TEMat

# El problema de la palabra en los grupos de trenzas

Javier Aguilar Martín
Universidad de Sevilla (US)
javiecija96@gmail.com

**Resumen:** El problema de la palabra es uno de los problemas más importantes en teoría combinatoria de grupos. En este artículo presentamos una familia de grupos, los grupos de trenzas, donde es posible resolverlo, junto con uno de los algoritmos más eficientes que existen para ello.

**Abstract:** The word problem is one of the most important problems in combinatorial group theory. In this paper we present a family of groups, the braid groups, in which it is possible to solve it, together with one of the most efficient algorithms for that purpose.

**Palabras clave:** trenzas, grupo, problema de la palabra, algoritmo.

**MSC2010:** 20F36.

*Recibido:* 24 de julio de 2019.
*Aceptado:* 20 de noviembre de 2019.

**Agradecimientos:** Quiero agradecer a mis directores de TFG, Juan González-Meneses y Ramón Flores Díaz, por el apoyo y conocimiento aportado, que me permitieron desarrollar el trabajo y extraer de él este artículo.

**Referencia:** Aguilar Martín, Javier. «El problema de la palabra en los grupos de trenzas». En: *TEMat*, 4 (2020), págs. 27-42. ISSN: 2530-9633. URL: https://temat.es/articulo/2020-p27.

# 1. Introducción

El problema de la palabra es uno de los problemas fundamentales de la teoría combinatoria de grupos propuestos por Max Dehn [7]. Este problema consiste en, dado un grupo $G$ con una presentación finita $\langle S \mid R \rangle$ y dados dos elementos $a$ y $b$ de $G$ expresados como productos de los elementos de $S$ y sus inversos, decidir si $a = b$ como elementos del grupo o, equivalentemente, si $ab^{-1} = 1$.

El nombre de este problema proviene de que podemos considerar el alfabeto $\Sigma = S \cup S^{-1}$, donde $S^{-1}$ representa el conjunto formado por los inversos de los elementos de $S$, y ver $G$ como un lenguaje sobre $\Sigma$, en el que dos palabras $a$ y $b$ representarán el mismo elemento si y solo si se puede transformar $a$ en $b$ mediante un número finito de pasos usando las reglas de reescritura proporcionadas por las relaciones de $R$ junto con la cancelación de inversos.

El propio Dehn describió algoritmos para resolver el problema de la palabra en grupos fundamentales de 2-variedades orientables cerradas con género mayor o igual que 2 [8]. Sin embargo, en 1955 Pyotr Novikov encontró ejemplos de grupos finitamente presentados donde el problema de la palabra era indecidible [18], es decir, que no se puede diseñar un algoritmo que lo resuelva. A pesar de esto, hay gran cantidad de grupos donde el problema de la palabra sí es resoluble. Ejemplos claros de ello son los grupos finitos y los grupos libres. Aquí estudiaremos los grupos de trenzas, que aparecen en numerosas ramas de las matemáticas, como el álgebra, la topología, la criptografía y el análisis, y en los cuales el problema de la palabra es resoluble.

En este artículo, basado en el TFG de Javier Aguilar Martín [1], empezamos con algunos preliminares sobre teoría de grupos y topología. A continuación introducimos los grupos de trenzas, destacando los subgrupos de trenzas puras y las presentaciones de dichos grupos. Por último, describimos una estructura en los grupos de trenzas basada en unos monoides incluidos en los grupos. Esta estructura permite resolver el problema de la palabra.

# 2. Preliminares

Dedicaremos esta sección a hablar sobre monoides, explicar qué son las presentaciones de grupos y dar una pequeña introducción a la teoría de homotopía.

## 2.1. Monoides

Empezaremos hablando de monoides, puesto que dentro del grupo de trenzas hay un monoide importante que nos permitirá desarrollar el algoritmo para resolver el problema de la palabra, además de que tendrán relevancia en las presentaciones de grupos.

**Definición 1.** Un **monoide** es un par $(S, *)$, donde $S$ es un conjunto y $* \colon S \times S \to S$ es una operación binaria que satisface las siguientes propiedades:

- Asociatividad, es decir, para cualesquiera $a, b, c \in S$, $(a * b) * c = a * (b * c)$.
- Existencia de elemento neutro, es decir, existe $e \in S$ tal que, para todo $a \in S$, $e * a = a * e = a$.

Habitualmente el símbolo de la operación será omitido y nos referiremos a $S$ como monoide, entendiéndose que en realidad es el par anterior. Un **homomorfismo de monoides** $f \colon S \to T$ es una aplicación que verifica que $f(ab) = f(a)f(b)$ para todo $a, b \in S$. ◂

*Observación* 2. Un monoide es análogo a un grupo, pero sin requerir la existencia de elementos inversos, esto es, no exigimos que para todo $s \in S$ exista $s^{-1} \in S$ tal que $ss^{-1} = s^{-1}s = e$. ◂

**Ejemplo 3.** En el contexto de los lenguajes formales es habitual llamar **alfabeto** a cualquier conjunto finito $X$. Esto es porque podemos considerar el monoide de palabras en este conjunto. Por ejemplo, sea $X = \{a, b\}$. El **lenguaje** generado por $X$ se denota $X^*$ y se corresponde con todas las **palabras** (cadenas de texto) formadas con las letras $a$ y $b$, así como la palabra vacía $\varepsilon$. La operación que dota de estructura de monoide al lenguaje es la concatenación. ◂

## 2.2. Presentaciones de grupos

**Definición 4.** Sea $X$ un conjunto, $L$ un grupo e $i\colon X \to L$ una función. Diremos que $(L,i)$ es **libre** en $X$ si para todo grupo $H$ y toda función $f\colon X \to H$ existe un único homomorfismo $\varphi\colon L \to H$ de modo que el siguiente diagrama conmuta.

$$\begin{array}{ccc} X & \xrightarrow{f} & H \\ {\scriptstyle i}\downarrow & \nearrow_{\exists!\varphi} & \\ L & & \end{array}$$

◂

*Observación* 5. Sea $H = \langle Y\rangle$ un grupo. Sea $X$ un conjunto con $|X| > |Y|$ y $(L,i)$ un grupo libre en $X$. Como $|X| > |Y|$, podemos tomar $f\colon X \to H$ tal que $Y \subseteq f(X)$. Entonces, existe $\varphi\colon L \to H$ homomorfismo sobreyectivo y tenemos que $H \cong L/\ker\varphi$. ◂

**Definición 6.** Una **presentación** de $H$ es un grupo libre $(L,i)$ y un subgrupo $N \trianglelefteq L$ tal que $L/N \cong H$. ◂

**Teorema 7** ([2, §II.5]). *Dado un conjunto $X$, existe $(L,i)$ libre en $X$.*

*Demostración.* Sea $X^{-1}$ un conjunto en biyección con $X$ mediante $x \mapsto x^{-1}$. Por abuso de notación, a la inversa también la denotamos $x \mapsto x^{-1}$. Sea $(X \cup X^{-1})^*$ el monoide de palabras en $X \cup X^{-1}$ con la concatenación. Decimos que $w = y_1 \cdots y_n \in (X \cup X^{-1})^*$ es **reducida** si para todo $1 \leq i \leq n-1$ tenemos que $y_i \neq y_{i+1}^{-1}$. Si $w$ no es reducida, entonces $w' = y_1 \cdots y_{i-1} y_{i+2} \cdots y_n$ se ha obtenido a través de una **reducción elemental** y escribimos $w \to w'$.

Dos palabras son equivalentes si se puede obtener una a partir de la otra mediante reducciones elementales o mediante el proceso inverso de introducir un par de la forma $y_i y_i^{-1}$. Es fácil comprobar que esta relación entre palabras es una relación de equivalencia.

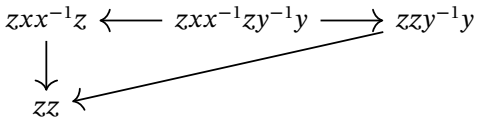



**Figura 1:** Palabras equivalentes.

Entonces se tiene que $F(X) = (X \cup X^{-1})^*/\sim$, siendo $\sim$ la relación de equivalencia anterior, es un grupo libre en $X$ y existe una única palabra reducida en cada clase de equivalencia. Para la segunda afirmación, ver el libro de Lyndon y Schupp [15, Capítulo 1, §1]. Para la primera tenemos que probar dos cosas: que $F(X)$ es un grupo y que es libre. La propiedad asociativa y la existencia de elemento neutro se heredan del monoide $(X \cup X^{-1})^*$. Dado un elemento representado por una palabra reducida $w = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}$, es inmediato comprobar que el inverso está representado por la palabra $w^{-1} = y_n^{-\varepsilon_n} \cdots y_1^{-\varepsilon_1}$.

