Grupo simétrico, Teorema de Keeler y El prisionero de Benda

Juliana Cuellar*, Diego F. Díaz†, Helen L. Quevedo‡

Departamento de Matemáticas, Pontificia Universidad Javeriana
*ju.cuellar@javeriana.edu.co, †di-diego@javeriana.edu.co,
‡hlquevedo@javeriana.edu.co

12 de mayo de 2021

Resumen. En el presente artículo se expone, mediante teoremas y ejemplos gráficos, una breve introducción de las propiedades más importantes del grupo simétrico para posteriormente exhibir el problema del intercambio de mentes y su solución mediante el Teorema de Keeler. Adicionalmente, se presentan algoritmos para la descomposición en ciclos disjuntos y el método para deshacer un intercambio.

2020 Mathematics Subject Classifications: 05A05, 20B30, 68Q87.

Palabras clave: grupo simétrico, intercambio de mentes, descomposición cíclica.

Introducción

El origen de los grupos de permutaciones se da por Joseph-Louis Lagrange en el año 1770, mientras estudiaba la solución de ecuaciones por radicales [Kle07]. Sin embargo, no fue sino hasta 1830 cuando Évariste Galois entendió el concepto de grupo como el conjunto de permutaciones de un conjunto finito y realizó avances conceptuales significativos que lo posicionan como el fundador de la teoría de grupos [Kle07]. Catorce años después, el trabajo de Galois fue tomado por el matemático francés Augustin-Louis Cauchy, quien fue el primero en considerar la posibilidad de estructuras grupales más abstractas [Kle07]. Al establecerse la definición abstracta, en 1854 el matemático inglés Arthur Cayley demostró la importancia de los grupos simétricos (una noción más general de los grupos de permutaciones [Gal17]) e identificó que todo grupo se puede pensar como un subgrupo de algún grupo simétrico [Sar08], dando una aproximación al teorema que años después fue nombrado en su honor.

Entre las muchas aplicaciones del grupo simétrico se encuentra una muy curiosa: el problema del intercambio de mentes [PP17]. En el episodio "El prisionero de Benda" de la serie animada *Futurama* se explica el mecanismo de una máquina que intercambia las mentes de dos cuerpos. El problema radica en que una vez se intercambien todas las mentes, se debe buscar la forma de revertir cada intercambio teniendo en cuenta que esta máquina no puede ser usada nuevamente con un mismo par de cuerpos [EHN14]. En el siguiente artículo se explora la solución de Ken Keeler, guionista de la serie y además doctor en Matemáticas Aplicadas de Harvard, que utiliza al grupo simétrico como herramienta. Para este propósito se ha dividido el artículo en dos secciones: en la sección 1 se presentan algunas propiedades importantes y ejemplos del grupo simétrico que serán útiles más adelante para la aplicación (aquí se asumirá que el lector está familiarizado con teoría grupos y con el grupo simétrico). Luego, en la sección 2 se presenta la solución que proporciona el Teorema de Keeler junto con algunos ejemplos, y se finaliza mostrando el algoritmo que deshace un intercambio de mentes.

1. Grupo simétrico: propiedades y ejemplos

En esta sección se realiza una breve revisión de los conceptos básicos de la descomposición cíclica de una permutación. A lo largo de este trabajo se utilizará la siguiente notación: S_n denotará el grupo simétrico en n letras, para las permutaciones se utilizará la notación por lista y para todo $n \in \mathbb{N}$, $[n] = \{1, 2, \ldots, n\}$. En primer lugar, se muestra que toda permutación puede expresarse en términos de ciclos disjuntos como se presenta en [Gal17]:

Teorema 1.1. *Cada permutación de un conjunto finito puede ser escrita como un ciclo o como un producto de ciclos disjuntos.*

Demostración. Sea $\alpha \in S_n$. Para escribir a α como producto de ciclos disjuntos, vamos a empezar escogiendo cualquier miembro de $[n]$, en particular a_1, y sea

$$a_2 = \alpha(a_1), \quad a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1)$$

y así sucesivamente hasta que lleguemos a $\alpha^m(a_1)$ para algún m. Note que sabemos de la existencia de m puesto que la sucesión $a_1, \alpha(a_1), \alpha^2(a_1), \ldots$ debe ser finita; así, eventualmente debe haber una repetición la cual llamaremos $\alpha^i(a_1) = \alpha^j(a_1)$ para algún i y j con $i < j$. Entonces $a_1 = \alpha^m(a_1)$, con $m = j - i$ y expresamos la relación entre $a_1, a_2, \ldots, a_m$ como:

