



**UNIVERSIDAD DE SEVILLA  
FACULTAD DE MATEMÁTICAS**

**Trabajo de Fin de Grado**

# **El problema de la palabra en los grupos de trenzas**

Por:

Javier Aguilar Martín

Dirigido por:

Juan González-Meneses López y Ramón Jesús Flores Díaz

Grado en Matemáticas

18 de Junio de 2018

# Índice general

<b>Abstract</b>	<b>3</b>
<b>Resumen</b>	<b>4</b>
<b>1 Preliminares</b>	<b>5</b>
1.1 Trenzas como colección de cuerdas . . . . .	5
1.1.1 Estructura de grupo . . . . .	7
1.2 Espacios de configuración . . . . .	9
1.3 Mapping Class Groups . . . . .	11
1.4 Presentación del grupo de trenzas . . . . .	13
1.5 El problema de la palabra . . . . .	14
1.6 Definiciones y resultados adicionales . . . . .	16
1.6.1 Producto semidirecto . . . . .	16
1.6.2 Monoides . . . . .	18
1.6.3 Espacios recubridores . . . . .	19
<b>2 Automorfismos del grupo libre</b>	<b>21</b>
2.1 Representación del grupo de trenzas como automorfismos del grupo libre	21
2.2 Solución al problema de la palabra . . . . .	23
<b>3 Peinado de trenzas</b>	<b>24</b>
3.1 Sucesiones exactas . . . . .	24
3.2 Trenzas puras como producto semidirecto de grupos libres . . . . .	26
3.3 Solución al problema de la palabra . . . . .	27
<b>4 Formas normales</b>	<b>31</b>
4.1 Estructura de Garside . . . . .	31
4.2 Solución al problema de la palabra . . . . .	35
<b>5 Representaciones lineales</b>	<b>39</b>
5.1 Representación de Burau reducida . . . . .	39
5.1.1 Definición a partir de espacios recubridores . . . . .	39
5.1.2 Expresión matricial . . . . .	41
5.2 Representación LKB . . . . .	43
5.2.1 Representación de Bigelow . . . . .	44
5.3 Solución al problema de la palabra . . . . .	45
<b>Bibliografía</b>	<b>47</b>

# Abstract

The word problem, the conjugacy problem and the isomorphism problem were three fundamental problems of group theory proposed by Max Dehn [11]. We will deal with the first one. This problem consists of: given a group  $G$  with a finite presentation  $\langle S|R \rangle$  and given two elements  $A, B \in G$  as a product of elements of  $S$  and their inverses, decide whether  $A = B$  as elements of the group or, equivalently, whether  $AB^{-1} = e$ , where  $e$  denotes the identity element.

The name of this problem comes from the fact that we can consider the alphabet  $\Sigma = S \cup S^{-1}$ , where  $S^{-1}$  is the set of inverses of the elements of  $S$ , and view  $G$  as a language over  $\Sigma$ , where two words  $A$  and  $B$  represent the same element if and only if one can transform  $A$  into  $B$  in a finite amount of steps using the rewriting rules given by  $R$  and the inverse cancellation.

Dehn described algorithms to solve the word problem for the fundamental groups of closed orientable two-dimensional manifolds of genus greater than or equal to 2 [10]. However, in 1955 Pyotr Novikov found examples of finitely presented groups where the word problem is undecidable [26], i.e., there cannot be any algorithm to solve it. Nevertheless, the word problem is solvable for many groups. Clear examples of this are the finite groups and the free groups. Here we study the word problem in the braid groups. These groups appear in many branches of mathematics such as algebra, topology and analysis, and the word problem is known to be solvable for them.

This project begins giving different equivalent definitions of the braid groups, starting from the intuitive idea of geometric braid. Each definition will give a different perspective and they will provide us more tools to solve the word problem. At the end of the first chapter we shall give some additional definitions and results that will be very important for the rest of the project.

In the second chapter we will explain the first known algorithm to solve the word problem in the braid groups, based on representing braids as automorphisms of a free group. In the third chapter we will see another method, called *braid combing*, based on the solvability of the word problem for the free groups. In the fourth chapter we will explore the *Garside structure* of the braid groups, which will allow us to solve the word problem by means of a *normal form* of the elements of the group. In the last chapter, we will present some examples of linear representations that generate another algorithm to solve the word problem.

In every chapter there will be concrete examples of solutions of the word problem using each one of the presented methods.

# Resumen

El problema de la palabra, el problema de la conjugación y el problema del isomorfismo fueron tres problemas fundamentales de la teoría de grupos propuestos por Max Dehn [11]. Aquí trataremos el primero de ellos, consistente en: dado un grupo  $G$  con una presentación finita  $\langle S|R \rangle$  y dados dos elementos  $A$  y  $B$  de  $G$  expresados como producto de los elementos de  $S$  y sus inversos, decidir si  $A = B$  como elementos del grupo o, equivalentemente, si  $AB^{-1} = e$ , donde  $e$  representa el elemento neutro.

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 [10]. Sin embargo, en 1955 Pyotr Novikov encontró ejemplos de grupos finitamente presentados donde el problema de la palabra era indecidible [26], 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 y el análisis, y en los cuales el problema de la palabra es resoluble.

Comenzaremos dando distintas definiciones equivalentes de los grupos de trenzas, partiendo de la idea intuitiva de las trenzas. Cada una de las definiciones aportará un enfoque distinto, lo cual proporcionará más herramientas para la resolución del problema de la palabra. Al final del primer capítulo daremos algunas definiciones y resultados que serán fundamentales para el desarrollo del resto del trabajo.

En el segundo capítulo daremos el primer algoritmo diseñado para resolver el problema de la palabra en los grupos de trenzas, consistente en representar estos grupos como automorfismos de un grupo libre. En el tercer capítulo veremos otro método, conocido como *peinado de trenzas*, basado también en la resolubilidad del problema de la palabra en los grupos libres. En el cuarto capítulo exploraremos la *estructura de Garside* de los grupos de trenzas, la cual nos permitirá resolver el problema de la palabra mediante el uso de unas *formas normales* para los elementos de este grupo. Por último, veremos algunos ejemplos de representaciones lineales del grupo de trenzas con los que se puede resolver el problema de la palabra.

En cada uno de estos capítulos se mostrarán ejemplos concretos de cómo resolver el problema de la palabra con cada uno de los métodos explicados.

# Capítulo 1

## Preliminares

Aunque el término *grupo de trenzas* fue acuñado por Artin en 1925 [2], estos grupos ya fueron considerados por Hurwitz en 1891 [21] como lo que en terminología moderna se llamaría “grupo fundamental de espacios de configuración de  $n$  puntos en el plano complejo”. Magnus en 1935 [24] consideró el mismo grupo desde el punto de vista de los *mapping classes*. Markov [25] dio una aproximación totalmente algebraica.

En este capítulo veremos varias de estas definiciones, que son todas equivalentes [32], ya que una sola definición no es suficiente para enunciar y demostrar los resultados que se presentan en el resto del trabajo. Esta variedad de definiciones permite estudiar los grupos de trenzas desde perspectivas muy distintas, lo cual aporta una gran riqueza a la teoría.

### 1.1. Trenzas como colección de cuerdas

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

**Definición 1.1.1.** Sea  $n \geq 1$  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  $1 \leq k \leq n$ ). Se define la *trenza geométrica de  $n$  cuerdas* como la  $n$ -upla  $\beta = (\beta_1, \dots, \beta_n)$  de caminos  $\beta_k : [0, 1] \rightarrow \mathbb{C} \times [0, 1]$  tal que:

- $\beta_k(t) = (\alpha_k(t), t)$ , donde  $\alpha_k(0) = P_k$  para todo  $1 \leq k \leq n$ ,
- existe una permutación  $\tau = \tau(\beta) \in \Sigma_n$  tal que  $\alpha_k(1) = P_{\tau(k)}$  para todo  $1 \leq k \leq n$ , llamada *permutación inducida por  $\beta$* ,
- $\alpha_k(t) \neq \alpha_l(t)$  para todo  $k \neq l$  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  $1 \leq k \leq n$ , 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.

El dibujo tridimensional de una trenza geométrica tiene la siguiente forma:

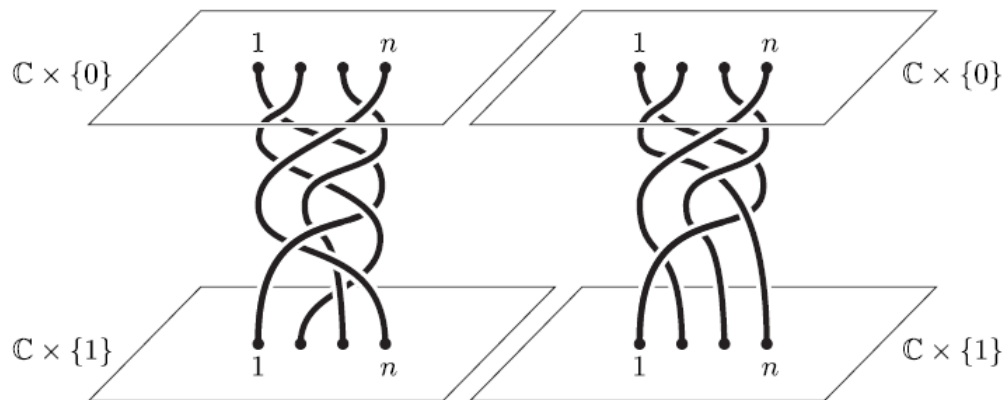


Figura 1.1: Una trenza geométrica pura y una trenza geométrica no pura.

**Observación 1.1.2.** 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  $90^\circ$ ). Los puntos en los que la proyección de dos cuerdas coincide los representaremos como en la Figura 1.2 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 1.4 se ilustra la proyección de la trenza no pura de la Figura 1.1.



Figura 1.2: Cruce positivo y cruce negativo, respectivamente.

**Definición 1.1.3.** 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 1.3.

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

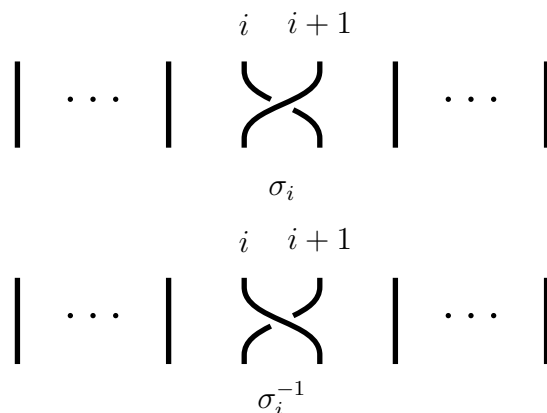


Figura 1.3: Generador de Artin y su inverso.

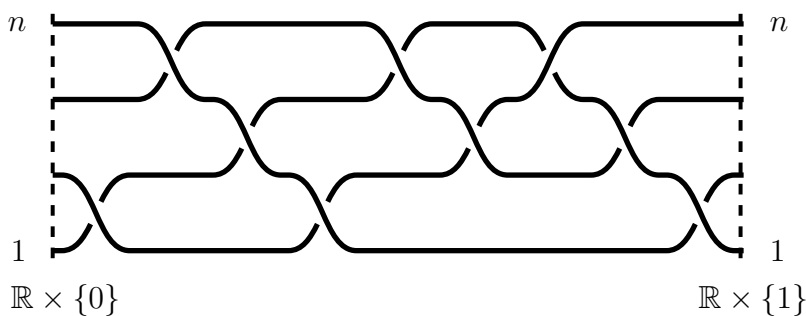


Figura 1.4: Ejemplo de representación plana.

### 1.1.1. 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 1.1.4.** 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 1.5 se ilustra un ejemplo. En ocasiones omitiremos el punto y escribiremos simplemente  $\alpha\beta$ . Asimismo, denotaremos  $\alpha^n = \underbrace{\alpha \cdots \alpha}_{n \text{ veces}}$ .

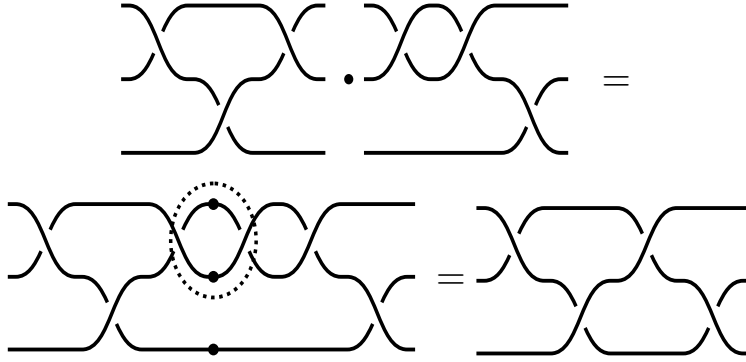


Figura 1.5: Producto de dos trenzas.

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 1.1.5.** El conjunto  $B_n$  dotado de esta operación tiene estructura de grupo, y se le llama *grupo de trenzas de  $n$  cuerdas*. El resultado también es cierto para  $PB_n$ , cuyo nombre es *grupo de trenzas puras de  $n$  cuerdas*.