Probamos a continuación que $F(X)$ es libre. Consideramos $i\colon X \to F(X)$ la aplicación que envía cada elemento a su clase de equivalencia (los elementos de $X$, de hecho, son palabras reducidas). Sean $G$ un grupo y $f\colon X \to G$ una función. Definimos $\varphi\colon F(X) \to G$ a partir de las palabras reducidas como $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n} \mapsto f(x_{i_1})^{\varepsilon_1} \cdots f(x_{i_n})^{\varepsilon_n}$. Cualquier homomorfismo de $F(X) \to G$ que haga que el diagrama conmute debe cumplir esa definición, luego es único. ∎

*Observación* 8. El grupo libre en $X$ es único salvo isomorfismo, esto es, si $(L_1,i_1)$ y $(L_2,i_2)$ son libres en $X$, entonces $L_1 \cong L_2$. ◂

Volvemos a las presentaciones. Dado $X$, el grupo libre en $X$ existe y es único salvo isomorfismo. Lo denotamos $\langle X \mid \rangle$.

Sea $G$ un grupo. Dado $R \subseteq G$, $\langle R^G\rangle$ denota el subgrupo generado por todos los $G$-conjugados de $R$, que coincide con el menor subgrupo normal que contiene a $R$:

$$\bigcap_{N \trianglelefteq G, R \subseteq N} N.$$

Dado un conjunto $X$ y $R \subseteq \langle X \mid \rangle$, denotamos por $\langle X \mid R \rangle$ al grupo $\langle X \mid \rangle / \langle R^{\langle X \mid \rangle} \rangle$. Por lo visto anteriormente, para todo grupo $G$ existen un conjunto $X$ y $R \subseteq \langle X \mid \rangle$ tales que $\langle X \mid R \rangle \cong G$.

**Ejemplo 9**.

1. Para $n \geq 1$, consideremos la presentación $\langle x \mid x^n \rangle$. Este es el grupo generado por un elemento de orden $n$, por lo que este grupo es isomorfo al grupo cíclico aditivo $\mathbb{Z}/n\mathbb{Z}$. A menudo, las relaciones se escriben como ecuaciones, de modo que esta presentación podría haberse escrito como $\langle x \mid x^n = 1 \rangle$.
2. La presentación del grupo libre abeliano de rango $n$, $\mathbb{Z}^n$, está dada por $\langle x_1, \dots, x_n \mid [x_i, x_j] = 1 \rangle$, donde $[x_i, x_j] = x_i x_j x_i^{-1} x_j^{-1}$ es el conmutador de los elementos $x_i$ y $x_j$. Es decir, la presentación expresa que el grupo está generado por $n$ elementos que conmutan entre sí y ninguna relación más, por lo que efectivamente es el grupo libre abeliano de rango $n$. Escribiendo las relaciones como ecuaciones podemos también despejar y escribir la presentación anterior como $\langle x_1, \dots, x_n \mid x_i x_j = x_j x_i \rangle$. ◂

## 2.3. Transformaciones de Tietze

Vamos a concentrarnos a partir de ahora en presentaciones **finitas**, es decir, tanto $X$ como $R$ serán conjuntos finitos. Se conocen como **transformaciones de Tietze** los siguientes isomorfismos:

1. Si $s \in \langle R^{\langle X \mid \rangle} \rangle$, entonces $\langle X \mid R \rangle \cong \langle X \mid R \cup \{s\} \rangle$.
2. Si $y \notin X$ y $u \in \langle X \mid \rangle$, entonces $\langle X \mid R \rangle \cong \langle X \cup \{y\} \mid R \cup \{yu\} \rangle$.

**Teorema 10** ([15, Capítulo 2, Proposición 2.1]). *Si $\langle X \mid R \rangle \cong \langle X \mid R' \rangle$ son presentaciones finitas, entonces se puede obtener una presentación de la otra mediante una sucesión finita de transformaciones de Tietze.*

Volviendo al problema de la palabra, sean $\langle X \mid R \rangle$ una presentación finita de un grupo $G$ y $w \in (X \cup X^{-1})^*$. Entonces, $w =_G 1$ si y solo si $w \in \langle R^{\langle X \mid \rangle} \rangle$ si y solo si $w = \prod_{i=1}^{M} p_i r_i^{\varepsilon_i} p_i^{-1}$ en $\langle X \mid \rangle$ para algún $M \in \mathbb{N}$, algunos $r_i \in R$ y algunos $p_i \in \langle X \mid \rangle$, con $i \in \{1, \dots, M\}$ y $\varepsilon_i = \pm 1$.

## 2.4. Relación entre monoides y grupos

De forma análoga a como se hace para grupos, podemos considerar los generadores de un monoide y una presentación de un monoide mediante generadores y relaciones. También se definen de forma análoga los morfismos entre monoides. De hecho, la definición de monoide libre es análoga a la de grupos, siendo el monoide libre en un conjunto $X$ el lenguaje generado por este conjunto.

**Definición 11**. Dado un monoide $S$ con presentación $\langle M \mid R \rangle$, su **grupo de fracciones** $G(S)$ es el grupo con presentación $\langle M \mid R \rangle$. ◂

Existe una aplicación natural de un monoide en su grupo de fracciones. Sin embargo, esta aplicación no siempre es inyectiva, pues la existencia de inverso en el grupo puede hacer que dos elementos distintos del monoide representen el mismo elemento del grupo de fracciones. Por ejemplo, si consideramos la presentación $\langle a, b, c \mid ab = cb \rangle$, los elementos $a$ y $c$ son distintos en el monoide; sin embargo, en el grupo son el mismo, pues multiplicando a la derecha por $b^{-1}$ en la relación obtenemos $a = c$. De aquí que consideremos la siguiente definición.

**Definición 12**. Decimos que un monoide $S$ se **inyecta** en su grupo de fracciones $G(S)$ si el morfismo de monoides $\iota \colon S \to G(S)$ dado por $\iota(a) = a$ es inyectivo. ◂

**Definición 13**. Decimos que un monoide $S$ satisface las **condiciones de Ore** [19] si se cumple lo siguiente:

- $S$ es cancelativo, es decir, $xay = xby$ implica $a = b$ para todo $x, y, a, b \in S$.
- Para todo $a, b \in S$ existen $a', b' \in S$ tales que $aa' = bb'$ (existe un múltiplo común). ◂

**Proposición 14** ([6, Teorema 1.23]). *Si un monoide satisface las condiciones de Ore, entonces se inyecta en su grupo de fracciones.*

## 2.5. Teoría de homotopía

Para definir algunos conceptos necesitaremos ciertas nociones básicas de teoría de homotopía que procedemos a enunciar.

**Definición 15.** Sean $f, g : X \to Y$ funciones continuas y sea $I = [0,1]$. Decimos que $f$ y $g$ son **homotópicas**, denotado $f \simeq g$, si existe $H : X \times I \to Y$ continua tal que $H(x,0) = f(x)$ y $H(x,1) = g(x)$. A la aplicación $H$ la llamamos **homotopía** entre $f$ y $g$. Si $A \subseteq X$, decimos que $f$ y $g$ son **homotópicas relativamente** a $A$ si la homotopía $H$ cumple además que $H(a,t) = f(a) = g(a)$ para todo $a \in A$. Si $A$ es un conjunto unitario, hablamos de **homotopía basada**. ◂

**Lema 16.** *Ser homotópicas es una relación de equivalencia (también serlo relativamente).*

*Demostración.* Vamos a demostrar que la relación de homotopía es reflexiva, simétrica y transitiva.

- Reflexiva: $f \simeq f$ mediante $H(x,t) = f(x)$.
- Simétrica: si $f \simeq g$ mediante $H$, entonces $g \simeq f$ mediante $\widetilde{H}(x,t) = H(x,1-t)$. Se cumple que

$$\widetilde{H}(x,0) = H(x,1) = g(x),$$
$$\widetilde{H}(x,1) = H(x,0) = f(x).$$

  Es inmediato probar que $\widetilde{H}$ es continua.
- Transitiva: sea $f \simeq g$ mediante $F$ y $g \simeq h$ mediante $G$. Entonces, $f \simeq h$ mediante

$$H(x,t) = \begin{cases} F(x,2t) & \text{si } 0 \le t \le 1/2, \\ G(x,2t-1) & \text{si } 1/2 \le t \le 1, \end{cases} \Longrightarrow \begin{cases} H(x,0) = F(x,0) = f(x), \\ H(x,1) = G(x,1) = h(x). \end{cases}$$

  Está bien definida en $t = 1/2$ pues $F(x,1) = g(x) = G(x,0)$. Es inmediato probar la continuidad de $H$ y adaptar la demostración al caso relativo. ∎