$$\alpha = (a_1 \ a_2 \ \ldots \ a_{m-1}) \ldots$$

Los puntos suspensivos al final indican la posibilidad de que no hayamos agotado el conjunto $[n]$ en el proceso; en tal caso, elegimos un $b \in [n]$ que no aparezca en el primer ciclo y procedemos a crear un nuevo ciclo como antes; esto es, $b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1)$ hasta obtener $\alpha^k(b_1)$ para algún k. Este nuevo ciclo no debe tener elementos en común con el ciclo construido anteriormente, por lo que si $\alpha^i(a_1) = \alpha^j(b_1)$ para algún i y j, entonces $\alpha^{i-j}(a_1) = b_1$ y $b_1 = a_1$ lo cual es una contradicción. Continuando con este proceso para cada elemento de $[n]$ obtenemos la permutación:

$$\alpha = (a_1 \ a_2 \ \ldots \ a_{m-1})(b_1 \ b_2 \ \ldots \ b_{k-1}) \ldots (c_1 \ c_2 \ \ldots \ c_{s-1}),$$

por lo tanto, toda permutación puede ser escrita como producto de ciclos disjuntos. □

Ejemplo 1.2. *Considere la permutación $\sigma = [4,2,5,6,3,1] \in S_6$. Con el Teorema 1.1 su descomposición en ciclos disjuntos es $\sigma = (1 \ 4 \ 6)(2)(3 \ 5)$.*

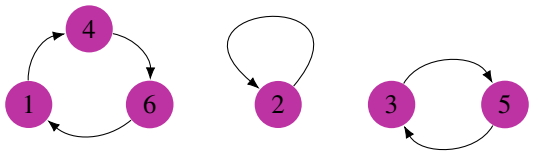

Figura 1: Descomposición en ciclos disjuntos de σ.

El siguiente teorema establece que los ciclos disjuntos conmutan, su demostración puede consultarse en [Gal17] y [Loe14].

Teorema 1.3. *Si el par de ciclos α y β son disjuntos, entonces se cumple que $\alpha\beta = \beta\alpha$.*

El concepto de transposición será necesario a lo largo del artículo, ya que con este se modela el intercambio de las mentes de dos cuerpos. A continuación, se presenta una definición detallada por Grillet en [Gri07].

Definición 1.4. *Sean $a, b \in [n]$ con $a \neq b$. Decimos que una permutación $\tau \in S_n$ es una **transposición** si $\tau(a) = b$, $\tau(b) = a$ y para todo $x \neq a, b$ se tiene $\tau(x) = x$.*

Ejemplo 1.5. *La permutación $\tau = [2,1,3,4] \in S_4$ es una transposición. Más aún, su descomposición en ciclos es $\tau = (1 \ 2)$. Al descomponer en ciclos disjuntos una transposición $\tau \in S_n$ obtenemos un 2-ciclo.*

Continuando con la descomposición cíclica, el siguiente corolario muestra la forma de descomponer una permutación como producto de transposiciones [Gal17].

Corolario 1.6. *Toda permutación $\sigma \in S_n$ con $n > 1$, es producto de 2-ciclos (transposiciones).*

Demostración. Primero, note que la identidad puede expresarse como $I = (1\ 2)(2\ 1)$, y por lo tanto es producto de *2-ciclos*. Por el Teorema 1.1 tenemos que toda permutación se puede escribir como:

$$(a_1\ a_2\ \cdots\ a_k)(b_1\ b_2\ \cdots\ b_t)\cdots(c_1\ c_2\ \cdots\ c_s).$$

Calculando directamente llegamos a que es lo mismo que:

$$(a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2)(b_1\ b_t)(b_1\ b_{t-1})\cdots(b_1\ b_2)\cdots(c_1\ c_s)(c_1\ c_{s-1})\cdots(c_1\ c_2),$$

lo que completa la prueba. □

Ejemplo 1.7. *Considere la permutación $\pi = [2,3,4,1,5] \in S_5$. Su descomposición en ciclos disjuntos es $\pi = (1\ 2\ 3\ 4)$ y al usar el Corolario 1.6 podemos expresar a π de la forma $\pi = (1\ 4)(1\ 3)(1\ 2) = (3\ 2)(3\ 1)(3\ 4)$. De la última igualdad se concluye que la descomposición en transposiciones de una permutación no es única.*

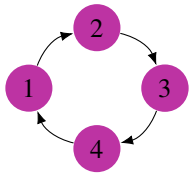

Figura 2: Descomposición en ciclos disjuntos de π.

