Capítulo 6

Grupos de permutaciones

En el capítulo anterior se probó que cada grupo G es isomorfo a un subgrupo del grupo de permutaciones $S(G)$. Cuando $G = \{x_1, \ldots, x_n\}$ es finito, el grupo de permutaciones se acostumbra a denotar S_n. En este caso los elementos $x_1, \ldots, x_n$ pueden ser reemplazados por los naturales $1, \ldots, n$. Así pues, S_n es el grupo de todas las funciones biyectivas del conjunto $I_n := \{1, 2, \ldots, n\}$.

En este capítulo estudiaremos con algún detalle al grupo S_n, denominado ***grupo simétrico de grado*** n. Destacamos en S_n algunos subgrupos importantes: el grupo alternante A_n y el grupo dihédrico de grado n, D_n.

6.1. Ciclos

Definición 6.1.1. *Sea f un elemento de S_n. Se dice que f es un* ***ciclo de longitud*** *m, $(1 \leq m \leq n)$, si existen $a_1, a_2, \ldots, a_m$ elementos diferentes de I_n tales que*

1. $f(a_1) = a_2, f(a_2) = a_3, \ldots, f(a_{m-1}) = a_m, f(a_m) = a_1,$
2. $f(x) = x$ *para* $x \notin \{a_1, \ldots, a_m\}$.

Se denota a f por

$$f = (a_1 a_2 \cdots a_m) = (a_2 a_3 \cdots a_m a_1) = (a_3 a_4 \cdots a_m a_1 a_2) = \cdots = (a_m a_1 a_2 \cdots a_{m-1})$$

Nótese que un ciclo de longitud 1 es la idéntica de I_n.

Sean $f = (a_1 \ldots a_m)$ y $g = (b_1 \ldots b_r)$ dos ciclos de S_n. Se dice que f y g son dos ***ciclos disyuntos*** si $\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, br\} = \emptyset$. Nótese que las siguientes permutaciones f y g de S_7 son ciclos disyuntos:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 \end{pmatrix} = (123)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 7 & 4 & 6 \end{pmatrix} = (4576)$$

Proposición 6.1.2. *En S_n el producto de ciclos disjuntos conmuta.*

Demostración. Sean $f = (a_1 \cdots a_m)$ y $g = (b_1 \cdots b_r)$ dos ciclos disyuntos de S_n. Sean $A := \{a_1, \ldots, a_m\}$ y $B := \{b_1, \ldots, b_r\}$. Sean $A_1 := I_n - A$ y $B_1 := I_n - B$. Dado $x \in I_n$ existen tres posibilidades

(i) $x \in A$: entonces $f(x) \in A, f(x) \notin B \Rightarrow g(f(x)) = f(x)$; $g(x) = x \Rightarrow f(g(x)) = f(x) \Rightarrow fg(x) = gf(x)$.

(ii) $x \in B$: es análogo al anterior.

(iii) $x \notin A$ y $x \notin B \Rightarrow f(x) = x, g(x) = x \Rightarrow fg(x) = x = gf(x)$.

De (i), (ii) y (iii) se desprende que $fg = gf$. □

La importancia de la anterior proposición se pone de manifiesto en el siguiente teorema.

Teorema 6.1.3. (i) *Sea $f = (a_1 \cdots a_m)$ un ciclo de longitud m de S_n. Entonces*

$$|f| = m.$$

(ii) *Sea $f = f_1 \cdots f_t$ una permutación de S_n, donde $f_1, \ldots, f_t$ son ciclos disyuntos de longitudes $m_1, \ldots, m_t$, respectivamente. Entonces*

$$|f| = m.c.m.(m_1, \ldots, m_t)$$

Demostración. (i) Probemos en primer lugar que $f^m = 1$: si $x \notin \{a_1, \ldots, a_m\} \Rightarrow f(x) = x \Rightarrow f^m(x) = x$. Sea $a_j \in \{a_1, \ldots, a_m\}, 1 \leq j \leq m$, f se puede expresar también como $f = (a_j a_{j+1} \cdots a_m a_1 a_2 \cdots a_{j-1}) \Rightarrow f(a_j) = a_{j+1} \Rightarrow f^2(a_j) = a_{j+2} \Rightarrow \cdots \Rightarrow f^{m-1}(a_j) = a_{j-1} \Rightarrow f^m(a_j) = a_j$; es decir, f^m actua también como la idéntica sobre los elementos de $\{a_1, \ldots, a_m\}$.