**Demostración.** 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, 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 1.1.1. 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  $Id = (Id_1, \dots, Id_n)$ , donde  $Id_k$  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  $\alpha^{-1} = [(\bar{a}_{\tau^{-1}(1)}, \dots, \bar{a}_{\tau^{-1}(n)})]$ , donde  $\bar{a}_k$  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 la homotopía de caminos con respecto al camino opuesto:

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

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

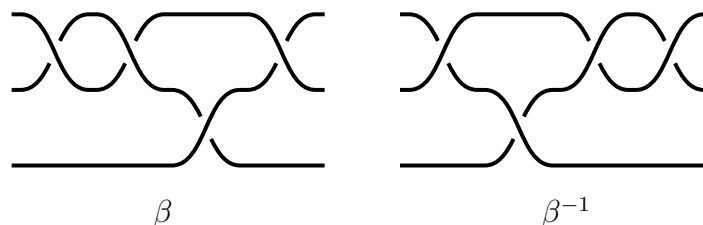


Figura 1.6: Inversa de una trenza.

## 1.2. Espacios de configuración

Vamos a empezar dando la noción general de espacio de configuración, introducida por Fadell en 1962 [16].

**Definición 1.2.1.** Dado un espacio topológico  $X$ , el  $n$ -ésimo *espacio de configuración* de  $X$  o *espacio de configuración de  $n$  puntos* de  $X$  se define como el conjunto

$$M_n(X) = \{(x_1, \dots, x_n) \in X^n \mid x_i \neq x_j \ \forall i \neq j\},$$

dotado de la topología de subespacio de  $X^n$ . Cuando el espacio topológico  $X$  se sobreentienda por el contexto, el espacio de configuración se denotará simplemente  $M_n$ .

Hay una acción natural del grupo simétrico  $\Sigma_n$  en los puntos de  $M_n(X)$  dada por

$$\begin{aligned} \Sigma_n \times M_n(X) &\rightarrow M_n(X) \\ (\sigma, x) &\mapsto \sigma(x). \end{aligned}$$

Esto da lugar al espacio definido a continuación:

**Definición 1.2.2.** Se define el  $n$ -ésimo *espacio de configuración no ordenado* de  $X$  o *espacio de configuración de  $n$  puntos no ordenados* de  $X$  como

$$N_n(X) = M_n(X)/\Sigma_n,$$

es decir, el espacio de órbitas de la acción. De igual manera que con el anterior espacio de configuración, cuando se sobreentienda  $X$ , lo denotaremos por  $N_n$ .

**Observación 1.2.3.** Para cualquier espacio topológico  $X$ ,  $M_1(X) = N_1(X) = X$ .

**Ejemplo 1.2.4.** Veamos un ejemplo no trivial de espacio de configuración. Consideremos  $M_2(\mathbb{R}^3) = \{(x_1, x_2) \in \mathbb{R}^3 \times \mathbb{R}^3 \mid x_1 \neq x_2\}$ . Podemos definir la aplicación  $M_2(\mathbb{R}^3) \rightarrow \mathbb{R}^3 \times (\mathbb{R}^3 \setminus \{0\})$  como

$$(x_1, x_2) \mapsto (x_1 + x_2, x_1 - x_2).$$

Es fácil ver que esta aplicación es un homeomorfismo, por lo que  $M_2(\mathbb{R}^3) \cong \mathbb{R}^3 \times (\mathbb{R}^3 \setminus \{0\})$ . Además, la aplicación es compatible con la acción de  $\Sigma_2$ , es decir, la aplicación sigue siendo un homeomorfismo sobre  $\mathbb{R}^3 \times (\mathbb{R}^3 \setminus \{0\})$  al permutar las componentes. Sin embargo, punto a punto, lo que se observa es que la primera coordenada se conserva y la segunda cambia de signo tras la permutación. Por lo tanto, en  $N_2(\mathbb{R}^3) = M_2(\mathbb{R}^3)/\Sigma_2$ ,  $(x, y) \sim (x, -y)$  y no hay más puntos distintos relacionados entre sí. Por tanto,  $N_2(\mathbb{R}^3) = \mathbb{R}^3 \times (\mathbb{R}_+^3 \setminus \{0\})$ , donde  $\mathbb{R}_+^3$  denota los puntos cuya primera coordenada no nula es positiva.

Consideremos ahora el espacio de configuración de  $n$  puntos distintos del plano complejo  $\mathbb{C}$ . Esto es,

$$M_n = \{(z_1, \dots, z_n) \in \mathbb{C}^n \mid z_i \neq z_j \ \forall i \neq j\}.$$

Obsérvese que es un espacio de dimensión real  $2n$ . No es una buena idea intentar visualizar el espacio de configuración  $M_n$  en  $2n$  dimensiones; en su lugar, basta considerar  $n$  puntos distintos y ordenados de  $\mathbb{C}$ . Esto es,  $(z_1, z_2, z_3, \dots, z_n)$  y  $(z_2, z_1, z_3, \dots, z_n)$  representarían puntos distintos en  $M_n$ .

**Definición 1.2.5.** El *grupo de trenzas puras* de  $n$  cuerdas,  $PB_n$ , es el grupo fundamental de  $M_n$ , es decir,

$$PB_n = \pi_1(M_n).$$

Tratemos de interpretar esta definición. Una trenza pura  $\beta \in \pi_1(M_n)$  es un lazo en  $M_n$

$$\begin{aligned} \beta : [0, 1] &\rightarrow M_n \\ t &\mapsto \beta(t) = (\beta_1(t), \dots, \beta_n(t)), \end{aligned}$$

Por tanto basta elegir un punto base de  $M_n$ , que puede ser, por ejemplo, la  $n$ -upla de enteros  $(1, 2, \dots, n)$ . Una trenza pura será representada por el movimiento de estos puntos en  $\mathbb{C}$ , teniendo en cuenta que en cada momento los puntos son todos distintos entre sí. Al final del movimiento, cada punto regresa a su posición original. Por supuesto, el lazo está definido salvo homotopía, lo que nos permite deformar el

movimiento de forma natural (evitando que dos puntos se encuentren en el mismo lugar al mismo tiempo), dando una trenza pura equivalente.

Este movimiento se puede ver también en  $\mathbb{C} \times [0, 1]$ , lo que nos daría una imagen similar a la de la Figura 1.1 a la izquierda.

La definición general de trenza se puede obtener inmediatamente a partir de la de trenzas puras, pues las trenzas (en general) surgen cuando no importa el orden de los puntos que se están moviendo, sino simplemente el conjunto de  $n$  puntos distintos de  $\mathbb{C}$ .

**Definición 1.2.6.** El *grupo de trenzas* de  $n$  cuerdas,  $B_n$ , es el grupo fundamental del  $N_n$ , es decir,

$$B_n = \pi_1(N_n) = \pi_1(M_n/\Sigma_n).$$

La equivalencia entre estas definiciones y la Definición 1.1.1 se puede encontrar en [32].

Al igual que antes, las trenzas pueden ser visualizadas como lazos, con la diferencia de que ahora, dado un lazo  $\beta : [0, 1] \rightarrow N_n$ ,  $\beta(1)$  puede tener como representante una permutación de las coordenadas de  $\beta(0)$ . De nuevo, dos trenzas son consideradas iguales si son homotópicamente equivalentes. Al representar el movimiento en  $\mathbb{C} \times [0, 1]$  nos quedaría un dibujo similar al de la Figura 1.1 a la derecha.

En ambos grupos de trenzas, el producto se corresponde con la concatenación de lazos, que a su vez consiste en realizar un movimiento después de otro, o en la representación tridimensional, con apilar trenzas (reescalando verticalmente) como en la Figura 1.5.

### 1.3. Mapping Class Groups

Otra interpretación conocida de las trenzas consiste en considerarlas como automorfismos del disco punteado, salvo deformación. Para ello necesitamos definir una topología adecuada para un espacio de automorfismos, que será la siguiente:

**Definición 1.3.1.** Sean  $X$  e  $Y$  espacios topológicos y  $C(X, Y)$  el conjunto de funciones continuas de  $X$  en  $Y$ . La topología *compacta-abierto* en  $C(X, Y)$  es aquella que tiene como subbase los conjuntos de la forma

$$B(K, U) = \{f \mid f(K) \subset U\},$$

donde  $K \subseteq X$  es compacto y  $U \subseteq Y$  es abierto. Es decir, los abiertos de la topología compacta-abierto son uniones arbitrarias de intersecciones finitas de subconjuntos de la forma anterior.

Sea pues  $\mathbb{D}_n$  el disco cerrado menos  $n$  puntos:

$$\mathbb{D}_n = \mathbb{D}^2 \setminus \{P_1, \dots, P_n\}.$$

Sea  $\text{Homeo}^+(\mathbb{D}_n)$  el conjunto de homeomorfismos de  $\mathbb{D}_n$  en sí mismo que preservan la orientación y fijan los puntos del borde. Este conjunto admite la topología compacta-abierta. Por tanto, tenemos una noción natural de *deformación continua* de un automorfismo de  $\mathbb{D}_n$ , fijando el borde y los agujeros. Esta noción se formaliza mediante la siguiente definición.

**Definición 1.3.2.** Una *isotopía* entre dos espacios topológicos  $X$  e  $Y$  es una familia continua de homeomorfismos  $h_t : X \rightarrow Y$  con  $0 \leq t \leq 1$ . Dos homeomorfismos  $f, g : X \rightarrow Y$  son *isotópicos* si existe una isotopía  $h_t : X \rightarrow Y$  con  $h_0 = f$  y  $h_1 = g$ .

Consideraremos que dos automorfismos son iguales si pueden ser transformados el uno en el otro mediante una isotopía de  $\mathbb{D}_n$  en sí mismo que fije el borde punto a punto. En otras palabras:

**Definición 1.3.3.** Si denotamos  $\text{Homeo}_0^+(\mathbb{D}_n)$  a la componente conexa de  $\text{Id}_{\mathbb{D}_n}$  en  $\text{Homeo}^+(\mathbb{D}_n)$ , definimos entonces el *mapping class group* (grupo de clases de aplicaciones) de  $\mathbb{D}_n$  como:

$$\mathcal{M}(\mathbb{D}_n) = \text{Homeo}^+(\mathbb{D}_n) / \text{Homeo}_0^+(\mathbb{D}_n).$$

Con esta definición se tiene [24]:

$$\mathcal{M}(\mathbb{D}_n) \cong B_n.$$

Se sabe que un automorfismo del disco cerrado  $\mathbb{D}^2$  que fije la frontera puede ser deformado mediante isotopía a la identidad (se prueba mediante el conocido como *truco de Alexander* [1]). Por tanto, dado un elemento de  $\mathcal{M}(\mathbb{D}_n)$ , se puede tomar un homeomorfismo de  $\mathbb{D}_n$  que lo represente y extenderlo de forma única a un homeomorfismo  $f$  de  $\mathbb{D}^2$ . A continuación, se toma una isotopía entre  $\text{Id}_{\mathbb{D}^2}$  y  $f$ , y se sigue el camino de los puntos  $P_1, \dots, P_n$  durante la deformación. Esto nos da un lazo en  $\pi_1(N_n(\mathbb{D}_n))$ , que se corresponde con una trenza.

## 1.4. Presentación del grupo de trenzas

Una de las características mejor conocidas de los grupos de trenzas es su presentación finita descubierta por Artin en [3]. Ya hemos mencionado los generadores  $\sigma_1, \dots, \sigma_{n-1} \in B_n$  en la Definición 1.1.3. La presentación completa sería la siguiente:

$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \left| \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i, & |i - j| > 1 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, & |i - j| = 1 \end{array} \right. \right\rangle. \quad (1.1)$$

La prueba de la completitud de esta presentación puede encontrarse en [24].

Vamos a dar también la presentación del grupo de trenzas puras, en concreto la dada por J. S. Birman en [7] (ver también [19]), pues nos será más útil para probar ciertos resultados. La presentación original dada por Artin se puede encontrar en [3]. Así pues, definimos los *generadores de Birman*

$$A_{ij} = \sigma_{j-1} \dots \sigma_{i+1} \sigma_i^2 \sigma_{i+1}^{-1} \dots \sigma_{j-1}^{-1} \quad (1 \leq i < j \leq n) \quad (1.2)$$

y las relaciones

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

En la Figura 1.7 se puede observar qué trenza representa geoméricamente el generador  $A_{ij}$ .

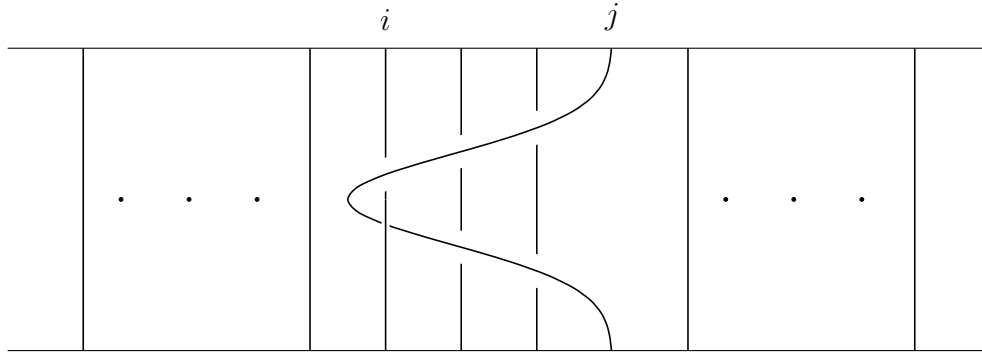


Figura 1.7: Interpretación geométrica de la trenza  $A_{ij}$ .