Con base en el Corolario 1.6, se define la paridad de una permutación de acuerdo a [Sar08] como sigue:

Definición 1.8. *Una permutación es **par** si puede ser escrita como el producto de un número par de transposiciones y es **impar** si puede ser escrita como el producto de un número impar de transposiciones.*

El siguiente teorema muestra que, si bien el número de transposiciones en la descomposición de una permutación puede variar, su paridad se mantiene (la demostración puede consultarse en [Sar08] y [Gal17]).

Teorema 1.9. *Una permutación no puede ser par e impar al mismo tiempo.*

Ejemplo 1.10. *Considere la permutación $\lambda = [1,3,5,4,2,8,7,6] \in S_8$. Su descomposición disjunta es $\lambda = (2\ 3\ 5)(6\ 8)$. Usando el Corolario 1.6 descomponemos en 2-ciclos como sigue: $\lambda = (2\ 5)(2\ 3)(6\ 8)$. Por lo tanto λ es impar.*

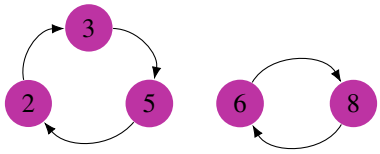

Figura 3: Descomposición en ciclos disjuntos de λ.

2. Teorema y algoritmo de Keeler

El problema de Keeler consiste en una máquina que intercambia las mentes de dos cuerpos. Esta máquina no puede ser usada nuevamente para revertir el cambio, por lo que la cuestión es, ¿cuántos cuerpos más serán necesarios para devolver cada mente a su respectivo cuerpo? En esta sección se explora la solución que proporciona el Teorema de Keeler y se presentan algoritmos para la descomposición en ciclos disjuntos y el método para deshacer un intercambio.

El intercambio de mentes puede traducirse en términos del grupo simétrico; los cuerpos serán representados como elementos de $[n]$. A su vez, un intercambio de dos mentes se puede ver como una transposición; por ejemplo, la transposición $\tau = (\alpha\ \beta)$ es la permutación que intercambia la mente de los cuerpos α y β, mientras que el k-ciclo $(a_1\ \ldots\ a_k)$ es la permutación que lleva la mente de $a_1 \mapsto a_2$, la de $a_2 \mapsto a_3$, …, y la de $a_k \mapsto a_1$ [EHN14]. Como se tiene la restricción que la máquina no funciona dos veces en el mismo par de cuerpos, cada transposición en S_n debe ser distinta [PP17]. Sea $P \neq I$ un producto de transposiciones distintas en S_n, esto representa el intercambio sucesivo de mentes [PP17]. En el Ejemplo 1.7, 1 cambia la mente con 2, 3 y 4, en ese orden respectivamente. Así, este intercambio sucesivo es $P = (1\ 4)(1\ 3)(1\ 2)$ lo que resulta en $P = (1\ 2\ 3\ 4)$.

Problema. *Para devolver todas las mentes a sus respectivos cuerpos, debemos encontrar una permutación σ que sea producto de transposiciones distintas tal que $\sigma P = I$ y tal que las transposiciones en σ sean distintas a aquellas de P. Bajo estas condiciones decimos que σ* ***deshace*** *P [EHN14].*

Como se verá más adelante, lo que propone el Teorema de Keeler es considerar a σ en S_{n+2}. Cada factor de la permutación σ tendrá al menos un elemento del conjunto $\{n+1, n+2\}$, de esta forma cada transposición será distinta a aquellas de P. Los elementos $n+1$ y $n+2$ pueden pensarse como dos cuerpos más que no hicieron parte del intercambio inicial P que ahora entrarán a la máquina en repetidas ocasiones para actuar como *almacenamiento*. Por simplicidad $\alpha := n+1$ y $\beta := n+2$. Por el Teorema 1.1 P se puede descomponer de forma única como $P = D_1 D_2 \cdots D_k$, donde $D_1, D_2, \ldots, D_k$ son todos ciclos disjuntos. Además, se asume que $l_1 + l_2 + \cdots + l_k = n$, donde l_i denota la longitud del ciclo D_i. Cabe resaltar que en caso que $l_1 + l_2 + \cdots + l_k = m < n$, se renombran los cuerpos y se trabaja en S_m; por ejemplo, el intercambio $(1\ 5\ 8)(7\ 6) \in S_8$ se renombra como $(1\ 5\ 3)(4\ 2) \in S_5$, cumpliendo de esta manera la suposición anterior.