El orden de f es el menor entero positivo k tal que $f^k = 1$. Supóngase que existe $1 \leq k < m$ tal que $f^k = 1$. Por lo tanto, $f(a_1) = a_2, f^2(a_1) = a_3, \ldots, f^{k-1}(a_1) = a_k, f^k(a_1) = a_1 = f(a_k) = a_{k+1}$, pero esto es una contradicción ya que los elementos del ciclo f son diferentes. Lo anterior prueba que $|f| = m$.

(ii) La demostración se efectua por inducción sobre t.

$t = 1$: la afirmación es consecuencia de (i).

$t = 2$: $f = f_1 f_2$, donde f_1 y f_2 son ciclos disyuntos de longitudes m_1 y m_2 respectivamente. Según la proposición 6.1.2, $f_1 f_2 = f_2 f_1$. Además, $\langle f_1 \rangle \cap \langle f_2 \rangle = 1$. En efecto, sea $g \neq 1$ tal que $g = f_1^s = f_2^r$ con $1 \leq s < m_1$ y $1 \leq r < m_2$. Sea $f_1 = (a_1 \cdots a_m)$. Puesto que $g \neq 1$ existe $x \in I_n$ tal que $g(x) \neq x$. Necesariamente $x \in \{a_1, \ldots, a_m\}$. Sea pues $x = a_j \Rightarrow f_1^s(a_j) \neq a_j$ pero $f_2^r(a_j) = a_j$, contradicción.

Así pues, $\langle f_1 \rangle \cap \langle f_2 \rangle = 1$, $f_1 f_2 = f_2 f_1 \Rightarrow |f_1 f_2| = m.c.m.(m_1, m_2)$.

Supongamos que la afirmación es cierta para t: sea $f = f_1 f_2 \cdots f_t f_{t+1}$, donde $f_1, f_2, \ldots, f_t, f_{t+1}$ son ciclos disyuntos dos a dos y de longitudes $m_1, m_2, \ldots, m_{t+1}$, respectivamente. Sea $f' := f_1 f_2 \cdots f_t$. Entonces, $f = f' f_{t+1}$. Nótese que $\langle f' \rangle \cap \langle f_{t+1} \rangle = 1$. Además, $f' f_{t+1} = f_{t+1} f'$; entonces

$$\begin{aligned} |f| = m.c.m.(|f'|, m_{t+1}) &= m.c.m.(m.c.m.(m_1, \ldots, m_t), m_{t+1}) \\ &= m.c.m.(m_1, \ldots, m_{t+1}). \end{aligned}$$

□

Teorema 6.1.4. *Cada permutación f de S_n es representable como producto de ciclos disyuntos dos a dos. Tal representación es única salvo el orden y la inclusión de ciclos de longitud* 1.

Demostración. La existencia se realiza por induccion sobre n.

$n = 1$: S_1 sólo posee un elemento, el cual es un ciclo de longitud 1.

Supóngase que la afirmación es válida para toda permutación de un conjunto de m elementos con $m < n$. Sea $f \in S_n$. Si f es un ciclo entonces no hay nada que probar. Sea f una permutación que no es un ciclo. Esto en particular implica que $f \neq 1$. Existe entonces $a_1 \in I_n$ tal que $f(a_1) \neq a_1$. Cosideremos la sucesión $f(a_1), f^2(a_1), f^3(a_1), \ldots$. En esta sucesión se tiene un número finito de elementos diferentes de I_n debido a que para cada k ≥ 1, $f^k(a_1) \in I_n$ y I_n es finito. Por lo tanto existen r y p enteros positivos diferentes (por ejemplo $r > p$) tales que

$$f^p(a_1) = f^r(a_1), \text{ luego } f^{r-p}(a_1) = a_1.$$

Sea $A := \{r \in \mathbb{N} \mid f^r(a_1) = a_1\}$. Según lo dicho anteriormente, $A \neq \emptyset$. Como $A \subset \mathbb{N}$ y $\mathbb{N}$ es bien ordenado A posee entonces primer elemento k, es decir, k es el menor entero positivo tal que $f^k(a_1) = a_1$. Los elementos $f(a_1), f^2(a_1), \ldots, f^{k-1}(a_1), f^k(a_1) = a_1$ son diferentes, ya que en caso contrario existiría un $s < k$ tal que $f^s(a_1) = a_1$. La permutación f determina así el k-ciclo $g = (a_1 a_2 \cdots a_k)$, donde

$$a_2 = f(a_1), a_3 = f(a_2) = f^2(a_1), \ldots, a_k = f(a_{k-1}) = f^{k-1}(a_1), a_1 = f(a_k) = f^k(a_1).$$