**Nota 1.4.1.** Cuando  $j = i + 1$ ,  $A_{ij} = \sigma_i^2$ .

También nos serán útiles a la hora de hacer cálculos las siguientes relaciones equivalentes a las anteriores, y que de nuevo se pueden encontrar en [19]:

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

## 1.5. El problema de la palabra

El problema de la palabra fue descrito por primera vez por Max Dehn [11] en 1911 y desde entonces se ha convertido en uno de los problemas más importantes de la teoría algorítmica de grupos. Este problema consiste en: dado un grupo  $G$  con una presentación finita  $\langle S|R \rangle$  y dados dos elementos  $A$  y  $B$  de  $G$  expresados como producto de los elementos de  $S$  y sus inversos, decidir si  $A = B$  como elementos del grupo o, equivalentemente, si  $AB^{-1} = e$ , donde  $e$  representa el elemento neutro.

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 problema de la palabra es un problema de *decisión*. Los problemas de decisión consisten en determinar si un objeto  $\mathcal{O}$  cumple una propiedad  $\mathcal{P}$ . En este caso, decidimos si dos elementos de un grupo son el mismo. Dentro de los problemas de decisión podemos encontrar los problemas de *conocimiento* y los problemas de *búsqueda*. Los problemas de conocimiento requieren una prueba de que el objeto  $\mathcal{O}$  cumple la propiedad  $\mathcal{P}$ , pero no se requiere ninguna construcción explícita. Un ejemplo ilustrativo sería decidir si una matriz es invertible. La solución al problema de conocimiento no requeriría construir la matriz inversa, sino que bastaría con calcular el determinante o reducir la matriz a la identidad. Los problemas de búsqueda requieren una construcción más explícita. En el caso del problema de la palabra, no solo consistiría en decidir si un elemento  $A$  de un grupo  $G = \langle S|R \rangle$  es trivial o no, sino que, en caso de que la respuesta sea afirmativa, se pide encontrar las transformaciones mediante relaciones de  $S$  que convierten  $A$  en el elemento neutro. Más información y ejemplos sobre los problemas de decisión en teoría de grupos se pueden encontrar en [30].

Por lo general, hay tres técnicas principales para resolver el problema de la palabra:

- Representaciones fieles en otros grupos: una representación fiel es un homomorfismo de grupos inyectivo. Si tenemos una representación fiel dada de forma explícita podemos trasladar el problema del grupo original a un grupo en el que ya sepamos resolverlo. Un ejemplo paradigmático son las representaciones lineales, en las que el grupo de llegada es un grupo de matrices.
- Cálculo de una forma normal: se trata de encontrar una forma única de escribir todos los elementos del grupo, con lo que dos elementos sean el mismo si y solo si sus formas normales coinciden.
- Cálculo de un invariante: calcular, a partir de una palabra, un invariante que tiene un valor determinado si y solo si la palabra representa el elemento trivial. Un ejemplo de este tipo de invariantes son las *coordenadas de Dynnikov* [13], que son un invariante específico de las trenzas.

En este trabajo veremos dos ejemplos de la primera técnica y otros dos de la segunda. La primera de ellas aparece en los capítulos 2 y 5, mientras que la segunda corresponde a los capítulos 3 y 4. En el capítulo 2 la representación de  $B_n$  se hará sobre los automorfismos del grupo libre de rango  $n$ , donde el problema de la palabra se resuelve simplemente calculando la forma reducida de las imágenes de los automorfismos. En el capítulo 5 se construyen varias representaciones lineales, que permiten resolver el problema de la palabra haciendo productos de matrices con coeficientes en unos ciertos anillos de polinomios. La forma normal del capítulo 3 se construirá usando los generadores de Birman (ecuación 1.2) y las propiedades del producto semidirecto (ver sección 1.6.1). Finalmente, en el capítulo 4 se describe una forma normal basada en un cierto orden parcial del que se puede dotar a los grupos de trenzas.

También existen algoritmos para resolver parcialmente el problema de la palabra, es decir, podemos encontrar ciertos invariantes de las palabras que representan el elemento neutro, de modo que si una palabra no los verifica sabemos que no es trivial en el grupo, aunque no podamos asegurar que sí lo sea en caso de que verifique las propiedades. Algunos de estos invariantes para los grupos de trenzas son:

- Suma de los exponentes: en cualquier grupo con relaciones homogéneas, para que un elemento represente el neutro, la suma de los exponentes de los generadores que lo representan debe ser cero. Esto se puede considerar como una representación no fiel (homomorfismo no inyectivo)  $\varphi : G \rightarrow \mathbb{Z}$ . En general, una representación no fiel nos dará una solución parcial al problema de la palabra.
- Permutación inducida: la trenza trivial es una trenza pura, por lo que la permutación inducida por cualquier palabra que represente la trenza trivial debe ser la identidad. En este caso también tenemos una representación no fiel  $\eta : B_n \rightarrow \Sigma_n$ .

Más invariantes de las trenzas se pueden encontrar en [4].

## 1.6. Definiciones y resultados adicionales

En esta sección veremos definiciones y resultados más generales que serán utilizados a lo largo del trabajo.

### 1.6.1. Producto semidirecto

**Definición 1.6.1.** Si un grupo  $G$  actúa (por la izquierda) sobre un grupo  $F$  mediante automorfismos de grupos

$$\rho : G \rightarrow \text{Aut}(F),$$

el *producto semidirecto*  $F \rtimes G$  es el grupo cuyo conjunto subyacente es el producto cartesiano  $F \times G$  y cuyo producto está definido como

$$(\delta, h)(\gamma, g) = (\delta\rho_h(\gamma), hg)$$

para  $\delta, \gamma \in F$  y  $h, g \in G$ . Análogamente se puede definir  $F \rtimes G$  utilizando una acción por la derecha.

En la definición hemos establecido que era un grupo, pero para ello tenemos que cerciorarnos de que se verifican los axiomas de grupo.

**Proposición 1.6.2.** El producto semidirecto  $F \rtimes G$  definido anteriormente es un grupo.

**Demostración.** La asociatividad y la existencia de elemento neutro se tiene inmediatamente de la definición de acción de grupo y de que  $G$  actúa sobre  $F$  mediante automorfismos. De hecho, el elemento neutro es  $e = (e_F, e_G)$ , donde  $e_F$  es el neutro de  $F$  y  $e_G$  el neutro de  $G$ . Vamos a probar entonces la existencia de elemento inverso. Dado  $(\delta, h) \in F \rtimes G$  buscamos  $(\gamma, g) \in F \rtimes G$  tal que  $(\delta, h)(\gamma, g) = (e_F, e_G) = (\gamma, g)(\delta, h)$ . Claramente se observa que  $g = h^{-1}$ . Por otro lado, tenemos

$$\delta\rho_h(\gamma) = e_F, \quad \gamma\rho_{h^{-1}}(\delta) = e_F.$$

Despejando  $\gamma$  obtenemos

$$\gamma = \rho_h^{-1}(\delta^{-1}), \quad \gamma = \rho_{h^{-1}}(\delta)^{-1}.$$

Ambas expresiones son la misma puesto que  $G$  actúa mediante automorfismos. Por tanto, el inverso de  $(\delta, h)$  es  $(\rho_{h^{-1}}(\delta^{-1}), h^{-1})$ . ■



Obsérvese que en el caso de que  $\rho_h = Id_F$  para todo  $h \in G$  se tiene el producto directo. Otro caso particularmente interesante por la frecuencia con la que aparece se da cuando  $G$  actúa por conjugación, en cuyo caso el producto sería

$$(\delta, h)(\gamma, g) = (\delta h \gamma h^{-1}, hg).$$

Por la forma en el que está definido el producto semidirecto, conseguimos conservar  $F$  y de  $G$  con cierta estructura dentro de  $F \rtimes G$ , es más

**Proposición 1.6.3.**  $F$  se puede ver como subgrupo normal de  $F \rtimes G$  mediante la aplicación  $\delta \mapsto (\delta, e_G)$ , mientras que  $G$  se puede ver como subgrupo mediante la aplicación  $h \mapsto (e_F, h)$ . Además, visto de esta forma, todo elemento de  $F \rtimes G$  se escribe de forma única como producto de un elemento de  $F$  y un elemento de  $G$ .

**Demostración.** En ambos casos es elemental probar que se tratan de morfismos inyectivos. Así que vamos a probar que la imagen de  $F$  mediante la aplicación  $\delta \mapsto (\delta, e_G)$  es un subgrupo normal de  $F \rtimes G$ . Para ello vamos a ver que  $F \times \{e_G\}$  es el núcleo de un cierto homomorfismo de grupos  $\varphi : F \rtimes G \rightarrow G$ . Este homomorfismo vendrá definido como  $\varphi(\delta, h) = h$ , el cual es fácil ver que efectivamente es homomorfismo de grupos. Claramente  $\ker \varphi = \{(\delta, h) \mid h = e_G\} = F \times \{e_G\}$ , como queríamos demostrar.

Para la segunda parte, supongamos que tenemos  $h_1 g_1 = h_2 g_2 \in F \rtimes G$  con  $h_1, h_2 \in F \times \{e_G\} \cong F$  y  $g_1, g_2 \in \{e_F\} \times G \cong G$ . Entonces consideramos la proyección  $p : F \rtimes G \rightarrow G$ , de modo que  $g_1 = p(h_1 g_1) = p(h_2 g_2) = g_2$ . Ahora basta multiplicar a derecha por  $g_1^{-1}$  para obtener  $h_1 = h_2$ . ■

Vamos a definir ahora una construcción que nos permitirá obtener productos semidirectos a partir de sucesiones exactas.

**Definición 1.6.4.** Dados tres grupos  $F$ ,  $G$  y  $H$ , se dice que  $H$  es una *extensión* de  $F$  por  $G$  si existe una sucesión exacta corta

$$1 \rightarrow F \rightarrow H \rightarrow G \rightarrow 1.$$

En el caso de que  $G$  sea un grupo finito, diremos que la extensión es *finita*.

**Proposición 1.6.5.** Si existe una la sucesión exacta escindible

$$1 \rightarrow F \rightarrow H \rightarrow G \rightarrow 1,$$

entonces  $H \cong F \rtimes G$ . El recíproco también es cierto.

**Demostración.** Supongamos que tenemos una sección  $s : G \rightarrow H$ . Como la imagen de  $F$  es isomorfa a  $F$ , podemos identificar ambos grupos. Definamos pues  $\rho : G \rightarrow \text{Aut}(F)$  como  $g \rightarrow C_{s(g)}|_F$ , donde  $C_{s(g)}$  denota la conjugación por  $s(g)$  en  $H$ . Al restringirlo a  $F$ , esto nos da un automorfismo bien definido al ser  $F$  normal en  $H$  al ser el núcleo de la aplicación  $H \rightarrow G$ . Así que hemos definido una acción mediante automorfismos que da lugar a un producto semidirecto isomorfo a  $F \rtimes G$ .

El recíproco nos lo da la Proposición 1.6.3, en la cual definimos la sección  $h \mapsto (e_F, h)$  y probamos que la imagen de  $F$  era normal en el producto semidirecto. ■

## 1.6.2. Monoïdes

**Definición 1.6.6.** Un *monoïde* es un par  $(S, *)$ , donde  $S$  es un conjunto y  $*$  :  $S \times S \rightarrow S$  es una operación binaria satisfaciendo:

- 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 monoïde, entendiéndose que en realidad es el par anterior.

De forma análoga a como se hace para grupos, podemos considerar los generadores de un monoïde y una presentación de un monoïde mediante generadores y relaciones. También se definen de forma análoga los morfismos entre monoïdes.

**Definición 1.6.7.** Dado un monoïde  $S$  con presentación  $\langle M \mid R \rangle$ , su *grupo de fracciones*  $G(S)$  es el grupo generado por la misma presentación.

Existe una aplicación natural de un monoïde 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 monoïde 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 monoïde; 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 1.6.8.** Decimos que un monoïde  $S$  se *inyecta* en su grupo de fracciones  $G(S)$ , si el morfismo de monoïdes  $\iota : S \rightarrow G(S)$  dado por  $\iota(a) = a$  es inyectivo.

**Definición 1.6.9.** Decimos que un monoide  $S$  satisface las *condiciones de Ore* [27] si se cumple:

- $S$  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 1.6.10.** Si un monoide satisface las condiciones de Ore, entonces se inyecta en su grupo de fracciones [9, Teorema 1.23].

### 1.6.3. Espacios recubridores

**Definición 1.6.11.** Sea  $X$  un espacio topológico. Un *espacio recubridor* de  $X$  es un espacio topológico  $\tilde{X}$  junto con una aplicación continua sobreyectiva  $p : \tilde{X} \rightarrow X$ , llamada *aplicación recubridora*, tal que para todo  $x \in X$  existe un entorno  $U$  de  $x$  de modo que  $p^{-1}(U)$  es unión disjunta de abiertos de  $\tilde{X}$  homeomorfos a  $U$ , llamados *hojas*. El espacio  $p^{-1}(x)$  se llama *fibra* de  $x$ .

