Lección nº B Junio, 2021

Apéndice B

Grupos simétricos

B.1. Definiciones y propiedades básicas

Sea X un conjunto. Denotamos por $\mathrm{Sym}(X)$ al conjunto de todas las funciones biyectivas $\sigma : X \to X$. Este es un grupo con la composición usual de funciones.

Definición. El grupo $\mathrm{Sym}(X)$ se llama el *grupo simétrico* sobre X o el *grupo de permutaciones* de X.

Teorema B.1 (Cayley)**.** *Todo grupo es (isomorfo a) un subgrupo de un grupo simétrico.*

Demostración. Sea G un grupo, y consideremos la aplicación $f : G \to \mathrm{Sym}(G)$ dada por $f(g)(h) = gh$ para todo $g, h \in G$. Notemos que esta aplicación está bien definida: Si $g \in G$ entonces $f(g) \in \mathrm{Sym}(G)$ pues

$$f(g)(f(g^{-1})(h)) = g(g^{-1}h) = h,$$

de modo que $f(g)f(g^{-1}) = 1$ y similarmente $f(g^{-1})f(g) = 1$, por lo que $f(g)$ es biyectiva. Ahora, si $g_1, g_2 \in G$, para todo $h \in G$ tenemos que

$$(f(g_1)f(g_2))(h) = f(g_1)(f(g_2)(h)) = g_1(g_2h) = (g_1g_2)h = f(g_1g_2)(h),$$

por lo que $f(g_1)f(g_2) = f(g_1g_2)$, así f es un homomorfismo de grupos.

El homomorfismo f es inyectivo: Si $f(g) = 1$, entonces $gh = h$ para todo $h \in G$, de donde en particular $g = g1 = 1$, por lo que $\ker(f) = \{1\}$. Por ende $G \cong f(G) \leq \mathrm{Sym}(G)$, como se deseaba. □

Proposición B.2. *Sean X, Y dos conjuntos y $f : X \to Y$ una biyección, entonces f induce un isomorfismo $f' : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$.*

Demostración. Definamos $f' : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ del siguiente modo: Si $\sigma \in \mathrm{Sym}(X)$, entonces $f'(\sigma) = f \circ \sigma \circ f^{-1} : Y \to Y$. Dado que $f'(\sigma)$ es una composición de biyecciones, se sigue que $f'(\sigma)$ es una biyección, y por ende f' está bien definida. Dados $\sigma, \tau \in \mathrm{Sym}(X)$ tenemos que

$$f'(\sigma\tau) = f \circ \sigma \circ \tau \circ f^{-1} = (f \circ \sigma \circ f^{-1}) \circ (f \circ \tau \circ f^{-1}) = f'(\sigma)f'(\tau),$$

por lo que f' es un homomorfismo de grupos. Además, tenemos que f' es invertible con inversa $\sigma \mapsto f^{-1} \circ \sigma \circ f$, por lo que f' es un isomorfismo. □

Definición. El *n-ésimo grupo simétrico* es el grupo

$$S_n := \mathrm{Sym}(\{1, 2, \ldots, n\}).$$

Notemos que si X es un conjunto finito, podemos enlistar sus elementos $X = \{x_1, x_2, \ldots, x_n\}$ y de este modo obtenemos una función biyectiva $f : \{1, 2, \ldots, n\} \to X$ dada por $i \mapsto x_i$. Por la proposición anterior, esta biyección induce un isomorfismo $f' : S_n \to \mathrm{Sym}(X)$, por lo cual, uno puede mirar a S_n como el grupo de permutaciones de cualquier conjunto de n elementos.

Notemos que S_n actúa sobre cualquier conjunto de n elementos $X = \{x_1, \ldots, x_n\}$ mediante

$$\sigma x_i = x_{\sigma(i)}, \quad 1 \leq i \leq n.$$

Esta acción es transitiva, pues si $i \neq j$, consideramos la permutación $\sigma \in S_n$ dada por $\sigma(k) = k$ si $k \neq i, j$, $\sigma(i) = j$ y $\sigma(j) = i$, con lo cual

$$\sigma x_i = x_j.$$

Proposición B.3. *El orden del grupo S_n es $n!$.*

Demostración. Procederemos por inducción sobre n. Para $n = 1$ no hay nada que probar. Supongamos que $n > 1$ y consideremos el estabilizador T del elemento n para la acción de S_n sobre el conjunto $\{1, 2, \ldots, n\}$, es decir,

$$T = \{\sigma \in S_n \,|\, \sigma(n) = n\}.$$

Este es un subgrupo de S_n isomorfo a S_{n-1}, y por la hipótesis de inducción, tenemos que

$$|T| = |S_{n-1}| = (n-1)!.$$

Por el teorema órbita-estabilizador, se sigue que existe una biyección

$$S_n/T \to \{1, 2, \ldots, n\},$$

pues la órbita de n es precisamente el conjunto $\{1, 2, \ldots, n\}$, ya que la acción de S_n en cualquier conjunto de n elementos es transitiva. De este modo, tenemos que

$$[S_n : T] = n.$$

Con esto, del teorema de Lagrange tenemos que

$$|S_n| = [S_n : T]|T| = n(n-1)! = n!,$$

lo que completa la demostración.

□

Si $X = \{x_1, x_2, \ldots, x_n\}$ y $\sigma \in \mathrm{Sym}(X)$, denotamos

$$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}.$$

A esta forma de escribir a σ la llamamos la *notación de dos filas*. Nótese que el orden en que aparecen los elementos en la primera fila depende únicamente de la elección del orden de los elementos de X. Por ejemplo, los elementos

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}, \quad \begin{pmatrix}2 & 1 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix} \quad \text{y} \quad \begin{pmatrix}4 & 2 & 3 & 1\\ 4 & 3 & 1 & 2\end{pmatrix}$$

representan al mismo elemento de S_4, explícitamente, a la permutación $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ y $4 \mapsto 4$.