## 2.6. Caminos

**Definición 17.** Dado un espacio topológico $X$, un **camino** entre $x$ e $y$ pertenecientes a $X$ es una aplicación continua $\alpha : I \to X$ tal que $\alpha(0) = x$ y $\alpha(1) = y$, siendo $I = [0,1]$. ◂

**Definición 18.** Dados $\alpha, \beta : I \to X$ dos caminos con $\alpha(0) = x, \alpha(1) = \beta(0) = y, \beta(1) = z$, se llama **concatenación** de $\alpha$ y $\beta$ al camino definido como

$$\alpha\beta(t) = \begin{cases} \alpha(2t) & \text{si } 0 \le t \le 1/2, \\ \beta(2t-1) & \text{si } 1/2 \le t \le 1. \end{cases}$$ ◂

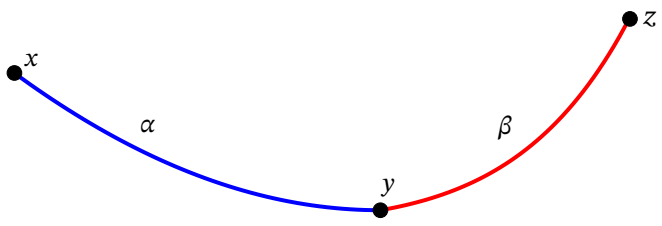



**Figura 2:** La concatenación $\alpha\beta$ es el camino resultante desde $x$ hasta $z$.

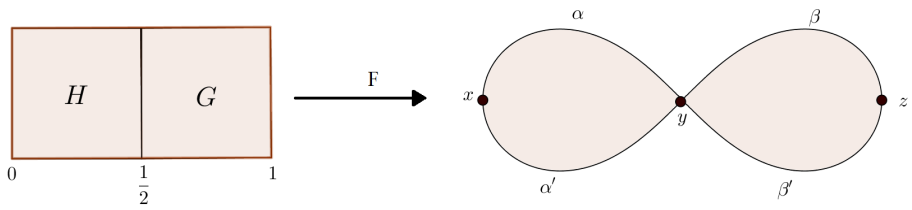
*Nota* 19. Si $\alpha$ y $\beta$ son caminos homotópicos relativamente a $\{0,1\}$, decimos que son **equivalentes** y escribimos $\alpha \sim \beta$ en lugar de $\alpha \simeq \beta$ relativamente a $\{0,1\}$. ◂

**Lema 20.** *La concatenación es compatible con la equivalencia de caminos, esto es, si $\alpha \sim \alpha'$ y $\beta \sim \beta'$, entonces $\alpha\beta \sim \alpha'\beta'$.*

*Demostración.* Sean $\alpha \sim \alpha'$ y $\beta \sim \beta'$ caminos con $\alpha(0) = \alpha'(0) = x$, $\alpha(1) = \alpha'(1) = \beta(0) = \beta'(0) = y$ y $\beta(1) = \beta'(1) = z$. Como $\alpha \sim \alpha'$, existe una homotopía $H$ entre $\alpha$ y $\alpha'$ relativa a $\{0,1\}$. Como $\beta \sim \beta'$, existe una homotopía $G$ entre $\beta$ y $\beta'$ relativa a $\{0,1\}$.

Sea $F\colon I \times I \to X$ la homotopía resultante de «unir» las dos anteriores,

$$F(t,s) = \begin{cases} H(2t,s) & \text{si } 0 \le t \le 1/2, \\ G(2t-1,s) & \text{si } 1/2 \le t \le 1. \end{cases}$$




$F(1/2,s)$ está bien definida pues, al ser $H$ y $G$ relativas a $\{0,1\}$, se tiene que $H(1,s) = y = G(0,s)$. Tenemos que

$$F(t,0) = \begin{cases} H(2t,0) = \alpha(2t) & \text{si } 0 \le t \le 1/2, \\ G(2t-1,0) = \beta(2t-1) & \text{si } 1/2 \le t \le 1, \end{cases}$$

que es justamente la concatenación de $\alpha$ y $\beta$. Análogamente, $F(t,1) = (\alpha'\beta')(t)$. Finalmente,

$$\left.\begin{array}{l} F(0,s) = H(0,s) = x \\ F(1,s) = G(1,s) = z \end{array}\right\} \implies \alpha\beta \sim \alpha'\beta'. \qquad \blacksquare$$

**Proposición 21.** *Se cumplen las siguientes propiedades de la concatenación con respecto a la equivalencia de caminos:*

1. *Propiedad asociativa:* $(\alpha\beta)\gamma \sim \alpha(\beta\gamma)$.
2. *Elemento neutro: si $c_x$ es el camino constante $x$ y $\alpha$ es un camino entre $x$ e $y$, entonces $c_x\alpha \sim \alpha \sim \alpha c_y$.*
3. *Elemento inverso: si $\alpha$ es un camino entre $x$ e $y$ y $\overline{\alpha}\colon I \to X$ es el camino $\overline{\alpha}(t) = \alpha(1-t)$ (camino opuesto), entonces $\alpha\overline{\alpha} \sim c_x$ y $\overline{\alpha}\alpha \sim c_y$.*

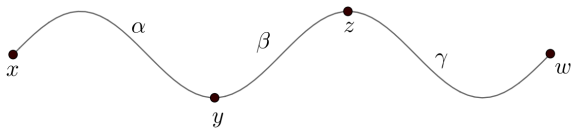



**Figura 3:** La triple concatenación está bien definida salvo homotopía.

*Demostración.*

1. Por definición, tenemos por un lado que

$$\alpha(\beta\gamma)(t) = \begin{cases} \alpha(2t) & \text{si } 0 \le t \le 1/2, \\ \beta\gamma(2t-1) & \text{si } 1/2 \le t \le 1, \end{cases} = \begin{cases} \alpha(2t) & \text{si } 0 \le t \le 1/2, \\ \beta(4t-2) & \text{si } 1/2 \le t \le 3/4, \\ \gamma(4t-3) & \text{si } 3/4 \le t \le 1. \end{cases}$$

   Por otro lado,

$$(\alpha\beta)\gamma(t) = \begin{cases} (\alpha\beta)(2t) & \text{si } 0 \le t \le 1/2, \\ \gamma(2t-1) & \text{si } 1/2 \le t \le 1, \end{cases} = \begin{cases} \alpha(4t) & \text{si } 0 \le t \le 1/4, \\ \beta(4t-1) & \text{si } 1/4 \le t \le 1/2, \\ \gamma(2t-1) & \text{si } 1/2 \le t \le 1. \end{cases}$$

Sea, por lo tanto,

$$F(t,s)=\begin{cases}\alpha\left(\dfrac{4t}{s+1}\right) & \text{si } 0\le t\le \dfrac{s+1}{4},\\ \beta\left(4t-(s+1)\right) & \text{si } \dfrac{s+1}{4}\le t\le \dfrac{s+2}{4},\\ \gamma\left(\dfrac{4t-s-2}{2-s}\right) & \text{si } \dfrac{s+2}{4}\le t\le 1.\end{cases}$$

Se tiene que $F$ es una homotopía relativa a $\{0,1\}$ entre $F(t,0)=(\alpha\beta)\gamma(t)$ y $F(t,1)=\alpha(\beta\gamma)(t)$.

2. Para probar que $c_x\alpha\sim\alpha$ definimos la homotopía

$$F(t,s)=\begin{cases}x & \text{si } 0\le t\le \dfrac{1-s}{2},\\ \alpha\left(\dfrac{2t+s-1}{s+1}\right) & \text{si } \dfrac{1-s}{2}\le t\le 1.\end{cases}$$

La relación $\alpha\sim\alpha c_y$ se demuestra de manera análoga.

3. Se tiene que

$$\alpha\overline{\alpha}(t)=\begin{cases}\alpha(2t) & \text{si } 0\le t\le 1/2,\\ \overline{\alpha}(2t-1)=\alpha(2-2t) & \text{si } 1/2\le t\le 1\end{cases}$$

define una homotopía relativa a $\{0,1\}$ entre $\alpha\overline{\alpha}$ y $c_x$. Análogamente, se puede encontrar una homotopía relativa a $\{0,1\}$ entre $\overline{\alpha}\alpha$ y $c_y$. ∎

# 3. Grupos de trenzas

Aunque el término *grupo de trenzas* fue acuñado por Artin [3] en 1925, estos grupos ya fueron considerados por Hurwitz [14] en 1891 como lo que en terminología moderna se llamaría «grupo fundamental de espacios de configuración de $n$ puntos en el plano complejo». En 1935, Magnus [16] consideró el mismo grupo desde el punto de vista de los *mapping class groups*. Markoff [17] dio una aproximación totalmente algebraica.

Esta variedad de definiciones permite estudiar los grupos de trenzas desde perspectivas muy distintas, lo cual aporta una gran riqueza a la teoría. Aquí veremos la definición más geométrica y mundana, además de su presentación, que también puede tomarse como definición algebraica del grupo.