Ahora se enuncia y demuestra el Teorema de Keeler de acuerdo a [EHN14]. Refinamientos a este teorema han sido trabajados por Huang et al. en [EHN14], quienes reducen el número de transposiciones requeridas. Patrama y Prakasa atacan el problema desde las ciencias de la computación en [PP17].

Teorema 2.1 (Teorema de Keeler)**.** *Sea $P = D_1 D_2 \cdots D_k$ una permutación en S_n, con $D_1, D_2, \ldots, D_k$ ciclos disjuntos tales que $l_1 + l_2 + \cdots + l_k = n$. Entonces existe $\sigma \in S_{n+2}$ que* ***deshace*** *P.*

Demostración. Si $D_i = (d_1\ \ldots\ d_{l_i})$ para algún $i \in \{1, 2, \ldots, k\}$, considere la permutación σ_i en S_{n+2} dada por:

$$\sigma_i = (\alpha\ d_1)(\alpha\ d_2)\cdots(\alpha\ d_{l_i-1})(\beta\ d_{l_i})(\alpha\ d_{l_i})(\beta\ d_1).$$

Calculando directamente se llega a que $\sigma_i D_i = (\alpha\ \beta)$. Como $\alpha, \beta \notin [n]$, por el Teorema 1.3 $(\alpha\ \beta)$ conmuta con toda transposición en S_n.

Con base en la construcción anterior se define $\tau := \sigma_k \cdots \sigma_2 \sigma_1$. Note que τ es un producto de transposiciones distintas y además:

$$\tau P = \sigma_k \cdots \sigma_2 \sigma_1 D_1 D_2 \cdots D_k = \sigma_k \cdots \sigma_2 (\alpha\ \beta) D_2 \cdots D_k = \sigma_k \cdots \sigma_3 (\alpha\ \beta)^2 D_3 \cdots D_k = \cdots = (\alpha\ \beta)^k.$$

Ahora veamos que $\sigma P = I$, donde σ se define como sigue:

$$\sigma = \begin{cases} (\alpha\ \beta)\tau & \text{Si } k \text{ es impar} \\ \tau & \text{Si } k \text{ es par} \end{cases}.$$

Si k es par, entonces $\sigma P = \tau P = (\alpha\ \beta)^k = I$. Ahora, si k es impar se tiene que $\sigma P = (\alpha\ \beta)\tau P = (\alpha\ \beta)(\alpha\ \beta)^k = (\alpha\ \beta)^{k+1} = I$. Luego σ ***deshace*** a P. □

Ejemplo 2.2. *Sea $P = (1\ 7\ 2)(3\ 5)(4\ 6) \in S_7$. Por el Teorema 2.1 se elige $\sigma_1 = (8\ 1)(8\ 7)(9\ 2)(8\ 2)(9\ 1)$, $\sigma_2 = (8\ 3)(9\ 5)(8\ 5)(9\ 3)$ y $\sigma_3 = (8\ 4)(9\ 6)(8\ 6)(9\ 4)$. Como P se descompone en tres ciclos disjuntos, tomaremos $\sigma = (8\ 9)\tau$. Vea que $\sigma P = (8\ 9)\tau P = (8\ 9)\sigma_3\sigma_2\sigma_1 P = (8\ 9)(8\ 9)^3 = (8\ 9)^4 = I$.*

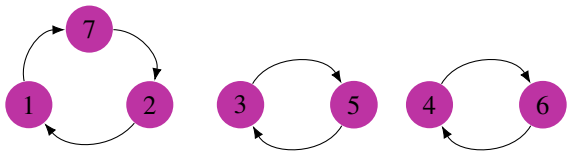

Figura 4: Intercambio de mentes P.

Ejemplo 2.3. *Sea $\Gamma = (1\ 4\ 3)(2\ 5) \in S_5$. Siguiendo el Teorema 2.1 se elige $\sigma_1 = (6\ 1)(6\ 4)(7\ 3)(6\ 3)(7\ 1)$ y $\sigma_2 = (6\ 2)(7\ 5)(6\ 5)(7\ 2)$. Como solo hay dos ciclos disjuntos $\sigma = \tau$. Por último, vea que $\sigma\Gamma = \tau\Gamma = \sigma_2\sigma_1(1\ 4\ 3)(2\ 5) = (6\ 7)^2 = I$.*

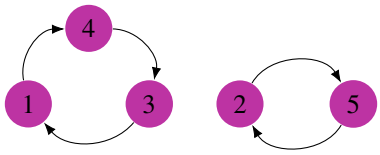

Figura 5: Intercambio de mentes Γ.