Notemos que si

$$\sigma = \begin{pmatrix}x_1 & x_2 & \cdots & x_n\\ y_1 & y_2 & \cdots & y_n\end{pmatrix} \in \mathrm{Sym}(X),$$

entonces

$$\sigma^{-1} = \begin{pmatrix}y_1 & y_2 & \cdots & y_n\\ x_1 & x_2 & \cdots & x_n\end{pmatrix}.$$

Esta notación, pese a tener su ventaja, no nos da luz acerca de la estructura del grupo S_n. Por este motivo, es conveniente usar la siguiente notación:

Definición. Un elemento $\sigma \in S_n$ se dice un *k-ciclo* si existen $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$, dos a dos distintos, tales que $\sigma(i_j) = i_{j+1}$ para $1 \leq j < k$, $\sigma(i_k) = i_1$ y $\sigma(i) = i$ para todo $i \neq i_j$, $1 \leq j \leq k$. En este caso escribiremos

$$\sigma = (i_1\ i_2\ \cdots\ i_k).$$

Un 2-ciclo se llama una *transposición*.

Dos ciclos $(i_1\ i_2\ \cdots\ i_k)$ y $(j_1\ j_2\ \cdots\ j_l)$ se dicen *disjuntos* si

$$\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_l\} = \emptyset.$$

Proposición B.4. *Los ciclos disjuntos conmutan. Es decir, si $(i_1\ i_2\ \cdots\ i_k)$ y $(j_1\ j_2\ \cdots\ j_l)$ son ciclos disjuntos, entonces*

$$(i_1\ i_2\ \cdots\ i_k)(j_1\ j_2\ \cdots\ j_l) = (j_1\ j_2\ \cdots\ j_l)(i_1\ i_2\ \cdots\ i_k)$$

Demostración. Escribamos $\sigma_1 = (i_1\ i_2\ \cdots\ i_k)$ y $\sigma_2 = (j_1\ j_2\ \cdots\ j_l)$. Recordemos que $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_l\} = \emptyset$. Sea $i \in \{1, 2, \ldots, n\}$ y consideremos tres posibilidades:

- Si $i \notin \{i_1, i_2, \ldots, i_k\} \cup \{j_1, j_2, \ldots, j_l\}$, en ese caso $\sigma_1(i) = \sigma_2(i) = i$ y por ende tenemos

  $$\sigma_1(\sigma_2(i)) = i = \sigma_2(\sigma_1(i)).$$

- Si $i \in \{i_1, \ldots, i_k\}$, entonces $i \notin \{j_1, \ldots, j_l\}$ y entonces $i = i_p$ para cierto $1 \leq p \leq k$. Si $p < k$, entonces

  $$\sigma_1(\sigma_2(i)) = \sigma_1(\sigma_2(i_p)) = \sigma_1(i_p) = i_{p+1}$$

  y

  $$\sigma_2(\sigma_1(i)) = \sigma_2(\sigma_1(i_p)) = \sigma_2(i_{p+1}) = i_{p+1},$$

  de modo que $\sigma_1\sigma_2(i) = \sigma_2\sigma_1(i)$. Si $p = k$ tenemos lo mismo sustituyendo i_{p+1} por i_1.

- Si $i \in \{j_1, \ldots, j_l\}$. Este caso es análogo al anterior.

Se concluye de lo anterior que $\sigma_1\sigma_2(i) = \sigma_2\sigma_1(i)$ para todo $i \in \{1, 2, \ldots, n\}$, de donde $\sigma_1\sigma_2 = \sigma_2\sigma_1$. $\square$

Teorema B.5. *Todo elemento de S_n se escribe de manera única (salvo el orden de los factores) como un producto de ciclos disjuntos.*

Demostración. Sea $\sigma \in S_n$ y sea $G = \langle \sigma \rangle$ el subgrupo cíclico de S_n generado por σ. El grupo G actúa sobre $\{1, 2, \ldots, n\}$ restringiendo la acción de S_n a G. Sean $O_1, O_2, \ldots, O_r$ las distintas órbitas bajo esta acción y elijamos $i_k \in O_k$ un representante de cada órbita. Sea n_k el menor entero positivo tal que $\sigma^{n_k}(i_k) = i_k$ y definamos

$$\sigma_k = (i_k \ \sigma(i_k) \ \cdots \ \sigma^{n_k-1}(i_k)).$$

Notemos que si $i \notin O_k$, entonces $\sigma_k(i) = i$, pues de no ser así $i = \sigma^j(i_k)$ para cierto j, de donde $i \in O_k$, lo que es absurdo. Mas aún, tenemos que

$$O_k = \{i_k, \sigma(i_k), \ldots, \sigma^{n_k-1}(i_k)\},$$

de modo que los ciclos σ_k son dos a dos disjuntos. Probaremos que $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$. En efecto, si $i \in \{1, 2, \ldots, n\}$ entonces $i \in O_k$ para un único O_k, y por ende $\sigma_l(i) = i$ para todo $l \neq k$. Más aún $\sigma(i) \in O_k$ y así $\sigma_l(\sigma(i)) = \sigma(i)$ para todo $l \neq k$. Dado que $i \in O_k$, tenemos que $i = \sigma^j(i_k)$ para cierto $0 \leq j \leq n_-1$ y así

$$\sigma_k(i) = \sigma_k(\sigma^j(i_k)) = \sigma^{j+1}(i_k) = \sigma(\sigma^j(i_k)) = \sigma(i)$$

con lo cual

$$\sigma_1 \cdots \sigma_k \cdots \sigma_r(i) = \sigma_1 \cdots \sigma_{k-1}\sigma_k(i) = \sigma_1 \cdots \sigma_{k-1}(\sigma(i)) = \sigma(i).$$

Esto prueba que tal descomposición en producto de ciclos disjuntos existe.

Para la unicidad, notemos que necesariamente los ciclos en la descomposición de σ están en correspondencia biunívoca con las órbitas de la acción de G sobre $\{1, 2, \ldots, n\}$, y cada órbita determina de manera única a los ciclos. □

B.2. Sistemas de generadores

En esta sección estudiamos aquellos subconjuntos de S_n que generan a S_n. Iniciemos por los más sencillos, que son las transposiciones. Para cada $1 \leq i < n$ denotaremos por s_i a la transposición $(i \ i+1)$. A los $n-1$ elementos s_i se los llama las *transposiciones simples* de S_n.