## 3.1. Trenzas como colección de cuerdas

Empezamos dando la definición más gráfica e intuitiva, consistente en visualizar las trenzas como cuerdas que se entrelazan.

**Definición 22.** Sea $n\ge 1$ un entero. Denotemos $\Sigma_n$ al grupo simétrico sobre $n$ elementos. Sean $n$ puntos $P_1,\dots,P_n$ en $\mathbb{C}$ (se puede suponer que $P_k=k$ para todo $1\le k\le n$). Se define una **trenza geométrica de $n$ cuerdas** como una $n$-upla $\beta=(\beta_1,\dots,\beta_n)$ de caminos $\beta_k\colon [0,1]\to\mathbb{C}\times[0,1]$ tal que

- $\beta_k(t)=(\alpha_k(t),t)$, donde $\alpha_k(0)=P_k$ para todo $1\le k\le n$,
- existe una permutación $\tau=\tau(\beta)\in\Sigma_n$ tal que $\alpha_k(1)=P_{\tau(k)}$ para todo $1\le k\le n$, llamada **permutación inducida por** $\beta$, y
- $\alpha_k(t)\ne\alpha_\ell(t)$ para todo $k\ne\ell$ y para todo $t\in[0,1]$.

Si la permutación inducida por $\beta$ es el elemento neutro de $\Sigma_n$, es decir, si $\beta_k(1)=(P_k,1)$ para todo $1\le k\le n$, entonces decimos que la trenza geométrica es **pura**.

Dos trenzas geométricas $\alpha$ y $\beta$ se dicen **homotópicas** si existe una familia continua de trenzas $\{\gamma_s\}_{s\in[0,1]}$ de modo que $\gamma_0=\alpha$ y $\gamma_1=\beta$. Es decir, dos trenzas geométricas son homotópicas si son homotópicas como colección de caminos relativamente a los puntos extremos. Consideraremos que dos trenzas geométricas son la misma si son homotópicas, y a la clase de homotopía de una trenza geométrica de $n$ cuerdas la

llamaremos **trenza de $n$ cuerdas**. Nótese que, si $\alpha$ y $\beta$ son homotópicas, entonces $\tau(\alpha) = \tau(\beta)$, así que diremos que una trenza es **pura** si los elementos de su clase de homotopía son trenzas geométricas puras. ◂

La forma de un dibujo tridimensional de una trenza geométrica se puede observar en la figura 4.

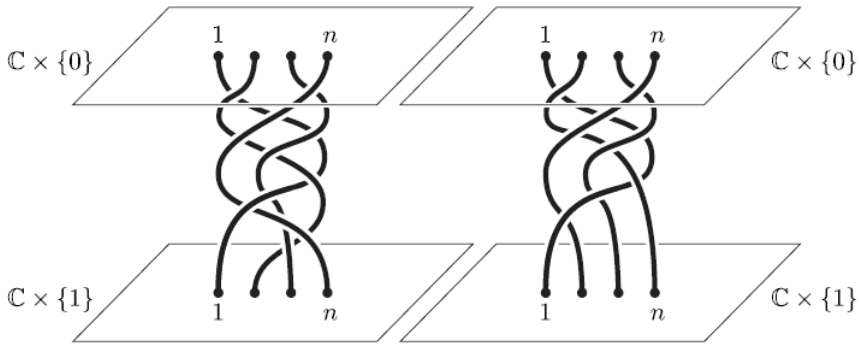



**Figura 4:** Una trenza geométrica pura y una trenza geométrica no pura.

*Observación* 23. Para cada $t \in [0,1]$, el plano $\mathbb{C} \times \{t\}$ es atravesado una sola vez por cada cuerda de la trenza. ◂

Normalmente, se representan las trenzas como su proyección en $\mathbb{R} \times [0,1]$ (posiblemente seguida de una rotación de 90°, ver figura 7). Los puntos en los que la proyección de dos cuerdas coincida los representaremos como en la figura 5 para conservar la información de cuál cruzaba originalmente por encima. Salvo homotopía, podemos suponer que la proyección tiene un número finito de puntos de cruce, en los cuales solo intervienen dos cuerdas. Además, podemos suponer también que los cruces ocurren a distintas alturas, es decir, para distintos valores de $t \in [0,1]$. En la figura 7 se ilustra la proyección de la trenza no pura de la figura 4.

**Figura 5:** Cruce positivo y cruce negativo, respectivamente.

**Definición 24.** Se definen los **generadores estándar** o **generadores de Artin** como las trenzas $\sigma_i$ con $1 \leq i \leq n-1$ indicadas en la figura 6. ◂

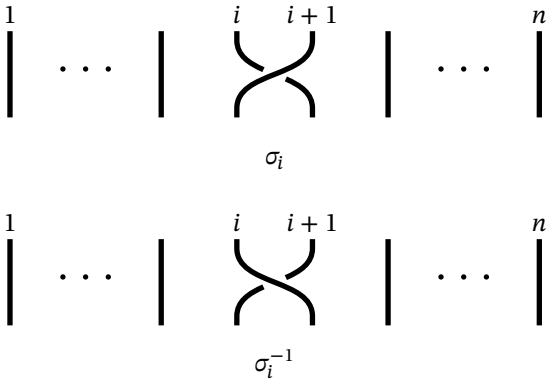



**Figura 6:** Generador de Artin y su inverso.

A partir de las observaciones anteriores, está claro que cualquier trenza se puede construir como concatenación de los generadores de Artin.

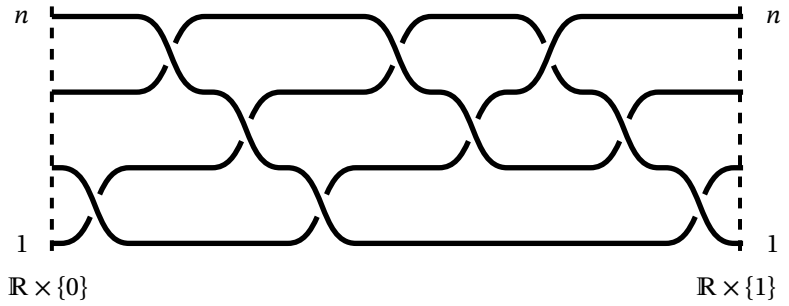



**Figura 7:** Ejemplo de representación plana.

## 3.2. Estructura de grupo

Una de las características más importantes del conjunto de clases de homotopía de trenzas es que puede dotarse de estructura de grupo para cada $n$. Para ello, definiremos el producto de trenzas.

**Definición 25.** El producto de dos trenzas $\alpha = (\alpha_1, \dots, \alpha_n)$ y $\beta = (\beta_1, \dots, \beta_n)$ se define como la trenza

$$\alpha \cdot \beta = (\alpha_1 \beta_{\tau(1)}, \dots, \alpha_n \beta_{\tau(n)}),$$

donde $\tau = \tau(\alpha)$. Es decir, el producto de dos trenzas en el mismo número de cuerdas es su concatenación, en la cual se recorre en primer lugar $\alpha$ y después $\beta$. En la figura 8 se ilustra un ejemplo. En ocasiones omitiremos el punto y escribiremos simplemente $\alpha\beta$. Asimismo, denotaremos $\alpha^n = \underbrace{\alpha \cdots \alpha}_{n \text{ veces}}$. ◂

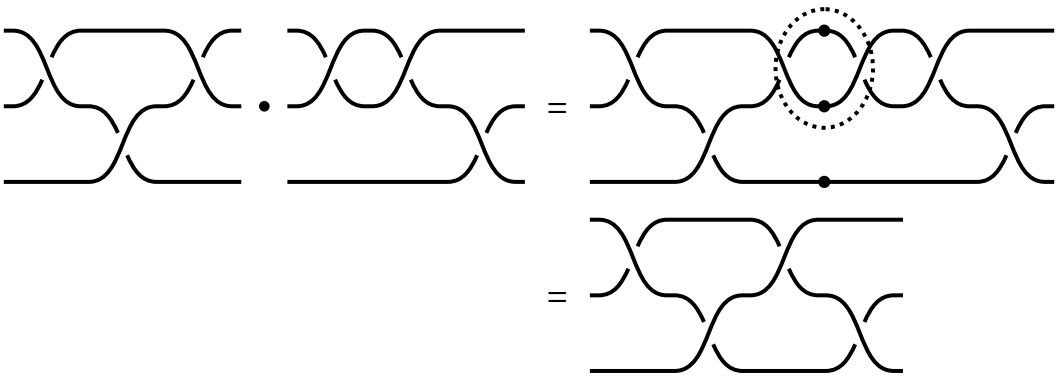


**Figura 8:** Producto de dos trenzas.

Denotemos $B_n$ al conjunto de clases de homotopía de trenzas de $n$ cuerdas y $PB_n$ al conjunto de clases de homotopía de trenzas puras de $n$ cuerdas. Es evidente que la multiplicación anterior induce una operación en $B_n$ (y por tanto en $PB_n$); es más, se tiene el siguiente resultado.