**Ejemplo 1.6.12.** El ejemplo más habitual de espacio recubridor se da para  $S^1$  usando como espacio recubridor  $\mathbb{R}$  con la aplicación  $p : \mathbb{R} \rightarrow S^1$  dada por  $p(t) = e^{2\pi it}$ .

**Definición 1.6.13.** Un *isomorfismo* de espacios recubridores  $p_1 : \tilde{X}_1 \rightarrow X$  y  $p_2 : \tilde{X}_2 \rightarrow X$  es un homeomorfismo  $f : \tilde{X}_1 \rightarrow \tilde{X}_2$  tal que  $p_1 = p_2 f$ .

**Definición 1.6.14.** Para un espacio recubridor  $p : \tilde{X} \rightarrow X$ , los isomorfismos  $\tilde{X} \rightarrow \tilde{X}$  se denominan *transformaciones recubridoras* (*deck transformations*).

Claramente, la inversa de un isomorfismo de espacios recubridores es isomorfismo y la composición de isomorfismos es isomorfismo. Por tanto, el conjunto de transformaciones recubridoras forma un grupo con elemento neutro la identidad denotado  $G(\tilde{X})$ .

**Ejemplo 1.6.15.** En el espacio recubridor el ejemplo 1.6.12, las transformaciones recubridoras son las aplicaciones de la forma  $f(t) = t + n$  para cada  $n \in \mathbb{Z}$ , por lo que  $G(\tilde{X}) \cong \mathbb{Z}$ . En particular,  $\mathbb{Z}$  actúa sobre el espacio recubridor mediante cada  $f$ .

**Definición 1.6.16.** Dado un espacio topológico  $X$  y un grupo  $G$ , se dice que un espacio recubridor  $\tilde{X}$  *se corresponde* con  $G$  si  $\pi_1(\tilde{X}) = G$ .

**Ejemplo 1.6.17.** Podemos dar un espacio recubridor de  $S^1$  que se corresponda, por ejemplo, al grupo libre de dos elementos  $\langle a, b \rangle$ . Para ello, fijado un punto base  $x \in S^1$ , basta tomar como espacio recubridor  $S^1 \vee S^1$  con punto base en el vértice, que denotaremos  $y$ . Etiquetamos cada una de las circunferencias como  $a$  y  $b$  respectivamente.

La aplicación  $p : S^1 \vee S^1 \rightarrow S^1$  enviando  $y \mapsto x$  e identificando  $a$  con  $b$  es claramente sobreyectiva y continua. Por tanto  $p$  es una aplicación recubridora. Además, es bien sabido que  $\pi_1(S^1 \vee S^1) = \langle a, b \rangle$ .

A continuación vamos a ver una serie de definiciones y resultados cuyas pruebas aparecen en [20], en la sección *Covering Spaces*, que usaremos más adelante.

**Definición 1.6.18.** Un espacio topológico  $X$  se dice que es *semilocalmente simplemente conexo* si todo punto  $x \in X$  tiene un entorno  $U$  tal que cualquier lazo de  $U$  basado en  $x$  es contráctil en  $X$ .

Nótese que esta condición no implica que  $U$  sea simplemente conexo, pues la contracción del lazo no se tiene por qué realizar enteramente dentro de  $U$ . Ejemplo de espacio topológico no semilocalmente simplemente conexo es el *pendiente hawaiano*<sup>1</sup>.

**Proposición 1.6.19.** Dado un espacio recubridor  $p : \tilde{X} \rightarrow X$ , una homotopía  $f_t : Y \rightarrow X$  y una aplicación continua  $\tilde{f}_0 : Y \rightarrow \tilde{X}$  levantando a  $f_0$ , se tiene que existe una única homotopía  $\tilde{f}_t : Y \rightarrow \tilde{X}$  de  $\tilde{f}_0$  que levanta a  $f_t$ .

En adelante, dado un punto base  $x \in X$ , supondremos fijado un punto base  $\tilde{x} \in \tilde{X}$  con  $\tilde{x} \in p^{-1}(x)$ .

**Proposición 1.6.20.** La aplicación  $p_* : \pi_1(\tilde{X}) \rightarrow \pi_1(X)$  inducida por  $p : \tilde{X} \rightarrow X$  es inyectiva. El subgrupo imagen  $p_*(\pi_1(\tilde{X}))$  consiste en las clases de homotopía de los lazos de  $X$  basados en  $x$  cuyos levantamientos a  $\tilde{X}$  son lazos basados en  $\tilde{x}$ .

**Proposición 1.6.21.** Sea  $X$  conexo por caminos, localmente conexo por caminos y semilocalmente simplemente conexo. Entonces, para todo subgrupo  $H \subseteq \pi_1(X)$ , existe un espacio recubridor  $p : \tilde{X} \rightarrow X$  tal que  $p_*(\pi_1(\tilde{X})) = H$  si se elige adecuadamente el punto base  $\tilde{x}$ .

Con esta última proposición, podemos asociar a cada subgrupo de  $\pi_1(X)$  un espacio recubridor  $\tilde{X}$  que se corresponda con ese subgrupo.

---

<sup>1</sup>[https://en.wikipedia.org/wiki/Hawaiian\\_earring](https://en.wikipedia.org/wiki/Hawaiian_earring)

# Capítulo 2

## Automorfismos del grupo libre

Vamos a empezar este capítulo dando otra interpretación de los grupos de trenzas. Aunque originalmente Artin visualizó las trenzas como una colección de cuerdas, existe una representación natural como automorfismos del grupo libre  $F_n$  de rango  $n$ . Definiremos esta representación por medio de *mapping classes*.

### 2.1. Representación del grupo de trenzas como automorfismos del grupo libre

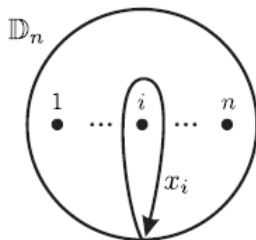


Figura 2.1: Los lazos  $x_1, \dots, x_n$  son generadores de  $\pi_1(\mathbb{D}_n)$ .

Observamos que el grupo fundamental del disco agujereado  $n$  veces, denotado  $\mathbb{D}_n$ , es precisamente el grupo libre de rango  $n$ , es decir,  $\pi_1(\mathbb{D}_n) = F_n$ . Si fijamos un punto base, digamos, en el borde del disco, podemos tomar como generadores los lazos  $x_1, \dots, x_n$  descritos en la Figura 2.1. Ahora, una trenza  $\beta \in B_n$  puede ser vista como un automorfismo de  $\mathbb{D}_n$  que es la identidad en el borde  $\partial(\mathbb{D}_n)$  salvo isotopía (que también fija los puntos de  $\partial(\mathbb{D}_n)$ ), así que  $\beta$  induce una acción bien definida sobre  $\pi_1(\mathbb{D}_n) = F_n$ , donde un lazo  $\gamma \in \pi_1(\mathbb{D}_n)$  es enviado a  $\beta(\gamma)$ . Esta acción es claramente un homomorfismo de grupos (respeta la concatenación), el cual es biyectivo pues  $\beta^{-1}$  da lugar a la acción inversa. Entonces,  $\beta$  induce un automorfismo de  $F_n$ , y esto nos da la representación

$$\begin{aligned} \rho : B_n &\rightarrow \text{Aut}(F_n) \\ \beta &\mapsto \rho_\beta. \end{aligned}$$

El automorfismo  $\rho_\beta$  puede ser descrito fácilmente cuando  $\beta = \sigma_i$ , identificando la imagen de los generadores  $x_1, \dots, x_n$  de  $F_n$  (ver Figura 2.2), esto es:

$$\rho_{\sigma_i}(x_i) = x_{i+1}, \quad \rho_{\sigma_i}(x_{i+1}) = x_{i+1}^{-1} x_i x_{i+1}, \quad \rho_{\sigma_i}(x_j) = x_j \quad (j \neq i, i+1).$$

El automorfismo  $\rho_{\sigma_i^{-1}} = \rho_{\sigma_i}^{-1}$  puede ser deducido fácilmente a partir de  $\rho_{\sigma_i}$ , lo que nos da

$$\rho_{\sigma_i}^{-1}(x_i) = x_i x_{i+1} x_i^{-1}, \quad \rho_{\sigma_i}^{-1}(x_{i+1}) = x_i, \quad \rho_{\sigma_i}^{-1}(x_j) = x_j \quad (j \neq i, i+1).$$

Para una trenza general  $\beta$ , escrita como producto de  $\sigma_1, \dots, \sigma_{n-1}$  y sus inversas, el automorfismo  $\rho_\beta$  es simplemente la composición de los correspondientes automorfismos inducidos por cada letra.

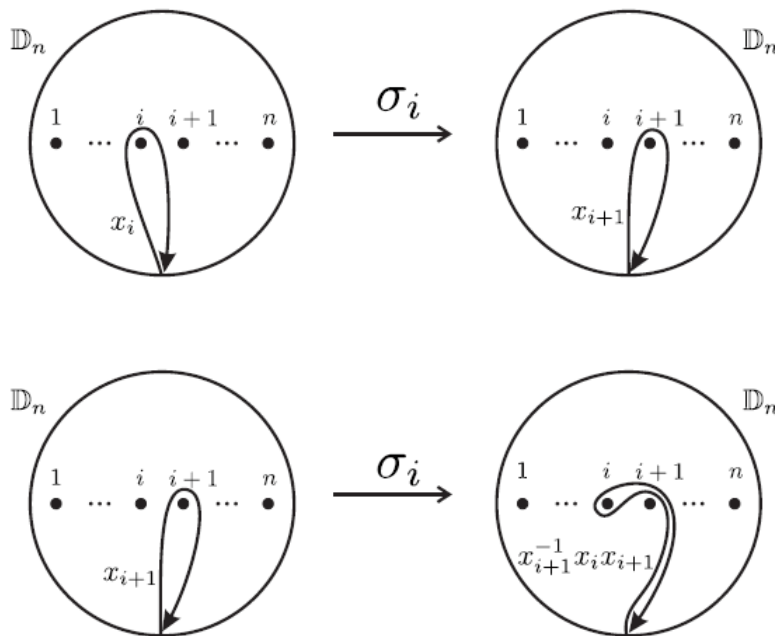


Figura 2.2: Acción de  $\sigma_i$  sobre los generadores  $x_i$  y  $x_{i+1}$ .

Es fácil ver que  $\rho$  está bien definido algebraicamente, ya que  $\rho_{\sigma_i \sigma_j} = \rho_{\sigma_j \sigma_i}$  si  $|i - j| > 1$ , y  $\rho_{\sigma_i \sigma_j \sigma_i} = \rho_{\sigma_j \sigma_i \sigma_j}$  si  $|i - j| = 1$ .

**Teorema 2.1.1.** La representación anterior es fiel, es decir, dos trenzas están representadas por el mismo automorfismo si y solo si son la misma.

La prueba de este resultado se puede encontrar en [7]. Lo significativo ahora es que esta representación nos permite resolver el problema de la palabra como explicaremos a continuación.

## 2.2. Solución al problema de la palabra

El hecho de que las trenzas puedan ser vistas fielmente como automorfismos del grupo libre  $F_n$  da lugar inmediatamente a una solución al problema de la palabra en  $B_n$ . Dadas dos trenzas  $\beta_1$  y  $\beta_2$ , expresadas como palabras en  $\sigma_1, \dots, \sigma_{n-1}$  y sus inversas, se pueden calcular sus correspondientes automorfismos  $\rho_{\beta_1}$  y  $\rho_{\beta_2}$ . Entonces  $\beta_1 = \beta_2$  si y solo si  $\rho_{\beta_1} \equiv \rho_{\beta_2}$ , lo cual ocurre si y solo si  $\rho_{\beta_1}(x_i) = \rho_{\beta_2}(x_i) \in F_n$  para  $i = 1, \dots, n$ . Como el problema de la palabra en  $F_n$  tiene solución conocida (basta calcular las palabras reducidas asociadas a  $\rho_{\beta_1}(x_i)$  y  $\rho_{\beta_2}(x_i)$ ), esto resuelve el problema de la palabra en  $B_n$ .

Merece la pena remarcar que este algoritmo no es en absoluto eficiente (de hecho tiene complejidad exponencial) y existen otros que lo son mucho más, pero esta es históricamente la primera solución conocida para el problema de la palabra en  $B_n$ , descubierta por Artin y publicada en [2].

Veamos un ejemplo de cómo se aplica este método.