El Teorema 1.1 incluye un algoritmo para descomponer en ciclos disjuntos una permutación. De igual forma, el Teorema 2.1 proporciona un método para deshacer un intercambio de mentes. A continuación, se presentan los algoritmos para estos dos teoremas y un ejemplo de su implementación en Python (ver código en https://github.com/ddiaz1999/Algebra_abstracta). Para un trabajo futuro se pueden implementar métodos más eficientes como en [EHN14].

Algoritmo 1: Descomposición disjunta

Datos: Lista $\alpha \in S_n$
inicio
  $actual, x \leftarrow a \in [n]$
  $ciclos \leftarrow [\,]$
  $ciclo \leftarrow [\,]$
  $ciclo \leftarrow ciclo + a$
  si $\alpha(x) \neq actual$ **entonces**
    $ciclo \leftarrow ciclo + \alpha(x)$
    $x \leftarrow \alpha(x)$
    Volver al paso 6
  fin
  en otro caso
    $ciclos \leftarrow ciclos + ciclo$
    $ciclo \leftarrow [\,]$
    si $\exists\, b \in [n]$ *t.q* $b \notin$ *ningún camino anterior* **entonces**
      $ciclo \leftarrow ciclo + b$
      $actual, x \leftarrow b$
      Volver al paso 6
    fin
    en otro caso
      devolver *ciclos*
    fin
  fin
fin

Algoritmo 2: Método de Keeler

Datos: Lista $P \in S_n$
inicio
  $S \leftarrow disjuntos(P)$
  $(k, \alpha, \beta, X) \leftarrow (|S|, n+1, n+2, [\,])$
  para $i = 1$*:* k **hacer**
    $\sigma_i \leftarrow [\,]$
    para $j = 1$*:* $|S[i]| - 1$ **hacer**
      $\sigma_i \leftarrow \sigma_i + [\alpha, S[i][j]]$
    fin
    $\sigma_i \leftarrow \sigma_i + [\alpha, S[i][-1]] + [\alpha, S[i][-1]] + [\alpha, S[i][0]]$
    $X \leftarrow X + \sigma_i$
  fin
  $\tau \leftarrow I$
  para $\sigma_j \in reversed.(X)$ **hacer**
    $\tau \leftarrow \tau \cdot \sigma_j$
  fin
  si $k\,\%2 == 0$ **entonces**
    $\sigma \leftarrow \tau$
  fin
  en otro caso
    $\sigma \leftarrow (\alpha\ \ \beta)\tau$
  fin
  devolver σ
fin

Figura 6: Descomposición en ciclos disjuntos y método de Keeler para deshacer un intercambio.

Ejemplo 2.4. *Sea* $\Phi = [13,18,10,15,19,6,4,14,1,12,9,2,5,20,11,7,17,8,16,3] \in S_{20}$. *Con la implementación del Algoritmo 1 se obtiene la descomposición disjunta:* $\Phi = (13\ 5\ 19\ 16\ 7\ 4\ 15\ 11\ 9\ 1)(18\ 8\ 14\ 20\ 3\ 10\ 12\ 2)$. *Al aplicar el Algoritmo 2 obtenemos* $\sigma = (1\ 9\ 11\ 15\ 4\ 7\ 16\ 19\ 5\ 13)(2\ 12\ 10\ 3\ 20\ 14\ 8\ 18)$ *y se verifica que* $\sigma \cdot \Phi = I$.

Referencias

[EHN14] Ron Evans, Lihua Huang, and Tuan Nguyen. Keeler's theorem and products of distinct transpositions. *Amer. Math. Monthly*, 121(2):136–144, 2014.

[Gal17] Joseph A. Gallian. *Contemporary abstract algebra*. Cengage Learning, ninth edition edition, 2017.

[Gri07] Pierre Antoine Grillet. *Abstract Algebra (Graduate Texts in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2007.

[Kle07] I. Kleiner. *A History of Abstract Algebra*. Birkhäuser Boston, 2007.

[Loe14] N. Loehr. *Advanced Linear Algebra*. Textbooks in Mathematics. Taylor & Francis, 2014.

[PP17] Yohanssen Pratama and Yohenry Prakasa. A survey on keeler's theorem and application of symmetric group for swapping game. *Journal of Physics: Conference Series*, 795:012048, jan 2017.

[Sar08] D. Saracino. *Abstract Algebra: A First Course*. Waveland Press, 2008.