**Proposición 26.** *El conjunto $B_n$ dotado de esta operación tiene estructura de grupo. El resultado también es cierto para $PB_n$.*

Al grupo $B_n$ se le llama **grupo de trenzas de *n* cuerdas** y a $PB_n$ se le llama **grupo de trenzas puras de *n* cuerdas**.

*Demostración de la proposición 26.* Sean $\alpha$ y $\beta$ dos trenzas con representantes $a = (a_1, \dots, a_n)$ y $b = (b_1, \dots, b_n)$, respectivamente. En primer lugar, veamos que la operación está bien definida, es decir, que $a \cdot b$ es una trenza geométrica y, por tanto, podemos definir $\alpha\beta = [a \cdot b]$. Sea $\tau = \tau(a)$ la permutación inducida por $a$. Como $a_k b_{\tau(k)}(0) = a_k(0) = (P_k, 0)$ para todo $1 \leq k \leq n$, se cumple la primera propiedad de la definición 22. Para la segunda, basta observar que la nueva permutación es $\tau(a \cdot b) = \tau(b) \circ \tau(a)$. En particular, si $a$ y $b$ son puras, entonces la permutación inducida por el producto también es la identidad, por lo que el producto es una trenza pura. Por último, si $t \in [0, 1/2]$, entonces $a_k \beta_{\tau(k)} = a_k(2t)$, y si $t \in [1/2, 1]$, $\alpha_k \beta_{\tau(k)} = \beta_{\tau(k)}(2t-1)$ para todo $1 \leq k \leq n$, por lo que se tiene claramente la tercera propiedad.

Por otra parte, si $a'$ y $b'$ son otros representantes de $\alpha$ y $\beta$, respectivamente, se tiene que $[a' \cdot b'] = [a \cdot b]$ por las propiedades de la homotopía de caminos con respecto a la concatenación.

Veamos ahora la estructura de grupo. Tenemos que probar que la operación es asociativa, pero esto se deduce de que la concatenación de caminos es asociativa salvo homotopía. Tenemos claramente que la identidad es la trenza constante representada por $\mathrm{Id} = (\mathrm{Id}_1, \dots, \mathrm{Id}_n)$, donde $\mathrm{Id}_k$ denota el camino $(P_k, t)$ para $t \in [0, 1]$ y para $1 \leq k \leq n$. Finalmente, dada $\alpha = [(a_1, \dots, a_n)]$ con permutación inducida $\tau$, se tiene que $\alpha^{-1} = [(\overline{a}_{\tau^{-1}(1)}, \dots, \overline{a}_{\tau^{-1}(n)})]$, donde $\overline{a}_k$ denota el camino que es opuesto a $a_k$ en la primera coordenada y que es idéntico a $a_k$ en la segunda coordenada.

En efecto, usando las propiedades de homotopía de caminos con respecto al camino opuesto tenemos que

$$\alpha\alpha^{-1} = [(a_1, \dots, a_n) \cdot (\overline{a}_{\tau^{-1}(1)}, \dots, \overline{a}_{\tau^{-1}(n)})] = [(a_1 \overline{a}_{\tau(\tau^{-1}(1))}, \dots, a_n \overline{a}_{\tau(\tau^{-1}(n))})] = [\mathrm{Id}].$$

Análogamente se prueba que $\alpha^{-1}\alpha = [\mathrm{Id}]$. ∎

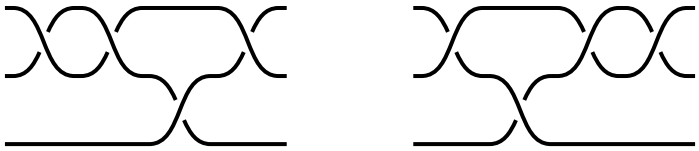



**Figura 9:** Una trenza y su inversa.

## 3.3. Presentación del grupo

Una de las características mejor conocidas de los grupos de trenzas es su presentación finita descubierta por Artin [4]. Ya hemos mencionado los generadores $\sigma_1, \dots, \sigma_{n-1} \in B_n$ en la definición 24. La presentación completa sería la siguiente:

(1)
$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i, & |i-j| > 1 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & |i-j| = 1 \end{array} \right\rangle.$$

La prueba de la completitud de esta presentación puede encontrarse en el artículo de Magnus [16].

Vamos a dar también la presentación del grupo de trenzas puras, en concreto la dada por Birman [5] (ver también el artículo de González-Meneses y Silvero [13]), pues nos será más útil para probar ciertos resultados. La presentación original fue dada por Artin [4]. Así pues, definimos los **generadores de Birman**

(2)
$$A_{ij} = \sigma_{j-1} \dots \sigma_{i+1} \sigma_i^2 \sigma_{i+1}^{-1} \dots \sigma_{j-1}^{-1} \; (1 \leq i < j \leq n)$$

y las relaciones

$$\begin{aligned}
A_{ij}^{-1} A_{rs} A_{ij} &= A_{rs} && (i < j < r < s) \text{ o bien } (r+1 < i < j < s), \\
A_{ij}^{-1} A_{js} A_{ij} &= A_{is} A_{js} A_{is}^{-1} && (i < j < s), \\
A_{ij}^{-1} A_{is} A_{ij} &= A_{is} A_{js} A_{is} A_{js}^{-1} A_{is}^{-1} && (i < j < s), \\
A_{ij}^{-1} A_{rs} A_{ij} &= A_{is} A_{js} A_{is}^{-1} A_{js}^{-1} A_{rs} A_{js} A_{is} A_{js}^{-1} A_{is}^{-1} && (i+1 < r < j < s).
\end{aligned}$$

En la figura 10 se puede observar qué trenza representa geométricamente el generador $A_{ij}$.

*Nota* 27. Cuando $j = i+1$, $A_{ij} = \sigma_i^2$. ◂

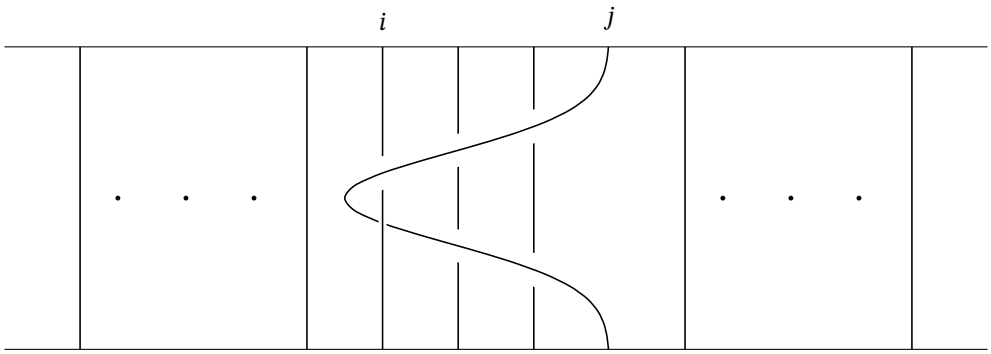



**Figura 10:** Interpretación geométrica de la trenza $A_{ij}$.

# 4. Algoritmo de Garside

El objetivo de esta sección es proporcionar una *forma normal* para las trenzas, es decir, una forma «estándar» de escribirlas, de modo que para ver si dos palabras representan la misma trenza sea suficiente calcular sus formas normales y comprobar si son iguales. Para llegar hasta esa forma normal estudiaremos la *estructura de Garside* del grupo de trenzas, para lo cual seguiremos la referencia «The braid group and other groups» [12]. Los resultados referentes a *Word Processing in Groups* [11] se pueden encontrar en el capítulo 9 de dicho libro.

## 4.1. Formas normales

Obsérvese que la presentación (1) solo involucra potencias positivas de los generadores. Por tanto, se puede considerar el monoide $B_n^+$ determinado por esa misma presentación. Los elementos de $B_n^+$ son palabras en $\sigma_1, \dots, \sigma_{n-1}$ (pero no sus inversos), y dos palabras son equivalentes si y solo si una puede obtenerse de la otra reemplazando reiteradamente subpalabras de la forma $\sigma_i\sigma_j$ con $|i-j|>1$ (respectivamente, $\sigma_i\sigma_j\sigma_i$ con $|i-j|=1$) por $\sigma_j\sigma_i$ (respectivamente, $\sigma_j\sigma_i\sigma_j$).

**Definición 28.** El monoide $B_n^+$ se denomina **monoide de las trenzas positivas** y sus palabras son llamadas **trenzas positivas**. ◂

En el monoide $B_n^+$ hay un orden parcial natural.

