Semana 9: Permutaciones

1. Definiciones

Definición 9.1. Sea A un conjunto cualquiera. Por *una permutación sobre* A entenderemos una función biyectiva $\alpha: A \to A$. Al conjunto de las permutaciones sobre el conjunto A lo denotaremos por S_A y si $A = \{1, 2, ..., n\}$, escribiremos S_n .

En esta sección el término permutación se referirá a los elementos de un conjunto S_n y muchas ocasiones no aclaremos esta referencia en contexto. La importancia de estudiar sólo permutaciones sobre un conjunto finitos es que existen exactamente n! permutaciones de un conjunto con n elementos. Es además común interpretar las permutaciones como un listado de los elementos de un conjunto, por ejemplo si $A = \{1, \ldots, n\}$, una permutación $\alpha: A \to A$ genera una lista de los elementos de A indicada como $i_1 = \alpha(1), \ldots, i_{n-1} = \alpha(n-1)$ y $i_n = \alpha(n)$. En esta lista aparecen todos los elementos de A y ninguno está repetido por eso, se acostumbra escribir una permutación en notación de dos filas:

$$\alpha = \begin{pmatrix} 1 & \dots & j & \dots & n \\ \alpha(1) & \dots & \alpha(j) & \dots & \alpha(n) \end{pmatrix}.$$

Una ventaja de esta notación, es que la composición de permutaciones se puede realizar de modo visual, eliminando un poco el nivel de abstracción con el que comúnmente se discuten las funciones. Es importante también notar que la composición no es conmutativa, lo cual es fácil de probar usando la notación de dos filas: Sean

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mathbf{y} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

en ese caso

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

pero

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

lo que nos permite concluir que $\alpha \circ \beta \neq \beta \circ \alpha$ y con esto hemos entonces construido un ejemplo profundamente interesante de lo que constituye una operación no conmutativa.

Ejemplo. El conjunto S₃ debe tener 6 elementos, a decir, está constituido por las permutaciones

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

La primera de éstas, representa a la función identidad y en este caso, la denotaremos como e. Además, podemos simplificar mucho la descripción de este conjunto eligiendo, por ejemplo,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \mathbf{y} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

las cuales son permutaciones que satisfacen

$$\alpha^2 = \beta^3 = e$$
.

Una simple comprobación (hazla), nos permite expresar el conjunto S_3 como

$$S_3 = \left\{e, \, \alpha, \, \beta, \, \alpha\beta, \, \beta\alpha, \, \alpha\beta\alpha \mid \alpha^2 = \beta^3 = e\right\}.$$

Proposición 9.1. La composición en el conjunto de permutaciones satisface las leyes de cancelación por izquierda y por la derecha, i.e., si $\gamma \circ \alpha = \gamma \circ \beta$ o $\alpha \circ \gamma = \beta \circ \gamma$ entonces $\alpha = \beta$.

Demostración. Vamos a probar sólo una de las leyes. Supongamos que A es un conjunto y que α , β y γ son permutaciones sobre A que satisfacen

$$\gamma \circ \alpha = \gamma \circ \beta$$
.

Entonces, como las permutaciones son funciones biyectivas, tienen inversa, en particular tomaremos la inversa γ^{-1} lo cual muestra que

$$\alpha = 1_A \circ \alpha$$

$$= (\gamma^{-1} \circ \gamma) \circ \alpha$$

$$= \gamma^{-1} \circ (\gamma \circ \alpha)$$

$$= \gamma^{-1} \circ (\gamma \circ \beta)$$

$$= (\gamma \circ \gamma^{-1}) \circ \beta$$

$$= 1_A \circ \beta$$

$$= \beta.$$

Lo que muestra la ley de cancelación izquierda. La otra ley se prueba de manera similar.

Proposición 9.2. *Para permutaciones* α γ β , *se cumple*

$$(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}.$$

En general, si $\alpha_1, \alpha_2, \ldots, \alpha_n$ son permutaciones, entonces

$$(\alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_n)^{-1} = \alpha_n^{-1} \circ \alpha_{n-1}^{-1} \circ \cdots \circ \alpha_1^{-1}.$$

Demostración. La primera parte es el ejercicio 9.2. La segunda sigue por inducción de la primera y se resuelve en el ejercicio 9.3. ■

Definición 9.2. Sea α una permutación. Para un entero positivo n, definimos la permutación

$$\alpha^n = \underbrace{\alpha \circ \cdots \circ \alpha}_{n \text{ veces}}.$$

Además,

$$\alpha^{-n} = \left(\alpha^{-1}\right)^n.$$

Comentario. En general, no utilizaremos el símbolo \circ para denotar la composición. Simplemente escribiremos $\alpha\beta$ para indicar el resultado de la composición $\alpha \circ \beta$. Esto nos permitirá simplificar muchos de los resultados, entre ellos la siguiente proposición.