Teorema B.6. *El grupo simétrico S_n está generado por las $n-1$ transposiciones simples.*

Demostración. Primero notemos que un cálculo directo nos da, para todo $1 \leq i < n-1$,

$$(i \ n) = s_i s_{i+1} \cdots s_{n-1}.$$

A continuación, probaremos el teorema por inducción sobre n. Para $n = 1, 2$ no hay nada que probar. Supongamos que el teorema es válido para el grupo S_{n-1} y sea T el estabilizador del elemento n en la acción de S_n sobre el conjunto $\{1, \ldots, n\}$. Entonces $S_{n-1} \cong T$. Sean $s'_1, \ldots, s'_{n-2}$ las transposiciones simples de S_{n-1}, entonces bajo el isomorfismo $S_{n-1} \cong T$ estas corresponden a las transposiciones simples $s_1, \ldots, s_{n-2}$ de S_n. Por hipótesis de inducción, $s'_1, \ldots, s'_{n-2}$ generan a S_{n-1} y por ende $s_1, \ldots, s_{n-2}$ generan a T.

Sea $\sigma \in S_n$, entonces, si $\sigma \in T$, tenemos que $\sigma \in \langle s_1, \ldots, s_{n-2} \rangle \subseteq \langle s_1, \ldots, s_{n-2}, s_{n-1} \rangle$. Si $\sigma \notin T$, entonces $\sigma(n) = i \neq n$. Sea $\tau = (i \ n) = s_i s_{i+1} \cdots s_{n-1}$, entonces $\tau \in \langle s_1, \ldots, s_{n-1} \rangle$ y así

$$\tau\sigma(n) = \tau(i) = n,$$

de donde $\tau\sigma \in T$, de donde $\tau\sigma \in \langle s_1, \ldots, s_{n-1}$. Pero entonces

$$\sigma = \tau(\tau\sigma) \in \langle s_1, \ldots, s_{n-1} \rangle.$$

Esto prueba que $S_n \subseteq \langle s_1, \ldots, s_{n-1} \rangle$. La otra inclusión es trivial. □

Teorema B.7. *El grupo simétrico S_n está generado por las $n-1$ transposiciones $(1\ i)$, $2 \leq i \leq n$.*

Demostración. Sea $G = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$. Notemos que

$$s_i = (i\ i+1) = (1\ i)(1\ i+1)(1\ i),$$

de modo que $s_i \in G$ para todo $1 \leq i \leq n$. Pero S_n es el subgrupo más pequeño que contiene a las transposiciones s_i, de modo que $S_n \leq G$. Pero por definición, $G \subseteq S_n$, de modo que $G = S_n$. □

El siguiente resultado es muy importante. Será utilizado en esta sección y en la siguiente.

Lema B.8. *Sean $\sigma \in S_n$, entonces para todo k-ciclo $(i_1\ i_2\ \cdots\ i_k)$ tenemos que*

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$$

Demostración. Por comodidad, escribamos $i_{k+1} = i_1$, $\tau = (i_1\ i_2\ \cdots\ i_k)$ y $\tau' = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$. Sea $m \in \{1, 2, \ldots, n\}$, y consideremos dos posibilidades:

- Si $m = \sigma(i_r)$ para cierto $1 \leq r \leq k$, entonces $\tau'(m) = \sigma(i_{r+1})$. Por otro lado,

  $$\sigma\tau\sigma^{-1}(m) = \sigma\tau(i_r) = \sigma(i_{r+1}).$$

  Así $\sigma\tau\sigma^{-1}(m) = \tau'(m)$.

- Si $m \neq \sigma(i_r)$ para todo $1 \leq r \leq k$, entonces $\tau'(m) = m$. Entonces tenemos que $\sigma^{-1}(m) \neq i_r$ para todo $1 \leq r \leq k$ y por ende $\tau(\sigma^{-1}(m)) = \sigma^{-1}(m)$, con lo cual

  $$\sigma\tau\sigma^{-1}(m) = \sigma(\sigma^{-1})(m) = m,$$

  por lo que $\sigma\tau\sigma^{-1}(m) = \tau'(m)$.

Entonces $\sigma\tau\sigma^{-1} = \tau'$, como se deseaba. □

Teorema B.9. *Para $n \geq 3$, el grupo simétrico S_n está generado por la transposición $(1\ 2)$ y el n-ciclo $(1\ 2\ \cdots\ n)$.*

Demostración. Escribamos $\sigma = (1\ 2\ \cdots\ n)$. Notemos que

$$\sigma^k(1) = k+1, \quad 1 \leq k \leq n-1,$$

Por el Lema B.8, tenemos que, para cada $2 \leq k \leq n-1$

$$\sigma^{k-1}(1\ 2)\sigma^{-(k-1)} = (\sigma^{k-1}(1)\ \sigma^{k-1}(2)) = (k\ k+1) = s_k,$$

de modo que $s_k \in \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$ para todo $1 \leq k \leq n-1$ y así $S_n \leq \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$. La otra inclusión es trivial, por ende $S_n = \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$. □

Corolario B.10. *Para $n \geq 3$, el grupo simétrico S_n está generado por la transposición $(1\ 2)$ y el $(n-1)$-ciclo $(2\ 3\ \cdots\ n)$.*

Demostración. Notemos que claramente $(1\ 2) \in \langle (1\ 2), (2\ 3\ \cdots\ n) \rangle$. Por otro lado notemos que

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

de modo que $(1\ 2\ \cdots\ n) \in \langle (1\ 2), (2\ 3\ \cdots\ n) \rangle$. Esto implica que $S_n \leq \langle (1\ 2), (2\ 3\ \cdots\ n) \rangle$ y por ende que $S_n = \langle (1\ 2), (2\ 3\ \cdots\ n) \rangle$. □

B.3. Clases de conjugación

Como todo grupo, S_n actúa sobre sí mismo por conjugación. Las órbitas de esta acción son las clases de conjugación. El propósito de esta sección es determinar de manera explícita las clases de conjugación de S_n proporcionando un criterio que permita discriminar cuando dos transposiciones son conjugadas entre sí.