**Definición 29.** Definimos en $B_n^+$ el orden parcial $\preccurlyeq$ tal que, dadas $a, b \in B_n^+$, $a \preccurlyeq b$ si $ac = b$ para alguna $c \in B_n^+$. Decimos en ese caso que $a$ es un **prefijo** de $b$. Escribimos $a \prec b$ si $c$ no es trivial. Si además $a \neq 1$, decimos que $a$ es un **prefijo propio** de $b$. ◂

Antes de continuar debemos probar que la relación que hemos definido es realmente un orden parcial.

**Lema 30.** *La relación $\preccurlyeq$ es una relación de orden.*

*Demostración.* Dada $x \in B_n^+$, se tiene que $x \preccurlyeq x \cdot 1 = x$, por lo que se cumple la propiedad reflexiva. Si $x, y \in B_n^+$ con $x \preccurlyeq y$ e $y \preccurlyeq x$, entonces tenemos que $y = xa$ y $x = yb$ para algunos $a, b \in B_n^+$, así que $y = yba$. Como en el monoide de trenzas positivas las relaciones son homogéneas, la longitud de las palabras dentro de una clase de equivalencia es constante , pero $\text{long}(yab) = \text{long}(y) + \text{long}(a) + \text{long}(b)$, por lo que tenemos necesariamente que $a = b = 1$, de donde $x = y$, cumpliéndose la propiedad antisimétrica. Por último, supongamos que $x \preccurlyeq y \preccurlyeq z$ para ciertas $x, y, z \in B_n^+$. Entonces $y = xa$ y $z = yb$ para $a, b \in B_n^+$. Sustituyendo, $z = xab$, por lo que $x \preccurlyeq z$, lo que prueba la propiedad transitiva. ∎

Nótese que $\preccurlyeq$ es invariante por multiplicación a izquierda, esto es, $a \preccurlyeq b$ implica $xa \preccurlyeq xb$ para todo $a, b, x \in B_n^+$.

Dado tal orden parcial, uno podría preguntarse si existe un único máximo común divisor o mínimo común múltiplo con respecto a $\preccurlyeq$. Esto es, dadas $a, b \in B_n^+$, ¿existe un único $d \in B_n^+$ tal que $d \preccurlyeq a$, $d \preccurlyeq b$ y $d' \preccurlyeq d$ para todo $d'$ prefijo común de $a$ y $b$? ¿Y existe un único $m \in B_n^+$ tal que $a \preccurlyeq m$, $b \preccurlyeq m$ y $m \preccurlyeq m'$ para todo $m'$ que tenga a $a$ y a $b$ como prefijos? En tales casos, escribimos $d = a \wedge b$ y $m = a \vee b$. Nótese que también tendríamos $xd = xa \wedge xb$ y $xm = xa \vee xb$ para todo $x \in B_n^+$.

*Nota* 31. Análogamente podríamos definir el orden parcial de **sufijos**, $\succcurlyeq$, invariante por multiplicación a derecha. Nótese que este orden no es equivalente al de prefijos, puesto que $b \succcurlyeq a$ no implica en general $a \preccurlyeq b$ ni recíprocamente. Por ejemplo, $\sigma_1 \preccurlyeq \sigma_1\sigma_2$, pero claramente $\sigma_1\sigma_2 \not\succcurlyeq \sigma_1$. ◂

**Proposición 32** ([12, Teorema 1.2]). *El mínimo común múltiplo de los generadores $\sigma_i$ y $\sigma_j$ viene dado por*

$$\sigma_i \vee \sigma_j = \begin{cases} \sigma_i\sigma_j & si\ |i-j| > 1, \\ \sigma_i\sigma_j\sigma_i & si\ |i-j| = 1. \end{cases}$$

En la prueba original se prueba también que $B_n^+$ es cancelativo, es decir, $xay = xby$ implica $a = b$ para todo $a, b, x, y \in B_n^+$. Este resultado permite probar que todo par de elementos de $B_n^+$ tiene un único mínimo común múltiplo y un único máximo común divisor, tal como hace Dehornoy [9].

Como las relaciones de (1) son homogéneas, palabras equivalentes en $B_n^+$ tienen la misma longitud, por lo que la longitud de una trenza positiva se define como la longitud de cualquier palabra que la represente.

Garside después estudia el siguiente elemento especial.

**Definición 33.** La **trenza fundamental** de $n$ cuerdas es la trenza

$$\Delta_n = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_1).$$

Cuando $n$ se sobreentiende, escribimos simplemente $\Delta$. ◂

**Proposición 34.** *Se verifican las siguientes propiedades:*

1. $\Delta = \sigma_1 \vee \ldots \vee \sigma_{n-1}$ [12, Lema 1].
2. $\sigma_i\Delta = \Delta\sigma_{n-i}$ *para todo* $i = 1, \ldots, n-1$ [12, Lema 4].

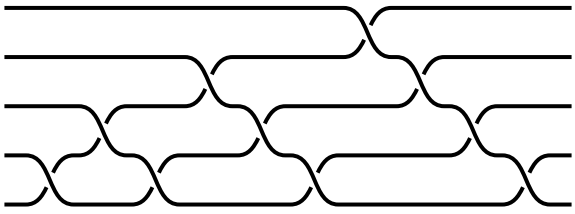


**Figura 11:** La trenza fundamental $\Delta_5$.

**Lema 35.** *Se tiene para $k > i \geq 1$ que $\sigma_i(\sigma_k \cdots \sigma_1) = (\sigma_k \cdots \sigma_1)\sigma_{i+1}$.*

*Demostración.* Usando las relaciones del monoide de trenzas positivas,

$$\begin{aligned} \sigma_i(\sigma_k \cdots \sigma_1) &= \sigma_i(\sigma_k \cdots \sigma_{i+2})(\sigma_{i+1}\sigma_i)(\sigma_{i-1} \cdots \sigma_1) \\ &= (\sigma_k \cdots \sigma_{i+2})(\sigma_i\sigma_{i+1}\sigma_i)(\sigma_{i-1} \cdots \sigma_1) \\ &= (\sigma_k \cdots \sigma_{i+2})(\sigma_{i+1}\sigma_i\sigma_{i+1})(\sigma_{i-1} \cdots \sigma_1) \\ &= (\sigma_k \cdots \sigma_{i+2})(\sigma_{i+1}\sigma_i)(\sigma_{i-1} \cdots \sigma_1)\sigma_{i+i} \\ &= (\sigma_k \cdots \sigma_1)\sigma_{i+1}. \end{aligned}$$

∎

A partir de este resultado podemos deducir las siguientes propiedades sobre $\Delta$.

**Proposición 36.** *Se cumplen las siguientes propiedades:*

1. $\sigma_1, \dots, \sigma_{n-1}$ *son también sufijos de* $\Delta$.
2. $\Delta^2$ *conmuta con todo elemento de* $B_n^+$.
3. *Para todo* $a \in B_n^+$ *se tiene que* $a \preccurlyeq \Delta^m$ *y* $\Delta^m \succcurlyeq a$, *donde* $m \geq 0$ *es la longitud de* $a$.

*Demostración.*

1. En primer lugar, por el lema 35 se tiene para $k > i \geq 1$ que $\sigma_i(\sigma_k \cdots \sigma_1) = (\sigma_k \cdots \sigma_1)\sigma_{i+1}$. Así pues, para expresar $\sigma_i$ como sufijo de $\Delta$ hacemos lo siguiente. Si $i = 1$, entonces por la definición de $\Delta$ ya tenemos que es un sufijo. Si $1 < i \leq n-1$, partimos de
$$\Delta = \sigma_1(\sigma_2\sigma_1) \cdots (\sigma_{n-i} \dots \underline{\sigma_1}) \cdots (\sigma_{n-1} \dots \sigma_1).$$
Procedemos a desplazar a la derecha el $\sigma_1$ subrayado tal como hemos hecho anteriormente. En cada paso irá aumentando el índice en una unidad. Por tanto, como hay $n - (n-i-1) = i+1$ bloques que se dejan atrás, obtenemos $\sigma_{1+i-1} = \sigma_i$, es decir,
$$\begin{aligned}\Delta &= \sigma_1(\sigma_2\sigma_1) \cdots (\sigma_{n-i} \dots \underline{\sigma_1})(\sigma_{n-i+1} \cdots \sigma_1) \cdots (\sigma_{n-1} \dots \sigma_1) \\ &= \sigma_1(\sigma_2\sigma_1) \cdots (\sigma_{n-i} \cdots \sigma_2)(\sigma_{n-i+1} \cdots \sigma_1\underline{\sigma_2}) \cdots (\sigma_{n-1} \dots \sigma_1) \\ &= \sigma_1(\sigma_2\sigma_1) \cdots (\sigma_{n-i} \cdots \sigma_2)(\sigma_{n-i+1} \cdots \sigma_1) \cdots (\sigma_{n-1} \dots \sigma_1)\underline{\sigma_i}.\end{aligned}$$
2. Basta probar que $\Delta^2$ conmuta con $\sigma_i$ para todo $1 \leq i \leq n-1$. Como $\sigma_i\Delta = \Delta\sigma_{n-i}$ y $\sigma_{n-i}\Delta = \Delta\sigma_i$, se tiene que
$$\sigma_i\Delta^2 = \Delta\sigma_{n-i}\Delta = \Delta^2\sigma_i.$$
3. Probamos que $a \preccurlyeq \Delta^m$, donde $m$ es la longitud de $a$, por inducción en $m$. Evidentemente, $1 \preccurlyeq \Delta^0 = 1$. Para una palabra de longitud 1 también está claro, porque $\sigma_i \preccurlyeq \Delta$ para todo $1 \leq i \leq n-1$ por definición de mínimo común múltiplo. Supongamos ahora que, para una palabra $a \in B_n^+$ de longitud $m-1$, se tiene el resultado. Entonces, cualquier palabra de longitud $m$ será de la forma $\sigma_j a$ para algún $1 \leq j \leq n-1$. Así que, usando la invarianza por multiplicación a izquierda y el caso $m = 1$,
$$a \preccurlyeq \Delta^{m-1} \implies \sigma_j a \preccurlyeq \sigma_j\Delta^{m-1} = \Delta^{m-1}\sigma_t \preccurlyeq \Delta^{m-1}\Delta = \Delta^m,$$
donde o bien $t = j$, o bien $t = n-j$, dependiendo de la paridad de $m$. De forma análoga, usando la invarianza por multiplicación a derecha se prueba que $\Delta^m \succcurlyeq a$. ∎