Proposición 9.3. Sean α y β permutaciones y sean enteros m y n. Entonces, si $\alpha\beta = \beta\alpha$, se tiene también

$$(\alpha\beta)^n = \alpha^n\beta^n$$
.

Demostración. Usaremos inducción para probar un resultado parcial. Primero, asumimos que α y β conmutan, en ese caso $(\alpha\beta)^1 = \alpha^1b^1$; supongamos ahora que $(\alpha\beta)^n = \alpha^n\beta^n$, entonces

$$(\alpha\beta)^{n+1} = (\alpha\beta)^n (\alpha\beta)$$
$$= \alpha^n \beta^n \alpha\beta$$
$$= (\alpha^n \alpha)(\beta^n \beta)$$
$$= \alpha^{n+1} \beta^{n+1}.$$

Por inducción, se satisface para todo entero no negativo n que $(\alpha \beta)^n = \alpha^n \beta^n$.

Para probar el resultado en los enteros negativos, debemos convencernos que α^{-1} y β^{-1} conmutan también y suponiendo que n es un entero positivo, la conclusión del párrafo anterior resulta en tener

$$(\alpha\beta)^{-n} = ((\alpha\beta)^{-1})^n$$

$$= (\alpha^{-1}\beta^{-1})^n$$

$$= (\alpha^{-1})^n (\beta^{-1})^n$$

$$= \alpha^{-n}\beta^{-n}.$$

El resultado entonces sigue indistintamente para enteros positivos y negativos como buscábamos.

2. Ciclos

Definición 9.3. Una permutación α se dice *fija el número i*, si $\alpha(i) = i$. De manera similar, se dice que *mueve el número i*, si $\alpha(i) \neq i$.

Definición 9.4. Una permutación se dice un k-ciclo, si existen $i_1, i_2, ..., i_k$ enteros positivos todos distintos entre sí de forma que

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \cdots, \alpha(i_{k-1}) = i_k, \quad \alpha(i_k) = i_1$$

y fija al resto de los enteros positivos. A una permutación con esta propiedad también se le denomina *un ciclo de longitud k*.

En general, será mucho más útil expresar a los ciclos de una manera mucho más breve que la notación a doble fila utilizando la siguiente convención. Si α es un k-ciclo de forma que $\alpha(i_j)=i_{j+1}$ para $1\leq i\leq k-1$ y $\alpha(i_k)=i_1$ escribiremos

$$\alpha = (i_1 \ i_2 \ \dots \ i_k).$$

Comentario. Debemos observar que un 1-ciclo es simplemente la identidad y eso quiere decir que (i) = (1) para cada para cada i. Por otro lado, un 2-ciclo simplemente mueve dos valores, fijando todos los demás. Un 2-ciclo es frecuentemente llamado *una transposición*. Como consecuencia de esto, en las transposiciones sólo interesan dos valores lo cual hace muy conveniente la representación de ciclos. Una transposición, entonces, tiene siempre la forma $(i \ j)$.

Ejemplo. En S_5 , por el 3-ciclo definido como $(2\,5\,4)$ nos referimos a la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}.$$

De manera similar, el 4-ciclo definido por (1 3 2 4), es la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

Debemos notar, sin embargo, en S₆, la permutación

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

no es un ciclo. En realidad es la composición de varios pues

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} = (14)(23)(56)$$

Definición 9.5. Dos permutaciones α y β se dicen *disjuntas* si cada i mueve una, lo fija la otra, i.e., si $\alpha(i) \neq i$, entonces $\beta(i) = i$, y si $\beta(i) \neq i$, entonces $\alpha(i) = i$.

Proposición 9.4. Las permutaciones disjuntas conmutan bajo la composición.