Consideremos la permutación $f_1 \in S_n$ definida por $f_1(a_i) = a_i$, $1 \leq i \leq k$, $f_1(x) = f(x)$, $x \in I_n - \{a_1, \ldots, a_k\}$. Nótese que $f = f_1 g$. En efecto, si $x \in \{a_1, \ldots, a_k\}$ entonces sea $x = a_j$ para algún $1 \leq j \leq k$. Si $j < k$ entonces

$$g(x) = g(a_j) = a_{j+1} \Rightarrow f_1 g(x) = f_1(a_{j+1}) = a_{j+1} = f(a_j) = f(x). \text{ Si } j = k \text{ entonces}$$
$$g(x) = g(a_k) = a_1 \Rightarrow f_1 g(x) = f_1(a_1) = a_1 = f(a_k) = f(x).$$

Ahora, si $x \notin \{a_1, \ldots, a_k\}$ entonces $g(x) = x$, luego $f_1 g(x) = f_1(x) = f(x)$.

Puesto que f_1 fija los elementos $a_1, \ldots, a_k$ entonces f_1 puede considerarse como una permutación del conjunto $I_n - \{a_1, \ldots, a_k\}$. Por la hipótesis de induccion f_1 es producto de ciclos disyuntos conformados por los elementos de $I_n - \{a_1, \ldots, a_k\}$. En

total f es producto de ciclos disyuntos conformados por los elementos de I_n. Esto completa la prueba de la primera afirmación del teorema.

Probemos ahora la unicidad de la descomposición: sean

$$\begin{aligned} f &= (a_{11}a_{12}\cdots a_{1k_1})(a_{21}a_{22}\cdots a_{2k_2})\cdots(a_{r1}a_{r2}\cdots a_{rk_r}) \\ &= (b_{11}b_{12}\cdots b_{1m_1})(b_{21}b_{22}\cdots b_{2m_2})\cdots(b_{s1}b_{s2}\cdots b_{sm_s}) \end{aligned}$$

dos descomposiciones de f en producto de ciclos disyuntos. Nótese que $1 \leq r \leq n, 1 \leq s \leq n$. Estamos considerando que los elementos de I_n que permanezcan fijos bajo f conforman ciclos de longitud 1, es decir,

$$1 \leq k_i \leq n, 1 \leq i \leq r;\ 1 \leq m_j \leq n, 1 \leq i \leq s.$$

En otras palabras, estamos considerando que

$$\begin{aligned} I_n &= \{a_{11}, a_{12}, \ldots, a_{1k_1}; \ldots; a_{r1}, a_{r2}, \ldots, a_{rk_r}\} \\ &= \{b_{11}, b_{12}, \ldots, b_{1m_1}; \ldots; b_{s1}, b_{s2}, \ldots, b_{sm_s}\}. \end{aligned}$$

El elemento a_{11} debe aparecer en alguno de los ciclos de la segunda descomposición. Por la conmutatividad de los factores podemos asumir que $a_{11} \in \{b_{11}, b_{12}, \ldots, b_{1m_1}\}$. Reordenando el ciclo $(b_{11}b_{12}\cdots b_{1m_1})$ podemos considerar sin pérdida de generalidad que $a_{11} = b_{11}$. Según el teorema 6.1.3, k_1 es el menor entero positivo tal que $f^{k_1}(a_{11}) = a_{11}$. Se obtiene pues que $k_1 = m_1$ y además

$$\begin{gathered} f(b_{11}) = b_{12} = f(a_{11}) = a_{12};\ f(b_{12}) = b_{13} = f(a_{12}) = a_{13};\ \ldots; \\ f(b_{1m_1-1}) = b_{1m_1} = f(a_{1k_1-1}) = a_{1k_1};\ f(b_{1m_1}) = b_{11} = f(a_{1k_1}) = a_{11}, \end{gathered}$$

es decir, $(a_{11}a_{12}\cdots a_{1k_1}) = (b_{11}b_{12}\cdots b_{1m_1})$. El mismo análisis podemos aplicar a $a_{21}, a_{31}\ldots, a_{r1}$ demostrando que $r \leq s$ y la igualdad de ciclos. En forma similar $s \leq r$, lo cual concluye la prueba del teorema. □

Ejemplo 6.1.5.

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

$f = (125794)(3)(6) = (125794)$;

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

$g = (134)(265)(78)(9) = (265)(134)(78) = (78)(134)(265) = (134)(78)(265) = (78)(265)(134) = (265)(78)(134)$.