Esto tiene importantes implicaciones. Como todo par de elementos de $B_n^+$ tiene un múltiplo común y $B_n^+$ es cancelativo, las condiciones de Ore (definición 13) implican que $B_n^+$ se inyecta en su grupo de fracciones, que es precisamente $B_n$. Por lo tanto, $B_n^+$ no es solamente un monoide definido algebraicamente, sino que puede ser considerado como un submonoide de $B_n$ formado por las trenzas que pueden ser escritas solo con potencias positivas de los generadores.

Las propiedades anteriores implican que el orden parcial $\preccurlyeq$ (respectivamente, $\succcurlyeq$) puede ser extendido a $B_n$ de la siguiente manera: dadas $a, b \in B_n$, $a \preccurlyeq b$ (respectivamente, $a \succcurlyeq b$) si $ac = b$ (respectivamente, $b = ca$) para algún $c \in B_n^+$. Esto da un orden parcial que es invariante por multiplicación a izquierda (respectivamente, a derecha), y el cual admite un único mínimo común múltiplo y un único máximo común divisor. Este hecho podrá ser probado una vez definida la *forma normal de Garside* en la sección a continuación.

## 4.2. Solución al problema de la palabra

Garside dio una nueva solución al problema de la palabra en los grupos de trenzas de la siguiente manera. Recordemos que para todo $i = 1, \dots, n-1$ se tiene que $\Delta \succcurlyeq \sigma_i$ por la proposición 36, apartado 1, esto es, $\Delta = X_i\sigma_i$ para algún $X_i \in B_n^+$. Dada una trenza escrita como una palabra en $\sigma_1, \dots, \sigma_{n-1}$ y sus inversos, se puede reemplazar cada aparición de $\sigma_i^{-1}$ por $\Delta^{-1}X_i$. Conjugar una trenza positiva por $\Delta$ sigue dando una

trenza positiva por la proposición 34, apartado 2, así que podemos mover todas las apariciones de $\Delta^{-1}$ a la izquierda, de la siguiente forma: si encontramos $\sigma_j\Delta^{-1}$ $(1 \leq j \leq n-1)$, entonces por la proposición 34 sabemos que $\Delta\sigma_j = \sigma_{n-j}\Delta$, si y solo si $\sigma_j\Delta^{-1} = \Delta^{-1}\sigma_{n-j}$, por lo que podemos sustituir $\sigma_j\Delta^{-1}$ por $\Delta^{-1}\sigma_{n-j}$. Esto muestra que toda trenza puede ser escrita como $\Delta^p A$ para algún $p \in \mathbb{Z}$ y algún $A \in B_n^+$. Además, si $\Delta \preccurlyeq A$, podemos reemplazar $\Delta^p$ por $\Delta^{p+1}$ y $A$ por $\Delta^{-1}A$. Esto reduce la longitud de $A$, así que solo puede hacerse una cantidad finita de veces. Por tanto, toda trenza puede descomponerse *de manera única*, como $\Delta^p A$, donde $p \in \mathbb{Z}$, $A \in B_n^+$ y $\Delta \not\preccurlyeq A$. Efectivamente, si tuviéramos dos expresiones $\Delta^p A = \Delta^q B$ con $p < q$ en las condiciones anteriores, dividiendo por $\Delta^p$ tendríamos que $A = \Delta^{q-p}B$, lo cual contradice el hecho de que $A$ no tenga a $\Delta$ como prefijo. Análogamente para $p > q$, luego $p = q$ y $A = B$.

**Definición 37**. En base a lo comentado en el párrafo anterior, definimos la **forma normal de Garside** de una palabra $w \in B_n$ como $w = \Delta^p A$, donde $p \in \mathbb{Z}$, $A \in B_n^+$ y $\Delta \not\preccurlyeq A$. ◂

Esta forma normal permite resolver el problema de la palabra, ya que se pueden enumerar todas las palabras positivas que representan la trenza positiva $A$ reiterando las relaciones del monoide de trenzas positivas de todas las formas posibles. Esta fue la solución dada por Garside [12]. Sin embargo, no es muy satisfactoria, ya que da lugar a un algoritmo altamente ineficiente.

Elrifai y Morton [10] lo mejoraron definiendo la **forma normal a la izquierda** de una trenza. Basta tomar la descomposición $\Delta^p A$ y después definir

$$\begin{aligned} a_1 &= A \wedge \Delta, \\ a_i &= (a_{i-1}^{-1} \cdots a_1^{-1} A) \wedge \Delta, \ \forall\, i > 1. \end{aligned}$$

Nótese que existe un $r \geq 0$ tal que $a_i = 1$ para todo $i > r$, ya que la longitud de $a_{i-1}^{-1} \cdots a_1^{-1}A$ es estrictamente decreciente. De esta forma, toda trenza puede ser escrita de manera única como

$$\Delta^p a_1 \cdots a_r,$$

donde los $a_i$ son los definidos anteriormente, los cuales por definición son unos prefijos propios de $\Delta$, es decir, $1 \prec a_i \prec \Delta$, y además se puede demostrar que $(a_i a_{i+1}) \wedge \Delta = a_i$ para todo $i = 1, \ldots, r-1$ [11]. Esta es la anteriormente mencionada forma normal a la izquierda de la trenza. Los prefijos positivos de $\Delta$ son llamados **trenzas simples** o **trenzas de permutación**. El nombre no es casual, ya que, como prueba Thurston [11], estas trenzas representan en cierto modo a las permutaciones que inducen. Estas trenzas se caracterizan por ser aquellas en las que los generadores $\sigma_i$ aparecen con exponente no superior a 1 en todas sus expresiones en términos de los generadores de Artin. Por tanto, la forma normal a la izquierda de una trenza es una descomposición única como producto de una potencia de $\Delta$ y una sucesión de elementos simples propios. Thurston [11] mostró que esta forma normal puede ser calculada en tiempo $O(\ell^2 n \log n)$ para una palabra de $\ell$ letras en $B_n$.

En [11] se puede encontrar además una forma más práctica de llevar a cabo el algoritmo de encontrar la forma normal a la izquierda, la cual utilizareos en el ejemplo 38. Antes de explicarla, vamos a introducir algo de nomenclatura. Dadas dos trenzas simples positivas $A$ y $B$, decimos que un prefijo no trivial $b \preccurlyeq B$ **se puede pasar** de $B$ a $A$ si $Ab$ es simple y, en tal caso, **pasar** $b$ de $B$ a $A$ consiste en realizar las transformaciones $A \to Ab$ y $B \to b^{-1}B$. Con esto presente, el algoritmo consiste en lo siguiente:

1. Una vez tenemos una palabra $w \in B_n$ en forma normal de Garside $w = \Delta^p A$, si $A = 1$, entonces no hay nada que hacer. En caso contrario, dividimos $A$ en bloques formados por elementos simples, digamos,
$$A = a_{1,0}a_{2,0} \ldots a_{m,0}.$$
2. En el paso $t \geq 0$ tenemos $A$ expresada en bloques de elementos simples como
$$A = a_{1,t}a_{2,t} \ldots a_{m,t}.$$
En este paso buscamos el primer par $a_{i,t}a_{i+1,t}$ de modo que se pueda pasar algún prefijo de $a_{i+1,t}$ a $a_{i,t}$ y lo pasamos. Esto nos dará la descomposición
$$A = a_{1,t+1}a_{2,t+1} \ldots a_{m,t+1}.$$
3. Volvemos al paso 2 y reiteramos hasta que no quede ningún par que verifique la condición.