Demostración. Sean α y β permutaciones disjuntas. Debemos probar que $\alpha\beta=\beta\alpha$ y para conseguir esto debemos observar que a cada i le corresponde sólo una de tres posibilidades: α mueve i o β mueve i o ni α ni β mueven i. Comencemos suponiendo que α mueve i, digamos $\alpha(i)=j$ con $i\neq j$, entonces α también mueve j pues en caso contrario, $\alpha(j)=j$ lo cual haría que α no fuera una función inyectiva. Como α mueve i y j entonces β fija i y j por lo que

$$\alpha\beta(i) = \alpha(i) = j = \beta(j) = \beta\alpha(i).$$

Si ahora β fija i, podemos proceder de modo similar. Finalmente, si ni α ni β mueven i, entonces

$$\alpha\beta(i) = i = \beta\alpha(i).$$

Proposición 9.5. Para un ciclo $(i_1, i_2, ..., i_k)$ su inverso es el ciclo $(i_k, i_{k-1}, ..., i_1)$.

Demostración. Supongamos que $\alpha \in S_n$ y tomemos $\beta = (i_k, i_{k-1}, \ldots, i_1)$. Basta entonces mostrar que las composiciones posibles son resultan en (1). Debemos observar que cualquier número i diferente a los valores i_1, i_2, \ldots, i_k es fijado tanto por α como por β , i.e.,

$$\alpha\beta(i) = i = \beta\alpha(i).$$

Además, $\beta(i_1) = i_k$ y en consecuencia

$$\alpha\beta(i_1) = \alpha(i_k) = i_1$$

y para cualquier i_j con $j \ge 2$ tenemos que $\beta(i_j) = i_{j-1}$ y en consecuencia

$$\alpha\beta(i_j) = \alpha(i_{j-1}) = i_j.$$

Lo anterior es suficiente para garantizar que $\alpha\beta=(1)$ y bajo un argumento similar es posible también concluir que $\beta\alpha=(1)$. El resultado sigue de esto.

Proposición 9.6. Cada permutación es o un ciclo o una composición de ciclos disjuntos.

Demostración. Tomemos primero una permutación α sobre n elementos. Realizaremos la prueba por inducción sobre el número r de elementos que mueve α . Si r=0, entonces α no mueve ningunún elemento y en consecuencia es la identidad la cual es un 1-ciclo. Supongamos ahora que r>0 y que el resultado es válido para cualquier número menor que r. En ese caso α mueve algún elemento, digamos i_1 , por lo que podemos definir el conjunto $S = \{i_1, i_2, \dots\}$ donde $\alpha(i_i) = i_{i+1}$. Como cada i_i satisface $1 \le i_i \le n$, entonces el conjunto S contiene al menos un elemento repetido. Tomemos i_{k+1} como el primer elemento repetido en la secuencia, i.e., k+1 es el menor entero positivo tal que $i_{k+1} = i_j$ para algún $j \le k$; luego $\alpha(i_k) = i_{k+1} = i_j$. Si j > 1, como α es inyectiva y $\alpha(i_k) = \alpha(i_{j-1})$ entonces $i_k = i_{j-1}$ lo cual contradice que i_{k+1} es el menor elemento repetido en la secuencia. Podemos entonces concluir que $\alpha(i_k) = i_1$. Esto quiere decir que podemos expresar el conjunto S como aquel formado por los elementos $i_1, i_2, ..., i_k$ todos distintos entre sí, y además tomar el k-ciclo: $\beta = (i_1, i_2, \dots, i_k)$. Si k = n, entonces α coincide con el ciclo β y el resultado sigue. Si por otro lado k < n, entonces debemos notar que el conjunto $T = \{1 \le j \le n \mid j \notin S\}$ debe satisfacer $\alpha[T] = T$ pues T es simplemente el complemento de S (ejercicio 9.4). Definimos entonces $\gamma = \alpha \beta^{-1}$ observando que γ y β son disjuntos. En efecto, si β mueve i, entonces $i = i_i \in S$ y en consecuencia

$$\gamma(i_j) = \alpha \beta^{-1}(i_j) = i_j$$

mostrando que γ fija i y de manera similar, si γ mueve i, entonces debemos de concluir que $i \notin S$ pues de otra manera γ lo fijaría, si este es el caso, entonces $\beta(i) = i$ por ser éste un ciclo. Esto indica que $\alpha = \gamma \beta$ es una factorización que involucra permutaciones disjuntas. Además, γ mueve r - k < r puntos y por tanto, por hipótesis de inducción, se puede factorizar en ciclos disjuntos. Luego, α se puede factorizar también en ciclos disjuntos y el resultado sigue.