Definición. Sea n un entero no negativo. Una *partición* de n es una sucesión $\lambda = (\lambda_1, \lambda_2, \dots)$ de enteros no negativos tal que

- λ es (débilmente) decreciente, es decir, $\lambda_1 \geq \lambda_2 \geq \cdots$.
- $\sum_{i \geq 0} \lambda_i = n$.

En este caso escribiremos $\lambda \vdash n$.

Notemos que por definición, existe $k \geq 1$ tal que $\lambda_j = 0$ para todo $j > k$, en este caso escribiremos

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k).$$

Nótese que no exigimos que $\lambda_k \neq 0$, de modo que, por ejemplo $(2, 2, 1, 0, 0)$, $(2, 2, 1, 0)$ y $(2, 2, 1)$ son la misma partición de 5.

Si $\sigma \in S_n$, podemos escribir $\sigma = \sigma_1 \cdots \sigma_r$, donde σ_i es un λ_i-ciclo y los σ_i son ciclos disjuntos. Dado que ciclos disjuntos conmutan, podemos asumir que $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$. Más aún, dado que cada $i \in \{1, \dots, n\}$ aparece exactamente una vez en alguno de los σ_k, tenemos que

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_r,$$

por lo que $\lambda = (\lambda_1, \dots, \lambda_r)$ es una partición de n. En este caso, diremos que σ es *de tipo* λ.

Teorema B.11. *Sean $\sigma, \tau \in S_n$ dos permutaciones. Las siguientes afirmaciones son equivalentes:*

(i) *σ y τ pertenecen a la misma clase de conjugación de S_n.*

(ii) *σ y τ son de tipo λ para una misma partición $\lambda \vdash n$.*

Demostración. Supongamos primero que σ y τ pertenecen a una misma clase de conjugación, entonces $\sigma = \rho\tau\rho^{-1}$ para cierto $\rho \in S_n$. Escribamos $\tau = \tau_1\tau_2\cdots\tau_r$, donde cada τ_i es un λ_i ciclo y los τ_i son ciclos disjuntos. Entonces τ es una permutación de tipo $\lambda = (\lambda_1, \ldots, \lambda_r)$. Probaremos que σ también es de tipo λ. Para ello, notemos que

$$\sigma = \rho\tau\rho^{-1} = (\rho\tau_1\rho^{-1})(\rho\tau_2\rho^{-1})\cdots(\rho\tau_r\rho^{-1}).$$

Escribamos $\tau_i = (k_1\ k_2\ \cdots\ k_{\lambda_i})$, entonces por el Lema B.8 tenemos que

$$\rho\tau_i\rho^{-1} = (\rho(k_1)\ \rho(k_2)\ \cdots\ \rho(k_{\lambda_i})),$$

es decir, que $\sigma_i := \rho\tau_i\rho^{-1}$ es un λ_i-ciclo. Dado que ρ es una biyección, esta aplica conjuntos disjuntos en conjuntos disjuntos, por lo que los ciclos σ_i son disjuntos. De este modo

$$\sigma = \sigma_1\sigma_2\cdots\sigma_k$$

y tenemos que σ es de tipo λ.

Recíprocamente, supongamos que σ y τ son de tipo λ. Escribamos las descomposiciones en ciclos disjuntos

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r, \quad \tau = \tau_1\tau_2\cdots\tau_r,$$

donde σ_i y τ_i son λ_i-ciclos. Sea $\mu_0 = 0$ y $\mu_k = \lambda_1 + \lambda_2 + \cdots + \lambda_k$. Entonces podemos escribir

$$\sigma_k = (i_{\mu_{k-1}+1}\ i_{\mu_{k-1}+2}\ \cdots\ i_{\mu_{k-1}+\lambda_k}) \quad \text{y} \quad \tau_k = (j_{\mu_{k-1}+1}\ j_{\mu_{k-1}+2}\ \cdots\ j_{\mu_{k-1}+\lambda_k}).$$

Entonces definimos

$$\rho = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} \in S_n.$$

Probemos que $\tau_k = \rho\sigma_k\rho^{-1}$ para cada $1 \leq k \leq r$. Sea $m \in \{1, \ldots, n\}$, entonces $m = j_p$ para cierto $1 \leq p \leq n$. Consideremos dos posibilidades:

- Si $p \leq \mu_{k-1}$ o $p > \mu_k$, entonces i_p no ocurre en el ciclo σ_k y j_p no ocurre en el ciclo τ_k y así

  $$\rho\sigma_k\rho^{-1}(m) = \rho\sigma_k(i_p) = \rho(i_p) = j_p = m,$$

  por otro lado, $\tau_k(m) = j_p = m$, de donde $\rho\sigma_k\rho^{-1}(m) = \tau_k(m)$.

- Si $\mu_{k-1} < p \leq \mu_k$, entonces i_p ocurre en el ciclo σ_k y j_p ocurre en el ciclo τ_k. Supongamos que $p < \mu_k = \lambda_k + \mu_{k-1}$, entonces

  $$\rho\sigma_k\rho^{-1}(m) = \rho\sigma_k(i_p) = \rho(i_{p+1}) = j_{p+1},$$

  y por otro lado $\tau_k(m) = \tau_k(j_p) = j_{p+1}$, de modo que $\rho\sigma_k\rho^{-1}(m) = \tau_k(m)$.

Con esto, tenemos que

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\cdots(\rho\sigma_r\rho^{-1}) = \tau_1\tau_2\cdots\tau_r = \tau,$$

lo que prueba que σ y τ pertenecen a la misma clase de conjugación. □

B.4. Grupos alternantes

Sea $\sigma \in S_n$, y supongamos que σ es de tipo $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$. Escribimos $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ para la descomposición de σ en producto de ciclos disjuntos. Definimos

$$N(\sigma) = n - r = \sum_{i=1}^{r}(\lambda_i - 1).$$

Lema B.12. *Sean $i, i_1, \ldots, i_p, j, j_1, \ldots, j_q$ números dos a dos distintos en el conjunto $\{1, 2, \ldots, n\}$. Entonces*

$$(i\ j)(i\ i_1\ i_2\ \cdots\ i_p\ j\ j_1\ j_2\ \cdots\ j_q) = (j\ j_1\ j_2\ \cdots\ j_q)(i\ i_1\ i_2\ \cdots\ i_p).$$