Este proceso, naturalmente, termina, porque el vector formado por las longitudes de los bloques aumenta en cada paso su orden lexicográfico, el cual está acotado por $(m, 0, \dots, 0)$, donde $m$ es la longitud de $A$. La forma normal a la izquierda se obtendrá eliminando los bloques triviales (que necesariamente estarán al final).

Alternativamente, podríamos empezar con una descomposición $w = \Delta^q A$ con $A \in B_n^+$, pero sin asegurarnos de que $\Delta \not\preccurlyeq A$, pues $\Delta$ aparecería al acumular elementos simples en caso de ser prefijo de $A$, y podríamos enviarlo al bloque de $\Delta^q$. En cualquier caso, este proceso acabará con la forma normal a la izquierda, pues no poder pasar ninguna letra del bloque $a_{i+1}$ al bloque $a_i$ es equivalente a que $a_i = (a_i a_{i+1}) \wedge \Delta$.

**Ejemplo 38.** En $B_4$, sean $\alpha_1 = \sigma_1\sigma_2^{-1}\sigma_3$ y $\alpha_2 = \sigma_3\sigma_1\sigma_1\sigma_2\sigma_1$. Queremos comprobar si $\alpha_1$ y $\alpha_2$ representan el mismo elemento. Lo primero que debemos hacer es eliminar el exponente negativo de $\alpha_1$. Para ello, tenemos que expresar $\Delta = \Delta_4 = \sigma_1(\sigma_2\sigma_1)(\sigma_3\sigma_2\sigma_1)$ de forma que tenga a $\sigma_2$ como sufijo. Esto es sencillo, pues basta usar la técnica de la demostración del primer apartado de la proposición 36 para escribir

$$\Delta = \sigma_1(\sigma_2)(\sigma_3\sigma_2\sigma_1)\sigma_2.$$

Así pues, $\sigma_2^{-1} = \Delta^{-1}\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$, de modo que $\alpha_1 = \sigma_1\Delta^{-1}\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_3$. Usando la proposición 34, pasamos $\Delta^{-1}$ a la izquierda:

$$\alpha_1 = \Delta^{-1}\sigma_3\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_3.$$

Ahora vamos a hacer la separación de bloques en las palabras positivas. Empezamos con $\alpha_2$. Vamos a dividirla en los bloques $b_{1,0} = \sigma_3\sigma_1$ y $b_{2,0} = \sigma_1\sigma_2\sigma_1$, que son claramente trenzas simples. En general, se puede comenzar por bloques de una sola letra para evitar esta verificación. Así, obtenemos

$$\alpha_2 = b_{1,0}b_{2,0} = (\sigma_3\sigma_1)(\sigma_1\sigma_2\sigma_1).$$

Aparentemente no podemos pasar ninguna letra de $b_{2,0}$ a $b_{1,0}$, pues aparecería $\sigma_1$ dos veces seguidas. Sin embargo, recordemos que las relaciones de (1) nos dan $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. Por lo tanto, reescribimos $\alpha_2$ y continuamos con

$$\alpha_2 = b_{1,1}b_{2,1} = (\sigma_3\sigma_1\sigma_2\sigma_1)(\sigma_2).$$

Ahora tenemos la situación inversa: aparentemente, podríamos añadir $\sigma_2$ al primer bloque, pero utilizando la misma relación de la presentación del grupo de trenzas que antes, nos aparecería $\sigma_2$ dos veces consecutivas, por lo que hemos finalizado el proceso y $\alpha_2 = \Delta^0 b_1 b_2$ con $b_1 = b_{1,1}$ y $b_2 = b_{2,1}$. Obsérvese que el bloque que hemos pasado a la izquierda $(\sigma_2\sigma_1)$ se corresponde con $b_{2,0} \wedge (b_{1,0}^{-1}\Delta)$ y el bloque resultante $(\sigma_3\sigma_1\sigma_2\sigma_1)$ se corresponde con $\alpha_2 \wedge \Delta$ en el algoritmo original de Elrifai y Morton. Además, esta claro que ninguno de los factores es una potencia de $\Delta$. ◂

## Referencias


[1] Aguilar Martín, Javier. *El problema de la palabra en los grupos de trenzas*. Trabajo de Fin de Grado. Universidad de Sevilla, 2018. URL: https://hdl.handle.net/11441/77489.

[2] Aluffi, Paolo. *Algebra: Chapter 0*. Vol. 104. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2009. https://doi.org/10.1090/gsm/104.

[3] Artin, Emil. «Theorie der Zöpfe». En: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 4.1 (1925), págs. 47-72. ISSN: 0025-5858. https://doi.org/10.1007/BF02950718.

[4] Artin, Emil. «Theory of braids». En: *Annals of Mathematics. Second Series* 48 (1947), págs. 101-126. ISSN: 0003-486X. https://doi.org/10.2307/1969218.

[5] Birman, Joan S. *Braids, Links, and Mapping Class Groups*. Vol. 82. Annals of Mathematics Studies. Princeton: Princeton University Press, 2016. https://doi.org/10.1515/9781400881420.

[6] Clifford, Alfred H. y Preston, Gordon B. *The algebraic theory of semigroups. Vol. I*. Mathematical Surveys, No. 7. Providence, Rhode Island: American Mathematical Society, 1961. ISBN: 978-0-8218-0272-4.

[7] Dehn, Max. «Über unendliche diskontinuierliche Gruppen». En: *Mathematische Annalen* 71.1 (1911), págs. 116-144. issn: 0025-5831. https://doi.org/10.1007/BF01456932.

[8] Dehn, Max. «Transformation der Kurven auf zweiseitigen Flächen». En: *Mathematische Annalen* 72.3 (1912), págs. 413-421. issn: 0025-5831. https://doi.org/10.1007/BF01456725.

[9] Dehornoy, Patrick. «Groupes de Garside». En: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 35.2 (2002), págs. 267-306. issn: 0012-9593. https://doi.org/10.1016/S0012-9593(02)01090-X.

[10] Elrifai, Elsayed A. y Morton, Hugh R. «Algorithms for positive braids». En: *The Quarterly Journal of Mathematics. Oxford. Second Series* 45.180 (1994), págs. 479-497. issn: 0033-5606. https://doi.org/10.1093/qmath/45.4.479.

[11] Epstein, David B. A.; Cannon, James W.; Holt, Derek F.; Levy, Silvio V. F.; Paterson, Michael S., y Thurston, William P. *Word Processing in Groups*. Boca Raton, Florida: CRC Press, 1992. isbn: 978-0-86720-244-1.

[12] Garside, Frank A. «The braid group and other groups». En: *The Quarterly Journal of Mathematics. Oxford. Second Series* 20 (1969), págs. 235-254. issn: 0033-5606. https://doi.org/10.1093/qmath/20.1.235.

[13] González-Meneses, Juan y Silvero, Marithania. «Polynomial braid combing». En: *Mathematics of Computation* 88.318 (2019), págs. 2027-2045. issn: 0025-5718. https://doi.org/10.1090/mcom/3392.

[14] Hurwitz, Adolf. «Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten». En: *Mathematische Annalen* 39.1 (1891), págs. 1-60. issn: 0025-5831. https://doi.org/10.1007/BF01199469.

[15] Lyndon, Roger C. y Schupp, Paul E. *Combinatorial Group Theory*. Vol. 89. Classics in Mathematics. Berlin, Heidelberg: Springer, 2001. https://doi.org/10.1007/978-3-642-61896-3.

[16] Magnus, Wilhelm. «Über Automorphismen von Fundamentalgruppen berandeter Flächen». En: *Mathematische Annalen* 109.1 (1934), págs. 617-646. issn: 0025-5831. https://doi.org/10.1007/BF01449158.

[17] Markoff Jr., Andrey. «Foundations of the algebraic theory of tresses». En: *Russian mathematicians in the 20th century* (2003), págs. 614-621.

[18] Novikov, Petr Sergeevič. *On the algorithmic unsolvability of the word problem in group theory*. Vol. 44. Trudy Matematicheskogo Instituta imeni V. A. Steklova. Moscú: Izdatelstvo Akademii Nauk SSSR, 1955. url: http://mi.mathnet.ru/eng/tm1180.

[19] Ore, Oystein. «Linear equations in non-commutative fields». En: *Annals of Mathematics. Second Series* 32.3 (1931), págs. 463-477. issn: 0003-486X. https://doi.org/10.2307/1968245.