**Ejemplo 2.2.1.** Dado  $n \geq 3$ , sean  $\beta_1 = \sigma_i \sigma_{i+1}^{-1} \sigma_i$  y  $\beta_2 = \sigma_{i+1} \sigma_i^{-1} \sigma_{i+1}$  para algún  $1 \leq i \leq n-2$ . Nos preguntamos si estas palabras representan la misma trenza. Serán la misma si y solo si  $\rho_{\beta_1}(x_j) = \rho_{\beta_2}(x_j)$  para todo  $1 \leq j \leq n-1$ , por lo que para probar que son distintas basta encontrar un generador del grupo libre para el que sus imágenes no coincidan. Sea pues  $x_i$ . Tenemos por un lado

$$\begin{aligned} \rho_{\beta_1}(x_i) &= \rho_{\sigma_i} \rho_{\sigma_{i+1}^{-1}} \rho_{\sigma_i}(x_i) = \rho_{\sigma_i} \rho_{\sigma_{i+1}^{-1}}(x_{i+1}) = \rho_{\sigma_i}(x_{i+1} x_{i+2} x_{i+1}^{-1}) = \\ & x_{i+1}^{-1} x_i x_{i+1} x_{i+2} x_{i+1}^{-1} x_i^{-1} x_{i+1} \end{aligned}$$

y por otro

$$\rho_{\beta_2}(x_i) = \rho_{\sigma_{i+1}} \rho_{\sigma_i^{-1}} \rho_{\sigma_{i+1}}(x_i) = \rho_{\sigma_{i+1}} \rho_{\sigma_i^{-1}}(x_i) = \rho_{\sigma_{i+1}}(x_{i+1}) = x_{i+2}.$$

Claramente  $x_{i+2} \neq x_{i+1}^{-1} x_i x_{i+1} x_{i+2} x_{i+1}^{-1} x_i^{-1} x_{i+1}$  en  $F_n$ , por lo que  $\beta_1 \neq \beta_2$ .

# Capítulo 3

## Peinado de trenzas

En este capítulo veremos un algoritmo para resolver el problema de la palabra basado en la posibilidad de expresar las trenzas puras como elementos de un producto semidirecto de grupos libres. El algoritmo requerirá una técnica denominada *peinado de trenzas* para que el orden de los factores sea el adecuado.

### 3.1. Sucesiones exactas

Hay dos sucesiones exactas relacionadas con los grupos de trenzas bien conocidas. La primera es bastante simple: a cada trenza de  $B_n$  se le puede asociar la permutación que induce en sus cuerdas, esto es, un elemento del grupo simétrico  $\Sigma_n$ . Esto da lugar a un homomorfismo de grupos bien definido  $\eta : B_n \rightarrow \Sigma_n$ . Nótese que  $\eta(\sigma_i) = (i \ i+1)$  para cada  $i = 1, \dots, n-1$ . El núcleo de  $\eta$  es el subgrupo de  $B_n$  formado por las trenzas que inducen la permutación trivial, esto es, el grupo de trenzas puras  $PB_n$ . Por tanto, tenemos una sucesión exacta:

$$1 \rightarrow PB_n \rightarrow B_n \xrightarrow{\eta} \Sigma_n \rightarrow 1. \quad (3.1)$$

Hay también una aplicación que relaciona las trenzas puras de distintos índices. Concretamente, dada una trenza pura  $\beta \in PB_{n+1}$ , se puede eliminar, por ejemplo, la última cuerda para obtener una trenza pura  $\rho(\beta) \in PB_n$ . Esto da lugar a un homomorfismo de grupos bien definido  $\rho : PB_{n+1} \rightarrow PB_n$ , que es claramente sobreyectivo. El núcleo de esta aplicación consiste en las trenzas puras de  $PB_{n+1}$  cuyas  $n$  primeras cuerdas forman la trenza trivial. Salvo isotopía, podemos considerar que estas  $n$  primeras cuerdas están en posición vertical. Si miramos este tipo de elementos como lazos en el espacio de configuración  $M_{n+1}$ , se corresponden al movimiento del  $(n+1)$ -ésimo punto mientras el resto de puntos permanecen quietos. Esto es por supuesto equivalente al movimiento de un punto en el plano complejo agujereado  $n$  veces  $\mathbb{C}_n$ . En otras palabras,  $\ker(\rho) = \pi_1(\mathbb{C}_n) \cong F_n$ , por lo que tenemos la sucesión exacta:

$$1 \rightarrow F_n \rightarrow PB_{n+1} \xrightarrow{\rho} PB_n \rightarrow 1. \quad (3.2)$$

En esta sucesión exacta, si  $F_n$  está generado por  $x_1, \dots, x_n$ , vamos a ver que podemos definir  $\iota : F_n \rightarrow PB_{n+1}$

$$\iota(x_i) = A_{i,n+1},$$



donde  $A_{i,n+1}$  son generadores de Birman (1.2). La aplicación está bien definida, es decir, la trenza resultante es pura por definición de los  $A_{i,n+1}$ . Para que sea la aplicación correcta y la sucesión sea exacta,  $\iota$  debe ser inyectiva, que es lo siguiente que vamos a probar.

**Proposición 3.1.1.** La aplicación  $\iota$  anteriormente definida es inyectiva.

**Demostración.** La idea de esta demostración será interpretar la sucesión exacta 3.2 en términos de otra que sabemos que es exacta y comprobar que  $\iota$  es la aplicación correspondiente con esa otra interpretación.

Para  $n \geq 1$  consideramos la aplicación

$$\begin{aligned} p: M_{n+1} &\longrightarrow M_n \\ (z_1, \dots, z_{n+1}) &\mapsto (z_1, \dots, z_n). \end{aligned} \tag{3.3}$$

Nótese que que cada fibra  $p^{-1}((z_1, \dots, z_n))$  es homeomorfa a  $\mathbb{C} \setminus \{z_1, \dots, z_n\} = \mathbb{C}_n$ . Como este espacio retrae con deformación sobre  $S^1 \vee \dots \vee S^1$ , su grupo fundamental es  $F_n$ . De la sucesión exacta larga de grupos de homotopía asociada a  $p$  de este fibrado [20] obtenemos:

$$\pi_2(\mathbb{C}_n) \rightarrow \pi_2(M_{n+1}) \rightarrow \pi_2(M_n) \rightarrow \pi_1(\mathbb{C}_n) \rightarrow \pi_1(M_{n+1}) \rightarrow \pi_1(M_n) \rightarrow 1.$$

Se sabe que  $\pi_2(\mathbb{C}_n) = 1$  [20]. Por otra parte,  $\pi_2(M_1) = \pi_2(\mathbb{C}) = 1$ . En la sucesión exacta anterior, esto implica que  $\pi_2(M_2) = 1$ . Inductivamente se prueba que  $\pi_2(M_n) = 1$  para todo  $n$ . Esto da lugar a la sucesión exacta

$$1 \rightarrow \pi_1(\mathbb{C}_n) \rightarrow \pi_1(M_{n+1}) \rightarrow \pi_1(M_n) \rightarrow 1,$$

que por definición es equivalente a 3.2.

Si denotamos  $j : \pi_1(\mathbb{C}_n) \rightarrow \pi_1(M_{n+1})$  a la aplicación natural de la anterior sucesión exacta, basta ver que  $j$  coincide con  $\iota$  para probar el resultado. Fijemos un punto base  $x$  en  $\mathbb{C}_n$  (véase la Figura 3.1).

Como se puede comprobar, un lazo basado en  $x$  en torno al agujero  $i$ -ésimo, que se corresponde con el generador  $x_i$  de  $F_n$ , se transforma de modo natural en el movimiento del punto  $n + 1$  tal como se describe en la figura. Este movimiento es el que se corresponde con la trenza  $A_{i,n+1}$ , por lo que esta transformación es justamente la aplicación  $\iota$ . ■

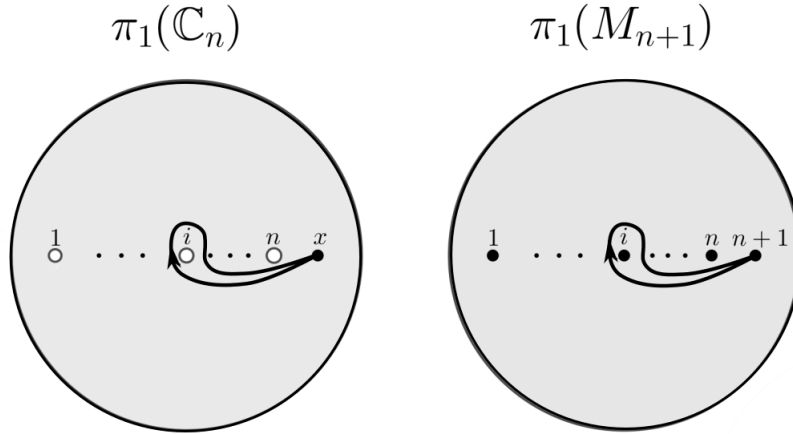


Figura 3.1: Inclusión de  $F_n$  en  $PB_{n+1}$ .

### 3.2. Trenzas puras como producto semidirecto de grupos libres

Un hecho importante sobre la sucesión exacta 3.2 es que escinde. Para verlo, consideremos la aplicación  $s : M_n \rightarrow M_{n+1}$  entre los espacios de configuración dada por  $s((z_1, \dots, z_n)) = (z_1, \dots, z_n, |z_1| + \dots + |z_n| + 1)$ . Esta aplicación es una sección para el fibrado 3.3. Esto es fácil de ver, pues al añadirse un punto con módulo  $|z_1| + \dots + |z_n| + 1$ , dicho punto nunca coincidirá con los anteriores. Por tanto,  $s$  da lugar a una sección que denotaremos de igual modo  $s : PB_n \rightarrow PB_{n+1}$ , por lo que la sucesión exacta escinde. La forma de interpretar esta sección es la siguiente:

Para cada  $n$  fijo, podemos considerar, salvo homeomorfismo, las trenzas de  $PB_n$  como colecciones de cuerdas en  $\mathbb{D}^2 \times [0, 1]$ , donde  $\mathbb{D}^2 \subset \mathbb{C}$  es el disco unidad, y las trenzas de  $PB_{n+1}$  como colecciones de cuerdas en  $\mathbb{C} \times [0, 1]$ , donde las primeras  $n$  cuerdas están en  $\mathbb{D}^2 \times [0, 1]$  y la última cuerda está en el exterior de dicho espacio. Entonces,  $s$  añade una sola cuerda vertical (salvo isotopía) basada en un punto  $z_{n+1} \in \mathbb{C} \setminus \mathbb{D}^2$ . Esto es claramente un homomorfismo de grupos que es una sección para  $\rho$ . Por tanto, tenemos la sucesión exacta con sección

$$1 \longrightarrow F_n \xrightarrow{\iota} PB_{n+1} \begin{array}{c} \xleftarrow{\rho} \\ \xrightarrow{s} \end{array} PB_n \longrightarrow 1.$$

Por exactitud,  $\iota(F_n) = \ker(\rho)$ , por lo que  $\iota(F_n)$  es normal en  $PB_{n+1}$ , así que por la Proposición 1.6.5, tenemos que  $PB_{n+1} \cong F_n \rtimes PB_n$ . Reiterando este proceso y teniendo en cuenta que  $PB_2 \cong F_1$ , llegamos a que

$$PB_{n+1} \cong F_n \rtimes (F_{n-1} \rtimes \dots \rtimes (F_3 \rtimes (F_2 \rtimes F_1)) \dots).$$

De igual modo, podríamos empezar con  $PB_{n+1} \cong PB_n \times F_n$ , lo que nos daría

$$PB_{n+1} \cong ((\cdots((F_1 \times F_2) \times F_3) \times \cdots \times F_{n-1}) \times F_n).$$

Por tanto, cada trenza de  $PB_{n+1}$  se expresa de forma única (Proposición 1.6.3) como producto de elementos de los grupos libres desde  $F_1$  hasta  $F_n$ , donde los generadores pueden ser vistos como los generadores de Birman de las trenzas puras. Esto nos permitirá resolver el problema de la palabra en los grupos de trenzas puras mediante un proceso denominado *peinado de trenzas*, consistente en expresar una trenza pura como un elemento del producto semidirecto anterior. El nombre es debido a que, geoméricamente, la trenza original se convierte en una trenza en que en cada nivel solo se mueve una cuerda (en el nivel  $j$  se mueve la cuerda  $j$  mediante los generadores  $A_{ij}$  con  $i < j$  de  $F_{j-1}$ , ver Figura 3.2).

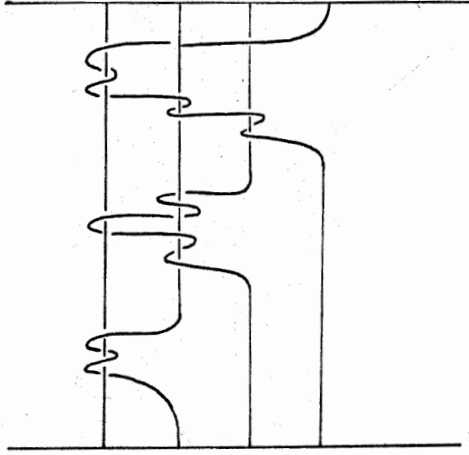


Figura 3.2: Trenza peinada.

### 3.3. Solución al problema de la palabra

Supongamos que tenemos que decidir si una palabra  $\beta \in B_n$  representa el elemento neutro. En primer lugar, mediante el homomorfismo  $\eta$  de la sucesión exacta 3.1 comprobamos si la permutación que induce  $\beta$  es la identidad. En caso de no serlo, sabemos que  $\beta$  no es trivial. Si  $\eta(\beta) = Id \in \Sigma_n$ , entonces  $\beta$  es pura por definición, por lo que trataremos de expresarla como elemento del producto semidirecto de grupos libres, ya que será trivial si y solo si cada uno de los factores lo es. Sin embargo, para conseguir esta expresión tenemos que escribir  $\beta$  como producto de los generadores de Birman, puesto que estos son los que representan cada grupo libre.