Demostración. Escribamos $\tau = (i\ j)$, $\sigma = (i\ i_1\ i_2\ \cdots\ i_p\ j\ j_1\ j_2\ \cdots\ j_q)$, $\sigma_1 = (j\ j_1\ j_2\ \cdots\ j_q)$ y $\sigma_2 = (i\ i_1\ i_2\ \cdots\ i_p)$. Entonces debemos probar que $\tau\sigma = \sigma_1\sigma_2$. Sea $m \in \{1, \ldots, n\}$. Si m no sucede en ninguno de los ciclos τ, σ, σ_1 o σ_2, entonces claramente $\tau\sigma(m) = \sigma_1\sigma_2(m)$. Supongamos que $m = i$, entonces

$$\tau\sigma(m) = \tau\sigma(i) = \tau(i_1) = i_1$$

y

$$\sigma_1\sigma_2(m) = \sigma_1\sigma_2(i) = \sigma_1(i_1) = i_1,$$

así $\tau\sigma(m) = \sigma_1\sigma_2(m)$. De manera análoga ocurre si $m = j$. Supongamos que $m = i_r$ con $1 \leq r < p$, entonces

$$\tau\sigma(m) = \tau\sigma(i_r) = \tau(i_{r+1}) = i_{r+1} = \sigma_1(i_{r+1}) = \sigma_1\sigma_2(i_r) = \sigma_1\sigma_2(m).$$

Si en cambio $m = i_p$, entonces

$$\tau\sigma(m) = \tau\sigma(i_p) = \tau(j) = i$$

mientras que

$$\sigma_1\sigma_2(m) = \sigma_1\sigma_2(i_p)\sigma_1(i) = i,$$

con lo cual $\tau\sigma(m) = \sigma_1\sigma_2(m)$. De manera análoga se tiene esta igualdad si $m = j_r$ para $1 \leq r \leq q$. □

Recordemos que S_n está generado por transposiciones (de hecho por ciertos subconjuntos de transposiciones, como se probó en la sección anterior).

Lema B.13. *Sea $\sigma \in S_n$ y escribamos $\sigma = \tau_k \cdots \tau_1$ donde cada τ_i es una transposición. Entonces*

$$k \equiv N(\sigma) \pmod 2.$$

Demostración. Procederemos por inducción sobre k. Si $k = 0$, entonces $\sigma = 1$ y $N(1) = 0$ de modo que $k = N(\sigma)$.

Sea $\sigma' = \tau_{k-1} \cdots \tau_1$, de modo que $\sigma = \tau_k\sigma'$. Por hipótesis de inducción tenemos que

$$k - 1 \equiv N(\sigma') \pmod 2.$$

Ahora, escribamos $\tau_k = (i\ j)$. Supongamos que i y j aparecen en el mismo ciclo σ_s en la descomposición de σ' en ciclos disjuntos, $\sigma' = \sigma_1 \ldots \sigma_\ell$. Entonces escribimos

$$\sigma_s = (i\ i_1\ i_2\ \cdots\ i_p\ j\ j_1\ j_2\ \cdots\ j_q),$$

con lo cual

$$\sigma = (i\ j)\sigma_s\sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \cdots \sigma_\ell,$$

donde hemos usado el hecho de que ciclos disjuntos conmutan. Por el Lema B.12 tenemos que

$$\sigma = (j\ j_1\ j_2\ \cdots\ j_q)(i\ i_1\ i_2\ \cdots\ i_p)\sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \cdots \sigma_\ell,$$

lo que significa que

$$N(\sigma) = N(\sigma') + 1,$$

y por ende

$$k \equiv N(\sigma') + 1 = N(\sigma) \pmod 2.$$

Supongamos ahora que i y j ocurren en ciclos disjuntos σ_s, σ_t y escribamos

$$\sigma_s = (j\ j_1\ j_2\ \cdots\ j_q) \quad \text{y} \quad \sigma_t = (i\ i_1\ i_2\ \cdots\ i_p).$$

De nuevo por el Lema B.12 tenemos que (al multiplicar ambos lados de la igualdad del lema por $(i\ j)^{-1} = (i\ j)$)

$$(i\ j)\sigma_s\sigma_t = (i\ i_1\ i_2\ \cdots\ i_p\ j\ j_1\ j_2\ \cdots\ j_q),$$

con lo cual

$$\begin{aligned}\sigma &= (i\ j)\sigma_s\sigma_t\sigma_1\cdots\hat{\sigma}_s\cdots\hat{\sigma}_t\cdots\sigma_\ell \\ &= (i\ i_1\ i_2\ \cdots\ i_p\ j\ j_1\ j_2\ \cdots\ j_q)\sigma_1\cdots\hat{\sigma}_s\cdots\hat{\sigma}_t\cdots\sigma_\ell,\end{aligned}$$

de donde

$$N(\sigma) = N(\sigma') - 1,$$

y así

$$k \equiv N(\sigma') + 1 \equiv N(\sigma') - 1 = N(\sigma) \pmod 2.$$

Esto completa la demostración. □

Teorema B.14. *Sea $\sigma \in S_n$ y supongamos que escribimos*

$$\sigma = \tau_1\cdots\tau_k = \tau_1'\cdots\tau_\ell',$$

donde τ_i y τ_j' son transposiciones, $1 \le i \le k$, $1 \le j \le \ell$. Entonces

$$k \equiv j \pmod 2.$$

Demostración. Por el Lema B.13 tenemos que

$$k \equiv N(\sigma) \equiv \ell \pmod 2.$$

□

Definición. Sea $\sigma \in S_n$. Diremos que σ es una permutación *par* si σ puede escribirse como el producto de un número par de transposiciones o, equivalentemente, si $N(\sigma)$ es par. En cambio diremos que σ es una permutación *impar* si σ puede escribirse como el producto de un número impar de transposiciones o, equivalentemente, si $N(\sigma)$ es impar.

