ i_5) = \\ &= (i_1\ i_2\ i_5\ i_3\ i_4) \in H\end{aligned}$$

De nuevo

$$(i_1\ i_5\ i_4)(i_1\ i_2\ i_5\ i_3\ i_4)(i_1\ i_4\ i_5) = (i_1\ i_5\ i_2\ i_4\ i_3) \in H$$

Por último

$$(i_1\ i_2\ i_5\ i_3\ i_4)(i_1\ i_5\ i_2\ i_4\ i_3) = (i_1\ i_3\ i_2) \in H$$

Así H tiene un 3-ciclo.

Si la descomposición en ciclos disjuntos tiene exactamente un 3-ciclo hay dos posibilidades: no hay más ciclos y se cumple trivialmente que H tiene un 3-ciclo, o existe al menos un 2-ciclo; en este caso sea

$$\theta = (i_1\ i_2\ i_3)(i_4\ i_5)\theta_3 \cdots \theta_k$$

donde los θ_i son 2-ciclos, entonces, por ser los ciclos disjuntos y por ser $\theta_i^2 = identidad$ se tiene

$$\begin{aligned}(i_1\ i_2\ i_4)\theta(i_1\ i_4\ i_2)\theta &= (i_1\ i_2\ i_4)(i_1\ i_2\ i_3)(i_4\ i_5)(i_1\ i_4\ i_2)(i_1\ i_2\ i_3)(i_4\ i_5)\\ &= (i_1\ i_4)(i_3\ i_5) \in H\end{aligned}$$

De la normalidad de H sobre A_n se tiene

$$(i_1\ i_4\ i_3)(i_1\ i_4)(i_3\ i_5)(i_1\ i_3\ i_4) = (i_1\ i_5)(i_3\ i_4) \in H$$

y

$$(i_1\ i_2\ i_3)(i_1\ i_4)(i_3\ i_5)(i_1\ i_3\ i_2) = (i_1\ i_5)(i_2\ i_4) \in H$$

Luego

$$(i_1\ i_5)(i_3\ i_4)(i_1\ i_5)(i_2\ i_4) = (i_2\ i_3\ i_4) \in H$$

Este caso esta demostrado.

Veamos el caso en que la descomposición en ciclos disjuntos contenga solo trasposiciones; por ser una permutación par debe tener un número par de trasposiciones. Supongamos que $\theta = (i\ j)(k\ l)\theta_3\theta_4 \cdots \theta_k$ donde el producto es de trasposiciones disjuntas. Veremos inicialmente que, si $H \lhd A_n$ y $\theta \in H$, entonces existe una permutación $\sigma \in H$ que tiene exactamente dos trasposiciones disjuntas. Puesto que $(i\ j\ k) \in A_n$, tenemos que

$$\theta(i\ j\ k)\theta(i\ j\ k)^{-1} \in H$$

Así, por ser ciclos disjuntos ninguno de los θ_i contienen a los elementos $\{i, j, k, l\}$ y por lo tanto conmutan con los ciclos

$$(i\ j), (k\ l), (i\ j\ k), (i\ j\ k)^{-1}$$

además $(\theta_i)^2 = identidad$. Esto explica la siguiente secuencia

$$\begin{aligned}\theta(i\ j\ k)\theta(i\ j\ k)^{-1} &= (i\ j)(k\ l)\theta_3\theta_4\cdots\theta_k(i\ j\ k)(i\ j)(k\ l)\theta_3\theta_4\cdots\theta_k(i\ j\ k)^{-1}\\ &= (i\ j)(k\ l)(i\ j\ k)(i\ j)(k\ l)(i\ j\ k)^{-1}\\ &= (i\ j)(k\ l)(j\ k)(i\ l) = (i\ k)(j\ l)\end{aligned}$$

Tenemos que $\sigma = (i\ k)(j\ l) \in H$.

Usamos ahora la hipótesis $n \geq 5$ para conseguir un ciclo de mayor longitud en H, existe $r \in [n]$ tal que $r \notin \{i, j, k, l\}$, luego $(i\ r\ l) \in A_n$ y por ser H normal en A_n se tiene que

$$(i\ r\ l)\sigma(i\ r\ l)^{-1} \in H$$

Desarrollamos la expresión

$$(i\ r\ l)\sigma(i\ r\ l)^{-1} = (i\ r\ l)(i\ k)(j\ l)(i\ r\ l)^{-1} = (k\ r)(j\ i)$$

Por ser H subgrupo se tiene $(k\ r)(j\ i)(i\ k)(j\ l) \in H$ y

$$(k\ r)(j\ i)(i\ k)(j\ l) = (i\ r\ k\ j\ l)$$

Usando la normalidad de H sobre A_n se tiene

$$(i\ j\ r)(i\ r\ k\ j\ l)(i\ j\ r)^{-1} = (j\ i\ k\ r\ l) \in H$$

y por ser H subgrupo

$$(i\ r\ k\ j\ l)(j\ i\ k\ r\ l) = (i\ j\ r) \in H$$

Obtenemos de esta manera un 3-ciclo en H.

Referencias

[1] Joshep J. Rotman. An Introduction to the Theory of Groups Graduate Texts in Mathematics. Springer-Verlag. 1994 North-Holland, 1977.

[2] Thomas W. Hungerford. Algebra Graduate Texts in Mathematics. Springer-Verlag. 1974

[3] Thomas W. Hungerford. Abstract Algebra An Introduction Harcourt College Publishers. 1997.

[4] I.N. Herstein. Álgebra Abstracta Grupo Editorial Iberoamericano. 1988.