La prueba de la proposición es más trascendetal de lo que parece pues nos entrega un proceso mecánico de como expresar una permutación en ciclos disjuntos. El proceso no es difícil, primero debemos tomar $i_1 = \alpha(1)$ y encontrar la secuencia de números $i_1, i_2, ..., i_k$ de números todos distintos de forma que $\alpha(i_k) = i_1$. Utilizamos éstos para formar un ciclo. Para formar el siguiente

ciclo, tomamos el menor elemento que no aparece en la anterior secuencia (o en todas las anteriores en los pasos sucesivos) y repetimos el proceso hasta que no quede ningún número en ninguno de los ciclos formados. Al final terminaremos con ciclos disjuntos cuya composición es simplemente la permutación α .

Ejemplo. Consideremos la permutación en S₇ dada por

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

Siguiendo el proceso anterior, tomamos primero $i_1=1$ y observamos que α no mueve i_1 por lo que el ciclo es simplemente (1). El menor número que no aparece es 2, tomamos entonces $i_1=2$, obteniendo en consecuencia $i_2=7$ y de ahí la secuencia se repite. Esto quiere decir que el siguiente ciclo simplemente (2, 7). El siguiente número que no aparece en los ciclos anteriores es 3, tomamos entonces $i_1=3$ y observamos que α no mueve a i_1 por lo que el ciclo es simplemente (3). El siguiente número que no aparece en ningún ciclo es 4 por lo que tomando $i_1=4$, obtenemos $i_2=5$ e $i_3=6$ notando que la secuencia se repite después de este punto. Esto indica que el último ciclo es (4 5 6). Como todos los números aparecen ya en alguno de los ciclos que hemos descrito, podemos entonces asegurar que

$$\alpha = (1)(27)(3)(456).$$

Ejemplo anterior, sugiere que un tipo especial de descomposición en ciclos disjuntos es admitido por cada permutación, vamos a definir cual es éste.

Definición 9.6. *Una factorización completa de una permutación* α es una expresión en ciclos disjuntos en la que cada elemento i aparece en uno y sólo uno de los ciclos.

El algoritmo que hemos descrito, obtiene una factorización completa de una permutación. Debemos observar, primero, que la proposición 9.6 garantiza la existencia de al menos una factorización completa y segundo, que los elementos de una factorización completa conmutan uno con otro al ser ciclos disjuntos. Debemos entonces preguntarnos si dichas expresiones no serán únicas salvo el orden en que se presenten. Vamos a concluir que esto es cierto y el teorema 9.9 es un análogo al teorema fundamental de la aritmética, de hecho, la prueba de la unicidad es muy similar.

Comentario. Existe una estrecha relación entre un k-ciclo y sus potencias. Si escribimos, para conseguir que este comentario tenga alguna utilidad, $\beta = (i_0 \ i_1 \ \dots \ i_{k-1})$, entonces $i_1 = \beta(i_0)$, $i_2 = \beta(i_1) = \beta^2(i_0)$, etc. Esto permite observar que, para $j \le k-1$, tenemos

$$i_i = \beta^j(i_0).$$

En general, para un entero $0 \le j \le k$ podemos afirmar que $j \equiv r \mod k$ si y sólo si

$$i_i = \beta^r(i_0).$$

Lema 9.7. Sea $\alpha = \beta \gamma$ donde β y γ son permutaciones disjuntas. Si β mueve i entonces $\alpha^k(i) = \beta^k(i)$ para toda $k \ge 1$.

Demostración. Como β y γ son disjuntas, entonces γ fija i y consecuencia cualquier potencia de γ fija i de igual manera. En ese caso, como son permutaciones disjuntos, entonces conmutan por lo que $\alpha^k = (\beta \gamma)^k = \beta^k \gamma^k$ y de esta forma

$$\alpha^k(i) = \beta^k \gamma^k(i) = \beta^k(i).$$

Lema 9.8. Si β y γ son ciclos de forma que ambos mueven un elemento i_0 y además $\beta^k(i_0) = \gamma^k(i_0)$ para todo $k \ge 1$, entonces $\beta = \gamma$.