Para ello, hagamos la siguiente consideración: dada una permutación  $\tau \in \Sigma_n$  podemos encontrar una trenza que induzca esta permutación. Además podemos hacerlo de forma inyectiva, pues para permutaciones distintas daremos trenzas distintas. Esto da lugar a una *sección conjuntista* (no es homomorfismo de grupos) en la sucesión exacta 3.1  $\varphi : \Sigma_n \rightarrow B_n$ . Estas trenzas pueden ser elegidas de modo que todos los cruces sean positivos y cada par de cuerdas solo se cruce como máximo una vez. Para ello, expresamos la permutación como producto de trasposiciones  $(i \ i + 1)$  con  $1 \leq i \leq n - 1$  de la forma más corta posible y sustituimos cada  $(i \ i + 1)$  por  $\sigma_i$ . A estas trenzas las llamaremos *trenzas simples* o *trenzas de permutación*. Las trenzas simples tendrán la forma  $\sigma_{i_1} \cdots \sigma_{i_k}$ , de modo que  $\sigma_{i_j} \neq \sigma_{i_{j+1}}$  en cualquier palabra que represente a la trenza.

Vamos a explicar en qué consiste entonces el algoritmo para resolver el problema de la palabra. Supongamos que tenemos una trenza pura  $\beta = \sigma_{i_1}^{\pm 1} \sigma_{i_2}^{\pm 1} \cdots \sigma_{i_k}^{\pm 1}$ . Vamos a multiplicar a izquierda y derecha cada generador por unas ciertas trenzas de permutación y sus inversas, de modo que nos quede un producto de trenzas puras que, por la forma que tendrá, será más sencillo de expresar en función de los generadores de Birman.

Sea  $s_j = \eta(\sigma_{i_1}^{\pm 1} \cdots \sigma_{i_j}^{\pm 1}) = \eta(\beta_j)$  para todo  $j = 0, \dots, k$ . Obsérvese que  $s_0 = s_k = Id$ . Ahora podemos escribir

$$\beta = (\varphi(s_0)\sigma_{i_1}^{\pm 1}\varphi(s_1)^{-1})(\varphi(s_1)\sigma_{i_2}^{\pm 1}\varphi(s_2)^{-1}) \cdots (\varphi(s_{k-1})\sigma_{i_k}\varphi(s_k))$$

Cada paréntesis es una trenza pura pues

$$\eta(\varphi(s_{j-1})\sigma_{i_j}^{\pm 1}\varphi(s_j)^{-1}) = s_{j-1}\eta(\sigma_{i_j}^{\pm 1})s_j^{-1} = \eta(\beta_{j-1})\eta(\sigma_{i_j}^{\pm 1})\eta(\beta_j^{-1}) = \eta(1) = Id.$$

Obsérvese que muchos términos se cancelarán y otros quedarán con una cierta simetría que facilitará expresarlos como producto de los generadores de Birman. En cualquier caso, como hay  $n!$  trenzas de permutación y  $2(n - 1)$  generadores contando las potencias negativas, hay a lo sumo  $n!2(n - 1)$  factores distintos para expresarlos como producto de los generadores de Birman. Al ser una cantidad finita, siempre es factible hacer una lista para transformarlos automáticamente. Para una forma sistemática de realizar esta transformación consultar [18]. Una vez que tengamos una palabra de la forma

$$A_{i_1, j_1}^{\pm 1} \cdots A_{i_r, j_r}^{\pm 1},$$

basta usar los dos conjuntos de relaciones del grupo de trenzas puras definidas en el primer capítulo para reordenarlos de modo que queden de la forma

$$w_n \cdots w_2$$

donde cada  $w_j$  es una palabra en los generadores  $A_{ij}$ . Equivalentemente podemos reordenarlas para que queden en orden contrario. Una vez expresada así, ya basta

comprobar si alguno de los factores no es trivial, que como cada uno está en un grupo libre sabemos que se puede resolver.

**Ejemplo 3.3.1.** Sea  $\beta = \sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_3^{-1}\sigma_1 \in B_4$ . Vamos a decidir si  $\beta$  es trivial. En primer lugar calculamos su permutación inducida,  $(12)(23)(34)(34)(12) = Id$ , por lo que la trenza es pura. Así que vamos utilizar las trenzas simples para expresarla como producto de los generadores de Birman.

$$\begin{aligned} (1\underline{\sigma_1\sigma_1^{-1}})(\underline{\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1}})(\underline{\sigma_1\sigma_2\sigma_2^{-1}\sigma_1^{-1}})(\underline{\sigma_1\sigma_3^{-1}\sigma_3^{-1}\sigma_1^{-1}})(\underline{\sigma_1\sigma_3\sigma_3^{-1}\sigma_1^{-1}})(\underline{\sigma_1\sigma_1}) &= \\ (\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1})(\sigma_1\sigma_1^{-1}\sigma_3^{-1}\sigma_3^{-1})A_{12} &= \\ (\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1})A_{34}^{-1}A_{12}. \end{aligned}$$

Nos quedan entonces un factor que expresar como producto de los generadores de Birman. Tenemos que

$$\begin{aligned} \sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1} &= \sigma_2^{-1}\underline{\sigma_2\sigma_1\sigma_2\sigma_2^{-1}\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1}} = (\sigma_2^{-1})\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1} \\ &= (\sigma_2^{-1})\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_2^{-1}\underline{\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}}(\sigma_2) = (\sigma_2^{-1})\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\underline{\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}}(\sigma_1^{-1}\sigma_2) \\ &= (\sigma_2^{-1})\sigma_1\sigma_2\sigma_1\underline{\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}}(\sigma_1^{-1}\sigma_1^{-1}\sigma_2) = (\sigma_2^{-1})\sigma_1\sigma_2\sigma_1\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}(\sigma_1^{-1}\sigma_1^{-1}\sigma_2) \\ &= (\sigma_2^{-1})(\sigma_1^{-1}\sigma_1^{-1}\sigma_2) = (\sigma_2^{-2})(\sigma_2\sigma_1^{-2}\sigma_2^{-1})(\sigma_2^2) \\ &= A_{23}^{-1}A_{13}^{-1}A_{23} \end{aligned}$$

Este hecho se puede observar geoméricamente en la Figura 3.3.

Por tanto,  $\beta = A_{23}^{-1}A_{13}^{-1}A_{23}A_{34}^{-1}A_{12}$ . Todavía no la tenemos de la forma buscada pues el orden no es el correcto. Por tanto, usamos las relaciones del grupo de trenzas puras para expresarla en el orden correcto. De todos modos, en este caso ya sabemos que no será trivial porque aparece  $A_{12}$ , generador de  $F_1$ , pero continuaremos el algoritmo por mostrar un ejemplo completo.

En este caso moveremos  $A_{12}$  hacia la izquierda con los siguientes pasos.

$$\begin{aligned} A_{23}^{-1}A_{13}^{-1}A_{23}A_{34}^{-1}A_{12} &= \\ A_{23}^{-1}A_{13}^{-1}A_{23}A_{12}A_{34}^{-1} &= \\ A_{23}^{-1}A_{13}^{-1}A_{12}(A_{13}A_{23}A_{13}^{-1})A_{34}^{-1} &= \\ A_{23}^{-1}A_{12}(A_{13}A_{23}A_{13}^{-1}A_{23}^{-1}A_{13}^{-1}A_{13}A_{23}A_{13}^{-1})A_{34}^{-1} &= \\ A_{12}(A_{13}A_{23}^{-1}A_{13}^{-1}A_{13}A_{23}A_{13}^{-1}A_{23}^{-1}A_{13}^{-1}A_{13}A_{23}A_{13}^{-1})A_{34}^{-1} &= \\ A_{12}A_{13}^{-1}A_{34}^{-1}. \end{aligned}$$

Tal como adelantábamos, claramente no es trivial.

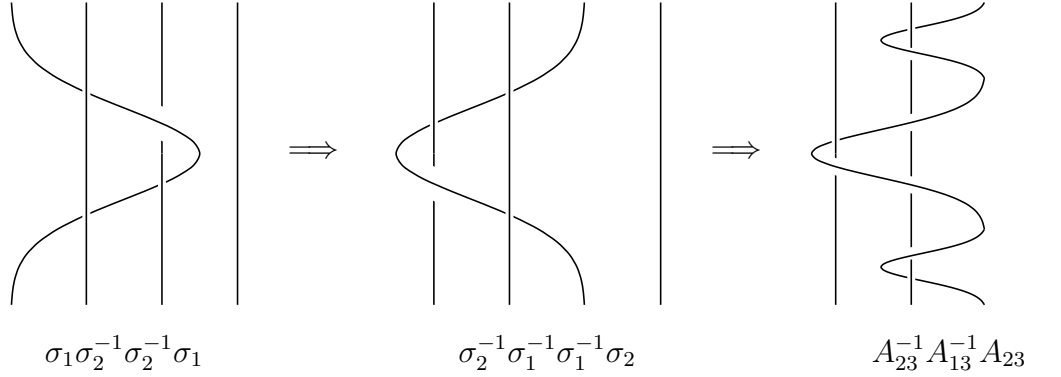


Figura 3.3: En el primer paso tiramos hacia la izquierda de la tercera cuerda, arras-trando con ella la primera, y en el segundo la vamos doblando.

En el ejemplo anterior hemos podido hacer varias cancelaciones en el último paso, sin embargo, en general la palabra se va haciendo exponencialmente más larga durante el proceso, convirtiendo este algoritmo en altamente ineficiente, hasta el punto de que el propio Artin comentara [3]:

*“Although it has been proved that every braid can be deformed into a similar normal form, the writer is convinced that any attempt to carry this out on a living person would only lead to violent protests and discrimination against mathematics. He would therefore discourage such an experiment”<sup>1</sup>.*

Sin embargo, versiones mejoradas hasta tiempo polinomial pueden ser encontradas en [19].

---

<sup>1</sup>“Aunque ha sido probado que toda trenza puede ser deformada en una forma normal similar, el escritor está convencido de que cualquier intento de llevar esto a cabo por una persona viva solo llevaría a violentas protestas y discriminación hacia las matemáticas. Por tanto, desaconsejaría tal experimento”.

# Capítulo 4

## Formas normales

El objetivo de este capítulo será 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. Los resultados referentes a *Word processing in groups* [15] se pueden encontrar en el capítulo 9 de dicho libro.

### 4.1. Estructura de Garside

Obsérvese que la presentación 1.1 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 4.1.1.** 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 4.1.2.** Definimos en  $B_n^+$  el orden parcial  $\preceq$  tal que dadas  $a, b \in B_n^+$ ,  $a \preceq b$  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 4.1.3.** La relación  $\preceq$  es una relación de orden.

**Demostración.** Dada  $x \in B_n^+$  se tiene que  $x \preceq x \cdot 1 = x$ , por lo que se cumple la propiedad reflexiva. Si  $x, y \in B_n^+$  con  $x \preceq y$  e  $y \preceq x$ , 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, tenemos necesariamente que  $a = b = 1$ , por lo que  $x = y$ , cumpliéndose la propiedad antisimétrica. Por último, supongamos que  $x \preceq y \preceq z$  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  $x \preceq z$ , lo que prueba la propiedad transitiva. ■

Nótese que  $\preceq$  es invariante por multiplicación a izquierda, esto es,  $a \preceq b$  implica  $xa \preceq xb$  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  $\preceq$ . Esto es, dadas  $a, b \in B_n^+$ , ¿existe un único  $d \in B_n^+$  tal que  $d \preceq a$ ,  $d \preceq b$  y  $d' \preceq d$  para todo  $d'$  prefijo común de  $a$  y  $b$ ? ¿Y existe un único  $m \in B_n^+$  tal que  $a \preceq m$ ,  $b \preceq m$  y  $m \preceq m'$  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 4.1.4.** 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  $a \preceq b$  ni recíprocamente. Por ejemplo,  $\sigma_1 \preceq \sigma_1\sigma_2$ , pero claramente  $\sigma_1\sigma_2 \not\succeq \sigma_1$ .

El punto clave en el trabajo de Garside fue demostrar mediante métodos elementales que  $\sigma_i$  y  $\sigma_j$  tienen mínimo común múltiplo en  $B_n^+$ . En concreto:

**Proposición 4.1.5.** ([17, Teorema 1.2]) El mínimo común múltiplo de los generadores  $\sigma_i$  y  $\sigma_j$  viene dado por

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

Garside prueba al mismo tiempo que  $B_n^+$  es cancelativo, es decir,  $xay = xby$  implica  $a = b$  para todo  $a, b, x, y \in B_n^+$ .

Como las relaciones de 1.1 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. Aunque Garside no lo menciona explícitamente, un argumento inductivo en esta longitud utilizando la cancelatividad permite probar a partir del resultado anterior que todo par de elementos tiene de  $B_n^+$  un único mínimo común múltiplo y un único máximo común divisor, tal como se prueba en [12].

Garside después estudia el siguiente elemento especial.

**Definición 4.1.6.** 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 4.1.7.** Se verifican:

1.  $\Delta = \sigma_1 \vee \cdots \vee \sigma_{n-1}$  [17, Lema 1].
2.  $\sigma_i \Delta = \Delta \sigma_{n-i}$  para todo  $i = 1, \dots, n-1$  [17, Lema 4].