Definimos una aplicación $\operatorname{sign} : S_n \to \{1, -1\}$ mediante

$$\operatorname{sign}(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es par,} \\ -1 & \text{si } \sigma \text{ es impar.} \end{cases}$$

Notemos que esta aplicación es un homomorfismo de grupos. En efecto, sean $\sigma_1, \sigma_2 \in S_n$ y escribamos

$$\sigma_1 = \tau_1\cdots\tau_k, \quad \sigma_2 = \tau_1'\cdots\tau_\ell',$$

donde τ_i y τ_j' son transposiciones, $1 \le i \le k$, $1 \le j \le \ell$. Entonces notemos que

$$\sigma_1\sigma_2 = \tau_1\cdots\tau_k\tau_1'\cdots\tau_\ell',$$

de donde:

- Si σ_1 y σ_2 son ambas pares o ambas impares, entonces $k+\ell$ es par y por ende $\sigma_1\sigma_2$ es par. En ambos casos
$$\text{sign}(\sigma_1\sigma_2) = 1 = \text{sign}(\sigma_1)\text{sign}(\sigma_2).$$
- Si σ_1 es par y σ_2 es impar (o viceversa) entonces $k+\ell$ es impar y por ende $\sigma_1\sigma_2$ es impar. En ambos casos
$$\text{sign}(\sigma_1\sigma_2) = -1 = \text{sign}(\sigma_1)\text{sign}(\sigma_2).$$

Definición. Si $\sigma \in S_n$, se define el *signo* de σ como $\text{sign}(\sigma)$.

Tenemos entonces que $A_n = \ker(\text{sign})$ es un subgrupo de S_n que está conformado por todas las permutaciones pares. Más aún, este es un subgrupo normal de S_n y por el primer teorema de isomorfía, tenemos que $[S_n : A_n] = 2$.

Definición. A_n se llama el *n-ésimo grupo alternante*.

De lo anteriormente visto, tenemos:

Proposición B.15. *A_n es un subgrupo normal de S_n y, si $n \geq 2$,*
$$|A_n| = \frac{n!}{2}.$$

B.5. Una presentación del grupo simétrico

Recordemos que las transposiciones $s_i = (i\ i+1)$, $1 \leq i \leq n-1$, las denominamos *transposiciones simples*. Este es un sistema de generadores del grupo simétrico S_n.

Proposición B.16. *Para $n \geq 2$, las transposiciones simples de S_n verifican las siguientes relaciones:*
$$\begin{aligned} s_i^2 &= 1 && \text{para } 1 \leq i \leq n-1, \\ s_i s_j &= s_j s_i && \text{si } |i-j| > 1, \\ s_i s_{i+1} s_i &= s_{i+1} s_i s_{i+1} && \text{para } 1 \leq i \leq n-2. \end{aligned}$$
La tercera de estas relaciones se conoce como relación de trenzas *y es equivalente a $(s_i s_{i+1})^3 = 1$.*

Demostración. La relación $s_i^2 = 1$ para todo $1 \leq i \leq n-1$ es trivial. Si $|i-j| > 1$ entonces s_i y s_j son 2-ciclos disjuntos, por ende conmutan, de donde $s_i s_j = s_j s_i$. Supongamos que $1 \leq i \leq n-2$, entonces
$$\begin{aligned} s_i s_{i+1} s_i &= (i\ i+1)(i+1\ i+2)(i\ i+1) \\ &= (i\ i+2) \\ &= (i+1\ i+2)(i\ i+1)(i+1\ i+2) \\ &= s_{i+1} s_i s_{i+1}, \end{aligned}$$
lo que prueba las relaciones de trenzas. La equivalencia entre la relación $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ y $(s_i s_{i+1})^3$ es inmediata del hecho de que $s_i = s_i^{-1}$. □

Consideremos la matriz simétrica $M = (m_{ij}) \in \mathbb{M}_{n-1}(\mathbb{Z})$ definida por

$$\begin{aligned} m_{ii} &= 1 && \text{para } 1 \leq i \leq n-1, \\ m_{ij} &= 2 && \text{si } |i-j| > 1, \\ m_{i,i+1} &= 3 && \text{para } 1 \leq i \leq n-2, \end{aligned}$$

de modo que

$$M = \begin{pmatrix} 1 & 3 & 2 & \cdots & 2 & 2 \\ 3 & 1 & 3 & \cdots & 2 & 2 \\ 2 & 3 & 1 & \cdots & 2 & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2 & 2 & 2 & \cdots & 1 & 3 \\ 2 & 2 & 2 & \cdots & 3 & 1 \end{pmatrix}.$$

Notemos que las relaciones dadas en la Proposición B.16 pueden reescribirse como

$$(s_i s_j)^{m_{ij}} = 1 \quad \text{para todo } 1 \leq i, j \leq n-1.$$

Nuestro objetivo será probar que estas relaciones caracterizan por completo al grupo simétrico S_n, es decir,

$$S_n \cong \langle s_1, s_2, \ldots, s_{n-1} \mid (s_i s_j)^{m_{ij}} = 1,\ 1 \leq i, j \leq n-1 \rangle.$$

Para ello, sea $S = \{t_1, \ldots, t_{n-1}\}$ un conjunto con $n-1$ símbolos formales y sea

$$W_n = \langle t_1, \ldots, t_{n-1} \mid (t_i t_j)^{n_{ij}} = 1,\ 1 \leq i, j \leq n-1 \rangle.$$

Recordemos que esto significa que $W_n = F/R$ donde F es el grupo libre generado por S y R es el subgrupo de F definido por

$$R = \langle (t_i t_j)^{n_{ij}} \mid 1 \leq i, j \leq n-1 \rangle.$$

Por el teorema de von Dyck, existe un epimorfismo

$$f : W_n \to S_n, \quad t_i \mapsto s_i, \quad 1 \leq i \leq n-1.$$

Por ende, basta probar que f es inyectiva. Para ello, dado que f es sobreyectiva y $|S_n| = n!$, basta probar que $|W_n| = n!$. El resto de esta sección tiene como objetivo probar esta afirmación.