Demostración. Supongamos que la longitud de β es r y la longitud de γ es s. Bajo estas consideraciones, podemos escribir $\beta=(i_0\ i_1\dots i_r)$ y $\gamma=(i_0\ j_1\dots j_s)$ esto nos permite escribir $i_k=\beta^k(i_0)$ y de manera similar $j_k=\gamma^k(i_0)$. Sin perdida de la generalidad, podemos asumir que $r\leq s$ y por la hipótesis del lema, podemos garantiza que $i_1=j_1,\ i_2=j_2,\ \dots,\ i_{r-1}=j_{r-1}$ y como $j_r=\gamma^r(i_0)=\beta^r(i_0)=i_0$. Lo anterior indica que la longitud de γ coincide con la de β y que además $i_k=j_k$ para todo k. Esto es simplemente una forma de expresar que $\beta=\gamma$.

Teorema 9.9. Cada permutación admite una factorización completa y esta factorización es única salvo el orden en que se presenten los ciclos.

Demostración. Supongamos que $\alpha = \beta_1 \dots \beta_r = \gamma_1 \dots \gamma_s$ son dos factorizaciones completas. Como los 1-ciclos son la identidad, asumiremos que las expresiones anteriores contienen ciclos de longitud mayor o igual que 2. Supongamos ahora que β_r mueve un elemento i, entonces alguno de los ciclos γ_t también mueve i. En ese caso, según el lema 9.7, tenemos, para toda k

$$\beta_r^k(i) = \alpha^k(i) = \gamma_t^k(i)$$

lo cual indica, según el lema 9.8 que $\beta_r = \gamma_t$. Por ley de cancelación, esto indica simplemente que

$$\beta_1 \dots \beta_{r-1} = \gamma_1 \dots \gamma_{t-1} \gamma_{t+1} \dots \gamma_s$$
.

Debemos observar que podemos repetir este proceso hasta cancelar todos las permutaciones de uno u otro lado de la igualdad. Esto haría imposible tener $r \neq s$ pues si lo fuera, obtendríamos que al menos uno de los ciclos sería (1), según el ejercicio 9.9); pero eso sería contradictorio pues hemos removido todos los ciclos de longitud 1. De esta forma, se tiene r = s y en consecuencia para cada $1 \leq j \leq r$, existe $1 \leq t \leq s$ de forma que $\beta_j = \gamma_t$ lo cual indica que las mismas permutaciones están involucradas en las permutaciones que planteamos.

Ejercicios

Ejercicio 9.1. Encuentra las factorizaciones completas de las siguientes permutaciones en S₇

(a)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 7 & 5 & 4 & 6 \end{pmatrix}$$
 (c)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 6 & 5 & 4 & 7 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

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

Ejercicio 9.2. Para permutaciones α y β , demuestra que $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

Ejercicio 9.3. Para permutaciones $\alpha_1, \alpha_2, \dots, \alpha_n$ son permutaciones, entonces

$$(\alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_n)^{-1} = \alpha_n^{-1} \circ \alpha_{n-1}^{-1} \circ \cdots \circ \alpha_1^{-1}.$$

- *Ejercicio* 9.4. Sea α una permutación y sea i_1 un elemento que mueve α . Si definimos $S = \{i_j \mid j \leq 1\}$ tomando $i_{j+1} = \alpha(i_j)$ muestra que $\alpha[S] = S$. Además, si $T = \{i \mid i \notin S\}$ muestra que $\alpha[T] = T$.
- *Ejercicio* 9.5. Si α es un k-ciclo, demuestra que $\alpha^k = (1)$.
- *Ejercicio* 9.6. Si α es un k-ciclo, demuestra que k es entero más pequeño de forma que $\alpha^k = (1)$.
- *Ejercicio* 9.7. Encuentra dos permutaciones α y β de forma que $(\alpha\beta)^2 \neq \alpha^2\beta^2$.
- *Ejercicio* 9.8. Muestra que una permutación α mueve un elemento i si y sólo si α^{-1} .
- *Ejercicio* 9.9. Muestra que si α y β son permutaciones disjuntas de forma que $\alpha\beta=(1)$, entonces $\alpha=(1)$ o $\beta=(1)$.

Referencias

[Gri97] Grimaldi, Ralph P.: *Matemáticas discreta y combinatoria*. Addison Wesley Iberoamericana, 3ª edición, 1997.

[Rot05] Rotman, Joseph J.: A first course in abstract algebra. Pearson, 3^a edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.