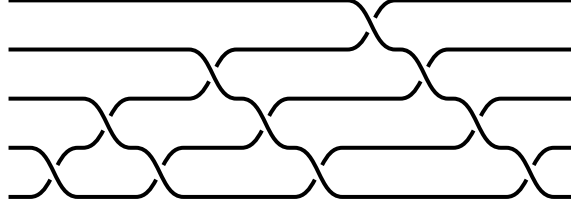


Figura 4.1: La trenza fundamental  $\Delta_5$ .

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

**Proposición 4.1.8.** Se cumplen:

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  $a \preceq \Delta^m$  y  $\Delta^m \succeq a$ , donde  $m \geq 0$  es la longitud de  $a$ .

**Demostración.**

1. En primer lugar, se tiene para  $k > i \geq 1$  que  $\sigma_i(\sigma_k \cdots \sigma_1) = (\sigma_k \cdots \sigma_1)\sigma_{i+1}$ . En efecto, usando las relaciones del monoide de trenzas positivas

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

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

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

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

$$\sigma_i \Delta^2 = \Delta \sigma_{n-i} \Delta = \Delta^2 \sigma_i.$$

3. Probamos  $a \preceq \Delta^m$  donde  $m$  es la longitud de  $a$  por inducción en  $m$ . Evidentemente,  $1 \preceq \Delta^0 = 1$ . Para una palabra de longitud 1 también es claro porque  $\sigma_i \preceq \Delta$  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  $m = 1$ ,

$$a \preceq \Delta^{m-1} \Rightarrow \sigma_j a \preceq \sigma_j \Delta^{m-1} = \Delta^{m-1} \sigma_t \preceq \Delta^{m-1} \Delta = \Delta^m$$

donde  $t = j$  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 (1.6.9) 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  $\preceq$  (respectivamente,  $\succcurlyeq$ ) puede ser extendido a  $B_n$  de la siguiente manera: dadas  $a, b \in B_n$ ,  $a \preceq b$  (resp.  $a \succcurlyeq b$ ) si  $ac = b$  (resp.  $b = ca$ ) para algún  $c \in B_n^+$ . Esto da un orden parcial que es invariante por multiplicación a izquierda (resp. 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  $\Delta \succ \sigma_i$  por la Proposición 4.1.8 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  $\Delta^{-1} X_i$ . Conjuguar una trenza positiva por  $\Delta$  sigue dando una trenza positiva por la Proposición 4.1.7 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 4.1.7 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 4.2.1.** 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 en [17]. Sin embargo, no es muy satisfactoria, ya que da lugar a un algoritmo altamente ineficiente.

El-rifai y Morton [14] lo mejoraron definiendo la *forma normal a la izquierda* de una trenza. Basta tomar la descomposición  $\Delta^p A$  y después definir

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

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 un prefijos propios de  $\Delta$ , es decir,  $1 \prec a_i \prec \Delta$ , y además se puede demostrar que  $(a_i a_{i+1}) \wedge \Delta = a_i$

[15] para todo  $i = 1, \dots, r - 1$ . Esta es la anteriormente mencionada forma normal a la izquierda de la trenza. Los prefijos positivos de  $\Delta$  son llamados *elementos simples* o *trenzas de permutación*. El nombre no es casual, ya que como prueba Thurston [15], estas trenzas son justamente las mismas trenzas de permutación definidas en 3.3. 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 [15] mostró que esta forma normal puede ser calculada en tiempo  $O(l^2 n \log(n))$  para una palabra de  $l$  letras en  $B_n$ .

En [15] se puede encontrar además una forma más práctica de llevar a cabo el algoritmo de encontrar la forma normal a la izquierda, la cual será la que utilicemos en el ejemplo 4.2.2. Antes de explicarla vamos a introducir algo de nomenclatura. Dadas dos trenzas simples positivas  $A$  y  $B$ , decimos que un prefijo no trivial  $b \preceq B$  se puede pasar de  $B$  a  $A$  si  $Ab$  es simple, y en tal caso *pasar  $b$  de  $B$  a  $A$*  consiste en las transformaciones  $A \rightarrow Ab$  y  $B \rightarrow b^{-1}B$ . 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,

$$A = a_{1,0} a_{2,0} \dots a_{m,0}.$$

2. En el paso  $t \geq 0$  tenemos  $A$  expresada en bloques de elementos simples como

$$A = a_{1,t} a_{2,t} \dots a_{m,t}.$$

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

$$A = a_{1,t+1} a_{2,t+1} \dots a_{m,t+1}.$$

3. Volvemos 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  $\Delta \not\preceq A$ , 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 4.2.2.** En  $B_4$  sean  $\alpha_1 = \sigma_1\sigma_2^{-1}\sigma_3$  y  $\alpha_2 = \sigma_3\sigma_1\sigma_1\sigma_2\sigma_1$ , las cuales queremos comprobar si 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 4.1.8 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 4.1.7, 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. 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 1.1 nos dan  $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ . Por lo tanto, reescribimos  $\alpha_2$  y continuamos

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

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 El-rifai y Morton. Además es claro que ninguno de los factores es una potencia de  $\Delta$ .

Vamos ahora con la parte positiva de  $\alpha_1$ , que la dividimos en bloques  $a_{1,0} = \sigma_3$ ,  $a_{2,0} = \sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$  y  $a_{3,0} = \sigma_3$ . Tenemos

$$\begin{aligned} \alpha_1 &= (\sigma_3)(\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1)(\sigma_3) = a_{1,0}a_{2,0}a_{3,0} \\ &= (\sigma_3\sigma_1\sigma_2\sigma_3)(\sigma_2\sigma_1)(\sigma_3) = a_{1,1}a_{2,1}a_{3,1} \\ &= (\sigma_3\sigma_1\sigma_2\sigma_3)(\sigma_2\sigma_1\sigma_3)(\sigma_3) = a_{1,2}a_{2,2}a_{3,2} \end{aligned}$$

Vemos que ya no podemos pasar ninguna letra más a la izquierda y que ningún factor es una potencia de  $\Delta$ , por lo que hemos terminado. Como  $a_{3,2}$  es trivial podemos eliminarlo, con lo que  $\alpha_1 = \Delta^{-1}a_1a_2$  donde  $a_1 = a_{1,2}$  y  $a_2 = a_{2,2}$ . Al comparar las descomposiciones finales de  $\alpha_1$  y  $\alpha_2$  comprobamos que nos tienen la misma forma normal, luego representan elementos distintos.

Antes de terminar este capítulo, como comentábamos al final de la sección anterior, la forma normal de Garside permite probar la existencia y unicidad de mínimo común múltiplo y máximo común divisor en  $B_n$  con el orden parcial inducido por el orden parcial definido en  $B_n^+$ .

**Proposición 4.2.3.** Dadas  $a, b \in B_n$ , existen  $c = a \wedge b \in B_n$  y  $d = a \vee b \in B_n$ , es decir, existen el máximo común divisor y el mínimo común múltiplo en  $B_n$ .

**Demostración.** Dadas  $a, b \in B_n$ , sean sus formas normales  $a = \Delta^{p_1} A$  y  $b = \Delta^{p_2} B$ , donde  $p_1, p_2 \in \mathbb{Z}$  y  $A, B \in B_n^+$ . Tomando  $q = \max\{|p_1|, |p_2|\}$  tenemos que  $\Delta^q a, \Delta^q b \in B_n^+$ . Por tanto, sabemos que existe un máximo común divisor  $c = (\Delta^q a \wedge \Delta^q b) \in B_n^+$ . Entonces, por la invarianza por multiplicación a izquierda del orden de prefijos

$$\begin{aligned} c \preceq \Delta^q a &\Leftrightarrow \Delta^{-q} c \preceq a, \\ c \preceq \Delta^q b &\Leftrightarrow \Delta^{-q} c \preceq b. \end{aligned}$$

Esto significa que  $\Delta^{-q} c$  es un prefijo común de  $a$  y de  $b$ . Sea  $d \in B_n$  con  $d \preceq a$  y  $d \preceq b$ . Existe entonces  $N \geq q$  de modo que  $\Delta^N d, \Delta^N a, \Delta^N b \in B_n^+$  y, además,  $\Delta^N d \preceq \Delta^N a$  y  $\Delta^N d \preceq \Delta^N b$ . Por tanto,

$$\Delta^N d \preceq \Delta^N a \wedge \Delta^N b = \Delta^{N-q}(\Delta^q a \wedge \Delta^q b) = \Delta^{N-q} c.$$

Por consiguiente,  $d \preceq \Delta^{-q} c$ , con lo que  $\Delta^{-q} c$  es de hecho el máximo común divisor de  $a$  y  $b$ . Análogamente se prueba para el mínimo común múltiplo. ■

# Capítulo 5

## Representaciones lineales

La existencia (o no existencia) de representaciones lineales fieles de los grupos de trenzas es una de las mayores cuestiones de esta área de investigación. Este problema fue por primera vez resuelto por Bigelow [5] y Krammer [23] en el año 2000, mediante la conocida como *representación LKB*. Además de esta representación existen otras, como la representación de Burau reducida, con la cual empezaremos este capítulo.

### 5.1. Representación de Burau reducida

#### 5.1.1. Definición a partir de espacios recubridores

Consideremos el disco agujereado  $n$  veces  $\mathbb{D}_n$  con un punto base  $d_0 \in \mathbb{D}_n$ .

**Definición 5.1.1.** Para cada lazo  $\alpha$  basado en  $d_0$  denominamos *índice total* a la suma de los índices (número de vueltas) de  $\alpha$  con respecto a cada agujero y lo denotamos  $\phi\alpha$ . Esto es, si un  $\alpha$  está representado en  $F_n$  por  $\prod_{i=1}^k x_{j_i}^{m_{j_i}}$ , entonces

$$\phi\alpha = \sum_{i=1}^k m_{j_i}.$$

Se observa que  $\phi$  es un homomorfismo de grupos  $\phi : \pi_1(\mathbb{D}_n) \rightarrow \mathbb{Z}$  al ser el índice total un invariante homotópico. Sea  $\tilde{\mathbb{D}}_n$  el espacio recubridor correspondiente a  $\ker \phi$  (ver Definición 1.6.16). Vamos a describir geoméricamente este espacio recubridor (ver Figura 5.1).

Para visualizarlo mejor, vamos a agrandar los agujeros de modo que se conviertan en bolas abiertas y llamamos a este nuevo espacio  $X$ . Dibujamos segmentos  $A_1, \dots, A_n$  desde el centro de las bolas hasta el borde del disco. Cortamos  $X$  a lo largo de estos segmentos, de modo que obtenemos dos copias disjuntas  $A_i^+$  y  $A_i^-$  de cada  $A_i$ . Llamamos a este espacio  $X^*$ . Sean  $h_i : A_i^+ \rightarrow A_i^-$  homeomorfismos y tomamos una cantidad numerable de copias  $X_j^*$  de  $X^*$ . Para cada  $j$  sea  $g_j : X_j^* \rightarrow X^*$  un homeomorfismo. El espacio  $\tilde{X}$  se define como la unión disjunta de los  $X_j^*$  identificando  $A_i^+ \subseteq X_j^*$  con  $A_i^- \subseteq X_{j+1}^*$  mediante  $g_{j+1}^{-1} h_i g_j$ .

El hecho de que este sea el recubrimiento correspondiente a  $\ker \phi$  se debe a que, fijada una preimagen  $\tilde{d}_0 \in \tilde{X}$  de  $d_0$ , un lazo en  $d_0$  se levanta a un lazo en  $\tilde{d}_0$  si y solo si su índice total es nulo, pues para cada vuelta positiva sube un nivel en el recubrimiento y para cada vuelta negativa lo baja, así que para acabar de nuevo en  $\tilde{d}_0$

deberá subir tantas veces como baja, es decir, que el número total de vueltas sea nulo.

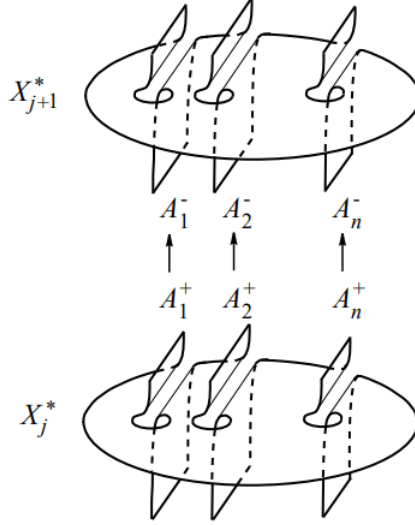


Figura 5.1: Dos hojas del espacio recubridor  $\tilde{X}$ .

Hay una acción natural de  $\mathbb{Z}$  en  $\tilde{X}$  como transformación recubridora dada por  $X_j^* \ni x \mapsto g_{j+n}^{-1} g_j x$  para cada  $n \in \mathbb{Z}$ . Esta acción se puede interpretar como cambiar el punto  $x$  de nivel. Además, la acción es claramente libre y el espacio de órbitas  $\tilde{X}/\mathbb{Z}$  es  $X$ .