Notemos que como $t_i^{-1} = t_i$ para todo $1 \leq i \leq n-1$, entonces todo elemento $w \in W$ puede escribirse en la forma

$$w = t_{i_1} t_{i_2} \cdots t_{i_k}, \quad 1 \leq i_1, i_2, \ldots, i_k \leq n.$$

Lema B.17. *Para todo $n \geq 2$,*

$$|W_n| \leq n!.$$

Demostración. Procedemos por inducción sobre n. Para $n = 2$, tenemos que $W_2 = \{1, t_1\}$, de modo que $|W_2| = 2 \leq 2!$. Supongamos que el resultado es válido para W_n. Sea

$$T = \langle t_1, \ldots, t_{n-1} \rangle \leq W_{n+1}$$

el subgrupo de W_{n+1} generado por $t_1, \ldots, t_{n-1}$. Dado que $(t_i t_j)^{m_{ij}} = 1$ para todo $1 \leq i, j \leq n-1$, por el teorema de von Dyck existe un epimorfismo

$$W_n \to T,$$

lo que junto con la hipótesis de inducción implica que

$$|T| \leq |W_n| \leq n!.$$

Definamos los conjuntos

$$T_0 = t_1 t_2 \cdots t_n T, \quad T_1 = t_2 \cdots t_n T, \quad , \cdots \quad T_{n-1} = t_n T, \quad T_n = T.$$

Notemos que si $1 \leq i, j \leq n$, entonces

$$t_i T_j = \begin{cases} T_{i-1} & \text{si } j = i, \\ T_i & \text{si } j = i-1, \\ T_j & \text{si } j \neq i, i-1. \end{cases}$$

En efecto, si $j = i$, tenemos

$$t_i T_j = t_i T_i = t_i t_{i+1} \cdots t_n T = T_{i-1}.$$

Si $j = i - 1$, tenemos

$$t_i T_j = t_i T_{i-1} = t_i t_i t_{i+1} \cdots t_n T = t_{i+1} \cdots t_n T = T_i.$$

Ahora, supongamos que $j \neq i, i-1$ y consideremos dos casos: Si $j \geq i+1$, entonces $|k - i| > 1$ para todo $j + 1 \leq k \leq n$, de donde $t_i t_k = t_k t_i$ para tales valores de k. Así

$$t_i T_j = t_i t_{j+1} t_{j+2} \cdots t_n T = t_{j+1} \cdots t_n t_i T.$$

Ahora, dado que $i < n$ (caso contrario sería imposible que $j \geq i + 1$) tenemos que $t_i \in T$, de modo que $t_i T = T$ y por ende

$$t_i T_j = t_{j+1} \cdots t_n T = T_j.$$

Si en cambio $j \leq i - 2$, tenemos que $t_i t_k = t_k t_i$ para todo $1 \leq k \leq i - 2$ y además de la relación de trenzas, tenemos que $t_i t_{i-1} t_i = t_{i-1} t_i t_{i-1}$, con lo cual

$$\begin{aligned} t_i T_j &= t_i t_{j+1} t_{j+2} \cdots t_n T \\ &= t_{j+1} \cdots t_{i-2} t_i t_{i-1} t_i t_{i+1} \cdots t_n T \\ &= t_{j+1} \cdots t_{i-2} t_{i-1} t_i t_{i-1} t_{i+1} \cdots t_n T. \end{aligned}$$

Ahora, $t_{i-1} t_k = t_k t_{i-1}$ para todo $i + 1 \leq k \leq n$, de modo que

$$t_i T_j = t_{j+1} \cdots t_n t_{i-1} T = t_{j+1} \cdots t_n T = T_j$$

donde hemos usado que $i - 1 \leq n$ y por ende $t_{i-1} \in T$.

Entonces hemos probado que para todo $1 \leq i, j \leq n$, existe $1 \leq k \leq n$ tal que $t_i T_j = T_k$. Si $w \in W$, escribimos $w = t_{i_1} \cdots t_{i_m}$ y de este modo $wT = wT_n = T_j$ para algún j, lo que significa que

$$W_{n+1}/T = \{T_0, T_1, \ldots, T_n\}.$$

Nótese que, *a priori*, los T_i no son dos a dos disjuntos y por ende

$$[W_{n+1} : T] \leq n + 1,$$

y de este modo

$$|W_{n+1}| = [W_{n+1} : T]|T| \leq (n+1)n! = (n+1)!,$$

como se deseaba. □

Ahora, dado que $f : W_n \to S_n$ es sobreyectiva, tenemos que $|W_n| \geq |S_n| = n!$, por lo que el lema anterior implica que $|W_n| = n!$. Esto prueba:

Teorema B.18. *Para $n \geq 2$, el grupo simétrico S_n admite la siguiente presentación:*

$$S_n \cong \langle s_1, s_2, \ldots, s_{n-1} \mid (s_i s_j)^{m_{ij}} = 1,\ 1 \leq i, j \leq n-1 \rangle.$$

Observación. El teorema anterior prueba que el par (S_n, S), donde $S = \{s_1, \ldots, s_{n-1}\}$, es un *sistema de Coxeter* de tipo A_{n-1}.

B.6. Largo y número de inversiones

Recordemos que, si $s_1, \ldots, s_{n-1}$ son las transposiciones simples de S_n, entonces todo elemento $\sigma \in S_n$ puede escribirse en la forma

$$\sigma = s_{i_1} s_{i_2} \cdots s_{i_k}, \quad 1 \leq i_1, \ldots, i_k \leq n.$$

Definición. Sea $\sigma \in S_n$. El *largo* de σ es el menor entero no negativo k tal que

$$\sigma = s_{i_1} s_{i_2} \cdots s_{i_k}, \quad 1 \leq i_1, \ldots, i_k \leq n.$$

Denotamos al largo de σ por $\ell(\sigma)$. Si $\ell(\sigma) = m$, cualquier expresión $\sigma = s_{i_1} s_{i_2} \cdots s_{i_m}$ se dice una *expresión reducida* para σ.

Notemos que, por definición del signo de una permutación, tenemos que

$$\operatorname{sign}(\sigma) = (-1)^{\ell(\sigma)}, \quad \text{para todo } \sigma \in S_n.$$

Ejercicio B.19. Demuestre que la función largo posee las siguientes propiedades:

(a) $\ell(\sigma) = \ell(\sigma^{-1})$, para todo $\sigma \in S_n$.

(b) $\ell(s_i \sigma) = \ell(\sigma) \pm 1$ para todo $1 \leq i \leq n-1$.