6.2. El grupo alternante A_n

Definición 6.2.1. *Para $n \geq 2$, los ciclos de longitud 2 de S_n se conocen como* ***transposiciones****.*

Teorema 6.2.2. *Cada permutación de S_n es representable como un producto finito de transposiciones.*

Demostración. Puesto que cada permutacion es representable como un producto de ciclos disyuntos entonces es suficiente demostrar el teorema para cada ciclo. Sea $f = (a_1 a_2 \cdots a_m)$ un m-ciclo. Si $m = 1$ entonces $f = 1$ y $f = (a_1 a_2)(a_1 a_2)$. Sea pues $m \neq 1$. Nótese que $(a_1 a_2 \cdots a_m) = (a_m a_1)(a_{m-1} a_1) \cdots (a_2 a_1)$. □

Observación 6.2.3. (i) A diferencia del teorema 6.1.4, la representación de una permutación en producto de transposiciones no es única:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (12435) = (51)(31)(41)(21) = (12)(52)(32)(42).$$

(ii) Según el teorema anterior, cada permutación f de S_n es representable como un número finito r de transposiciones; además se vió que dicha representación no es única. De tal manera que podría presentarse la posibilidad de que en una descomposición r sea par y en otra r sea impar. Sin embargo, la siguiente proposición muestra que tal situación es imposible.

Proposición 6.2.4. *Sea f una permutación de S_n la cual tiene dos descomposiciones en producto de r y s transposiciones. Entonces, r es par si, y sólo si,, s es par.*

Demostración. Sea f una permutación de S_n la cual tiene dos descomposiciones en producto de transposiciones $f = f_1 \cdots f_r = f'_1 \cdots f'_s$ $r \geq 1, s \geq 1$. Consideremos el natural $p = \Pi_{j>i}(j - i)$, $i, j \in I_n$ (por ejemplo para $n = 4$ se tiene que $p = (4-3)(4-2)(4-1)(3-2)(3-1)(2-1) = 12$). Sea f una permutación cualquiera de S_n. Definamos la acción de f sobre p como $pf = \Pi_{j>i}(f(j) - f(i))$.

Nótese que pf es un entero (no necesariamente positivo como p); los factores $(f(j) - f(i))$ que conforman pf son diferencias de elementos de I_n y además $|pf| = p$. En efecto, demostraremos que si $f = f_1 \cdots f_r$, donde cada f_i, $1 \leq i \leq r$, es una transposición, entonces

$$pf = (-1)^r p.$$

(a) Sea $f = (ab)$ una transposición con $a > b$. Los factores $(j - i)$ de p en los cuales no intervienen ni a ni b no cambian al aplicar f. Consideremos pues aquellos factores donde aparezcan a o b o ambos. Se presentan entonces las siguientes posibilidades.

(i) Factores donde aparece a pero no b:

$$(n-a),((n-1)-a),((n-2)-a)\cdots((a+1)-a),$$
$$(a-(a-1)),(a-(a-2))\cdots(a-(b+1)),(a-(b-1))\cdots(a-1).$$

Al aplicar f a los factores de la primera fila obtenemos

$$(n-b),((n-1)-b)\cdots((a+1)-b)$$

y no hay cambios de signo. Al aplicar f a los factores de la seguda fila obtenemos

$$(b-(a-1)),(b-(a-2))\cdots(b-(b+1))(b-(b-1))\cdots(b-1)$$

y hay $a-b-1$ cambios de signo.

(ii) Los factores donde aparece b pero no a :

$$(n-b),((n-1)-b)\cdots((a+1)-b)$$
$$((a-1)-b),((a-2)-b)\cdots((b+1)-b)$$
$$(b-(b-1))\cdots(b-1).$$

Aplicando f a los factores anteriores obtenemos

$$(n-a),((n-1)-a)\cdots((a+1)-a)$$
$$((a-1)-a),((a-2)-a)\cdots((b+1)-a)$$
$$(a-(b-1))\cdots(a-1).$$

se presenta en este caso $a-b-1$ cambios de signo.

(iii) Factor donde aparece a y b: $(a-b)$

Al aplicar f obtenemos $(b-a)$ y hay un cambio de signo.

En total al aplicar f a p se efectuan $2(a-b-1)+1$ cambios de signos y así pf tiene signo menos.

Nótese que los factores de (i) mediante f se convierten en los factores de (ii) con algunos signos cambiados, y a su vez los de (ii) en los de (i) con algunos signos cambiados. De lo anterior se desprende que

$$pf=-p, f=(ab), a>b.$$

(b) Si $f=f_1\cdots f_r$ es un producto de r transposiciones, entonces

$$pf=(pf_1)f_2\cdots f_r=(-1)^r p.$$

(c) $pf=(-1)^r p=(-1)^s p$, entonces $(-1)^r=(-1)^s \Leftrightarrow r$ y s son pares o r y s son impares. □

Según la proposición anterior se pueden distinguir aquellas permutaciones que son producto de un número par de transposiciones.