En lo que sigue, la siguiente notación resultará útil. Si $\sigma \in S_n$, escribiremos $x_i = \sigma(i)$ y

$$\sigma = x_1 x_2 \cdots x_n.$$

Así, si por ejemplo $\sigma = (1\ 3\ 4)(2\ 6) \in S_6$, entonces escribimos

$$\sigma = 364152.$$

Lema B.20. *Sea $\sigma = x_1 x_2 \cdots x_n \in S_n$, entonces para toda transposición simple s_i, $1 \leq i \leq n-1$ se verifica*

$$\sigma s_i = x_1 \cdots x_{i-1} x_{i+1} x_i x_{i+2} \cdots x_n.$$

Demostración. Escribamos $\tau = x_1 \cdots x_{i-1} x_{i+1} x_i x_{i+2} \cdots x_n$ y sea $m \in \{1, \ldots, n\}$. Si $m \neq i, i+1$, entonces $s_i(m) = m$ y tenemos que

$$\sigma s_i(m) = \sigma(m) = x_m = \tau(m).$$

Si $m = i$, entonces $s_i(m) = i+1$ y por ende

$$\sigma s_i(m) = \sigma(i+1) = x_{i+1} = \tau(i) = \tau(m).$$

Si $m = i+1$, entonces $s_i(m) = i$ y así

$$\sigma s_i(m) = \sigma(i) = x_i = \tau(i+1) = \tau(m).$$

De este modo $\sigma s_i = \tau$, como se deseaba. □

Definición. Sea $\sigma \in S_n$, una *inversión* de σ es un par ordenado (i, j) tal que $1 \leq i < j \leq n$ y $\sigma(i) > \sigma(j)$. Al conjunto de todas las inversiones de σ lo denotamos por $\mathrm{Inv}(\sigma)$, es decir,

$$\mathrm{Inv}(\sigma) = \{(i, j) \mid 1 \leq i <\leq n \text{ y } \sigma(i) > \sigma(j)\}.$$

El *número de inversiones* de σ, denotado por $\mathrm{inv}(\sigma)$, es la cardinalidad del conjunto $\mathrm{Inv}(\sigma)$, es decir

$$\mathrm{inv}(\sigma) = |\mathrm{Inv}(\sigma)|.$$

Lema B.21. *Sea $\sigma \in S_n$ y s_i una transposición simple, con $1 \leq i \leq n-1$. Entonces*

$$\mathrm{inv}(\sigma s_i) = \begin{cases} \mathrm{inv}(\sigma) + 1 & \textit{si } \sigma(i) < \sigma(i+1), \\ \mathrm{inv}(\sigma) - 1 & \textit{si } \sigma(i) > \sigma(i+1). \end{cases}$$

Demostración. Supongamos que $\sigma(i) < \sigma(i+1)$ y escribamos $\sigma = x_1 x_2 \cdots x_{i-1} x_i x_{i+1} x_{i+2} \cdots x_n$. Entonces, por el Lema B.20 tenemos que

$$\sigma s_i = x_1 x_2 \cdots x_{i-1} x_{i+1} x_i x_{i+2} \cdots x_n.$$

Notemos que entonces

$$\mathrm{Inv}(\sigma s_i) = \mathrm{Inv}(\sigma) \sqcup \{(i, i+1)\},$$

de donde $\mathrm{inv}(\sigma s_i) = \mathrm{inv}(\sigma) + 1$. Si en cambio $\sigma(i) > \sigma(i+1)$, tenemos que

$$\mathrm{Inv}(\sigma s_i) = \mathrm{Inv}(\sigma) \setminus \{(i, i+1)\},$$

de donde $\mathrm{inv}(\sigma s_i) = \mathrm{inv}(\sigma) - 1$. □

Teorema B.22. *Para todo $\sigma \in S_n$ tenemos que $\ell(\sigma) = \mathrm{inv}(\sigma)$.*

Demostración. Probaremos primero, por inducción sobre $\ell(\sigma)$, que $\mathrm{inv}(x) \leq \ell(\sigma)$. En efecto, si $\ell(\sigma) = 0$, entonces $\sigma = 1$ y por ende $\mathrm{inv}(\sigma) = 0$, de donde $\mathrm{inv}(\sigma) \leq \ell(\sigma)$.

Supongamos entonces que $\ell(\sigma) = k \geq 1$ y sea $\sigma = s_{i_1} \cdots s_{i_k}$ una expresión reducida para σ. Sea $\sigma' = s_{i_1} \cdots s_{i_{k-1}}$, de modo que $\ell(\sigma') \leq k - 1$ y por hipótesis de inducción tenemos que $\mathrm{inv}(\sigma') \leq \ell(\sigma') \leq k - 1$. Por el Lema B.21 tenemos que

$$\mathrm{inv}(\sigma) = \mathrm{inv}(\sigma' s_{i_k}) = \mathrm{inv}(\sigma') \pm 1 \leq k - 1 \pm 1 \leq k,$$

de donde $\mathrm{inv}(\sigma) \leq \ell(\sigma)$.

Ahora, procederemos por inducción sobre $\mathrm{inv}(\sigma)$ para probar que $\ell(\sigma) \leq \mathrm{inv}(\sigma)$. Si $\mathrm{inv}(\sigma) = 0$, entonces necesariamente $\sigma = 1$ y tenemos que $\ell(\sigma) = 0 \leq \mathrm{inv}(\sigma)$.

Supongamos que $\mathrm{inv}(\sigma) = k \geq 1$, entonces sigma tiene al menos una inversión $(i, i+1)$. Sea $\sigma' = \sigma s_i$, entonces, como $\sigma(i) > \sigma(i+1)$, por el Lema B.21 se sigue que $\mathrm{inv}(\sigma') = \mathrm{inv}(\sigma) - 1 = k - 1$. Por hipótesis de inducción se tiene que $\ell(\sigma') \leq \mathrm{inv}(\sigma')$, y por ende

$$\ell(\sigma) = \ell(\sigma' s_i) \leq \ell(\sigma') + 1 \leq k - 1 + 1 = k,$$

es decir, $\ell(\sigma) \leq \mathrm{inv}(\sigma)$. □