Vamos a ver cómo definir la representación de Burau reducida. Sea  $\beta \in B_n$  inducida por un automorfismo  $h$  de  $\mathbb{D}_n$  que fija el borde punto a punto, lo cual vamos a denotar como  $\beta = [h]$ . Entonces, para cualquier lazo  $\gamma$  en  $\mathbb{D}_n$  se tiene que  $\phi(h\gamma) = \phi\gamma$ , de modo que  $h$  induce una equivalencia de homotopía  $\tilde{h}$  de  $\tilde{\mathbb{D}}_n$  que fija el borde [20]. Pasando a la homología, esto nos da un automorfismo de  $H_1(\tilde{\mathbb{D}}_n)$ . Si  $h'$  es cualquier otro automorfismo con  $[h'] = \beta$ , entonces  $[h]^{-1}[h'] = 1$ , así que como la aplicación inducida por el recubrimiento  $\pi_1(\tilde{\mathbb{D}}_n) \rightarrow \pi_1(\mathbb{D}_n)$  es inyectiva (1.6.20) tenemos que  $[\tilde{h}]^{-1}[\tilde{h}'] = 1$  como aplicación en  $\pi_1(\tilde{\mathbb{D}}_n)$ . Pasando a homología, esto nos da  $[\tilde{h}]^{-1}[\tilde{h}'] = 1$  como aplicación en  $H_1(\tilde{\mathbb{D}}_n)$ .

**Definición 5.1.2.** Sea el homomorfismo  $\psi_r : B_n \rightarrow GL(H_1(\tilde{\mathbb{D}}_n))$  dado por  $\psi_r(\beta) = [\tilde{h}]$ . Esta aplicación está bien definida por las observaciones anteriores y se conoce como *representación de Burau reducida* de  $B_n$ .

Se llama *reducida* porque existe una representación  $n$ -dimensional de la cual la forma reducida es un sumando irreducible, es decir, que no se puede expresar como



una combinación de dos representaciones lineales. Esta mencionada representación  $n$ -dimensional puede encontrarse en [22]. Como veremos con la siguiente proposición, la representación que hemos dado es  $(n - 1)$ -dimensional.

**Proposición 5.1.3.**  $H_1(\tilde{\mathbb{D}}_n)$  es un módulo libre de rango  $n - 1$  sobre  $\mathbb{Z}[t, t^{-1}]$ .

**Demostración.** Vamos a calcular la homología de  $\tilde{X}$ , que es claramente del mismo tipo de homotopía que  $\tilde{\mathbb{D}}_n$ . Además podemos considerar  $\phi$  como una aplicación  $\pi_1(X) \rightarrow \mathbb{Z}$  por ser  $X$  homotópicamente equivalente a  $\mathbb{D}_n$ . Eligiendo entonces un generador  $t \in \pi_1(X)/\ker \phi$  podemos ver  $H_1(\tilde{X})$  como un  $\mathbb{Z}[t, t^{-1}]$ -módulo, donde la suma se corresponde con la concatenación de lazos y el producto por  $t$  con la conjugación por un lazo  $x_i$ .

Sean  $A = \bigcup_{j \in \mathbb{Z}} X_{2j}^*$  y  $B = \bigcup_{j \in \mathbb{Z}} X_{2j+1}^*$  subespacios cuya unión es  $\tilde{X}$ . La sucesión de Mayer-Vietoris nos da

$$0 \rightarrow H_1(\tilde{X}) \xrightarrow{\Delta} H_0(A \cap B) \xrightarrow{i_*} H_0(A) \oplus H_0(B),$$

donde el 0 proviene de que  $A$  y  $B$  son homotópicamente equivalentes a un espacio discreto. Por tanto,  $H_1(\tilde{X}) \cong \text{Im } \Delta = \ker i_*$ . Ahora,  $H_0(A \cap B)$  es isomorfo a  $\bigoplus_{j \in \mathbb{Z}} \mathbb{Z}^n$ , ya que para cada  $j \in \mathbb{Z}$ , la intersección  $X_j^* \cap X_{j+1}^*$  es homotópicamente equivalente a un espacio de  $n$  puntos. Entonces  $\{a_{j,1}, \dots, a_{j,n}\}_{j \in \mathbb{Z}}$  es una  $\mathbb{Z}$ -base para  $H_0(A \cap B)$ . Es fácil ver que  $\{a_{j,1} - a_{j,2}, \dots, a_{j,n-1} - a_{j,n}\}_{j \in \mathbb{Z}}$  es una base para  $\ker i_*$ . Sea  $\tilde{d}_0 \in \tilde{X}$  un levantamiento del punto base  $d_0 \in X$ , digamos  $\tilde{d}_0 \in X_0^*$ . Denotamos por  $v_i$  el elemento de  $H_1(\tilde{X})$  representado por el levantamiento del lazo  $x_i x_{i+1}^{-1}$  ( $1 \leq i \leq n - 1$ ). Se tiene que  $\Delta(v_i) = a_{0,i} - a_{0,i+1}$  [22] y para todo  $j \in \mathbb{Z}$  se tiene  $\Delta(t^j v_i) = a_{j,i} - a_{j,i+1}$ . Por tanto, los  $t^j v_i$  forman una base de  $H_1(\tilde{X})$  como  $\mathbb{Z}$ -módulo, y como consecuencia  $\{v_1, \dots, v_{n-1}\}$  es una base de  $H_1(\tilde{X})$  como  $\mathbb{Z}[t, t^{-1}]$ -módulo. ■

### 5.1.2. Expresión matricial

A partir de la demostración de la Proposición 5.1.3 podemos obtener la expresión matricial de la representación de Burau reducida. Como explicaremos con ayuda de la Figura 5.2, la acción de  $\sigma_i$  sobre  $H_1(\tilde{X})$  viene dada por

$$\psi_r \sigma_i(v_j) = \begin{cases} v_j + t v_{j+1} & j = i - 1, \\ -t v_j & j = i, \\ v_{j-1} + v_j & j = i + 1, \\ v_j & c.c. \end{cases}$$

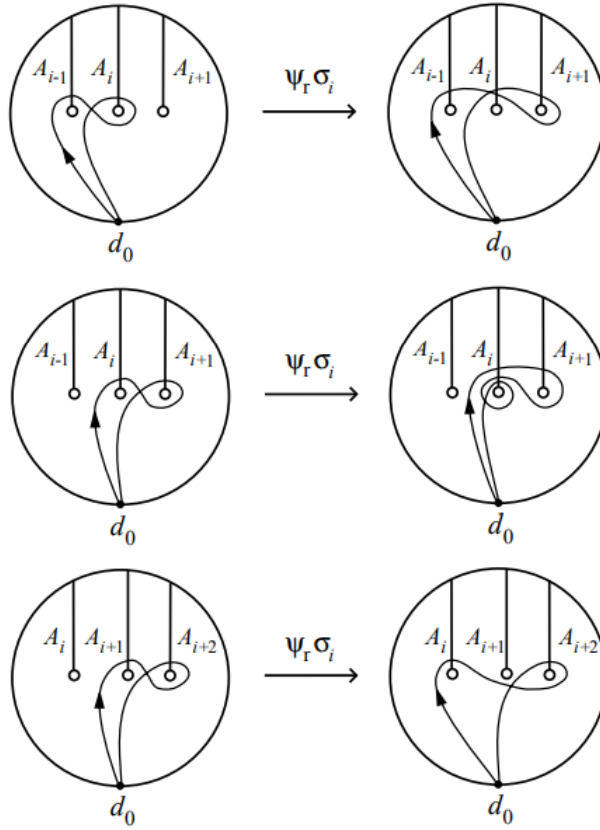


Figura 5.2: Acción de  $\psi_r(\sigma_i)$  sobre  $H_1(\tilde{X})$ .

Así, las matrices para la representación con respecto a la base  $\{v_1, \dots, v_{n-1}\}$  son

$$\psi_r(\sigma_1) = \begin{pmatrix} -t & 0 & & \\ 1 & 1 & & \\ & & I_{n-3} & \end{pmatrix}, \psi_r(\sigma_{n-1}) = \begin{pmatrix} I_{n-3} & & & \\ & 1 & t & \\ & 0 & -t & \end{pmatrix},$$

$$\psi_r(\sigma_i) = \begin{pmatrix} I_{i-2} & & & & \\ & 1 & t & 0 & \\ & 0 & -t & 0 & \\ & 0 & 1 & 1 & \\ & & & & I_{n-i-2} \end{pmatrix}.$$

Vamos a ver exactamente cómo obtener esta representación a partir de la Figura 5.2. Tenemos en la figura todos los casos en los que la acción de  $\sigma_i$  afecta a un generador  $v_j$  de  $H_1(\tilde{X})$  representado por un levantamiento de un lazo de la forma  $x_j x_{j+1}^{-1}$ . Buscamos expresar la imagen de cada  $v_j$  como combinación con coeficientes

en  $\mathbb{Z}[t, t^{-1}]$  de la base de  $H_1(\tilde{X})$ , para lo cual seguiremos la interpretación de  $H_1(\tilde{X})$  como  $\mathbb{Z}[t, t^{-1}]$ -módulo de la demostración de la Proposición 5.1.3.

En el primer caso de la Figura 5.2 partimos de  $v_{i-1}$ , y su imagen está representada por un levantamiento de  $x_{i-1}x_i x_{i+1}^{-1} x_i^{-1} = (x_{i-1}x_i^{-1})(x_i x_{i+1}^{-1} x_i^{-1})$ , que representa a  $v_{i-1} + tv_i$ .

En el segundo caso el generador es  $v_i$ . La imagen viene dada por el levantamiento de  $x_i x_{i+1} x_i^{-1} x_i^{-1} = x_i (x_i x_{i+1}^{-1})^{-1} x_i^{-1}$ , es decir, un representante de  $-tv_i$ .

Por último, en el tercer caso la imagen de  $v_{i+1}$  es un levantamiento de  $x_i x_{i+2}^{-1} = (x_i x_{i+1}^{-1})(x_{i+1} x_{i+2}^{-1})$ , que representa al elemento  $v_i + v_{i+1}$ .

En los casos en los que  $\sigma_i$  no modifica el lazo  $x_j x_{j+1}^{-1}$  es claro que la acción resultante es la identidad.

Se puede comprobar directamente que las matrices anteriores satisfacen las relaciones de la presentación 1.1. Un hecho interesante de esta representación es que se sabe que es fiel para  $n \leq 3$  [7] y que no es fiel para  $n \geq 5$  [6][29], pero el caso  $n = 4$  sigue siendo un problema abierto.

## 5.2. Representación LKB

Siguiendo [23], denotamos  $Ref_n$  al conjunto de pares de enteros  $(i, j)$  tales que  $1 \leq i < j \leq n$ . Claramente, el cardinal de  $Ref_n$  es  $\frac{n(n-1)}{2}$ .

Sea  $R$  un anillo conmutativo con unidad y  $q, t \in R$  dos elementos invertibles. Sea  $V = \bigoplus_{s \in Ref_n} Rx_s$  el  $R$ -módulo libre de rango  $\frac{n(n-1)}{2}$  con base  $\{x_s\}_{s \in Ref_n}$ .

Krammer [23] define una acción  $R$ -lineal de  $B_n$  sobre  $V$  como sigue:

$$\sigma_k(x_{i,j}) = \begin{cases} x_{i,j} & \text{si } (k < i) \text{ o } (j < k), \\ x_{i-1,k} + (1-q)x_{i,j} & \text{si } (k = i-1), \\ tq(q-1)x_{i,i+1} + qx_{i+1,j} & \text{si } (k = i < j-1), \\ tq^2 x_{i,j} & \text{si } k = i = j-1, \\ x_{i,j} + tq^{k-i}(q-1)^2 x_{k,k+1} & \text{si } (i < k < j-1), \\ x_{i,j-1} + tq^{j-1}(q-1)x_{j-1,j} & \text{si } (i < k = j-1), \\ (1-q)x_{i,j} + qx_{i,j+1} & \text{si } (k = j), \end{cases} \quad (5.1)$$

donde  $1 \leq i < j \leq n$  y  $k = 1, \dots, n-1$ . Que la acción de  $\sigma_k$  es invertible y que se cumplen las relaciones de 1.1 se verifica mediante cálculo directo. Esta es la conocida como *representación LKB* (Lawrence-Krammer-Bigelow) o *representación de Krammer* de  $B_n$ .

**Teorema 5.2.1.** Sea  $R = \mathbb{R}[t^{\pm 1}]$  y  $0 < q < 1$ . Entonces, la representación  $B_n \rightarrow \text{Aut}(V)$  es fiel para todo  $n \geq 1$ .

La prueba de este teorema se encuentra en [23].

### 5.2.1. Representación de Bigelow

Existe un caso particular de la representación LKB encontrado independientemente por Bigelow [6], la cual se puede obtener usando  $R = \mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$ . La ventaja de esta representación es que tiene una interpretación geométrica mucho más clara, como veremos a continuación.

Consideremos  $C = M_2(\mathbb{D}_n)/\Sigma_2$ . Aquí,  $\Sigma_2$  actúa sobre  $M_2(\mathbb{D}_n)$  enviando  $(x, y)$  a  $(y, x)$ . Se denotarán los puntos de  $C$  como  $\{x, y\}$  ya que al actuar  $\Sigma_2$  no importa el orden. La proyección  $M_2(\mathbb{D}_n) \rightarrow C$  que lleva  $(x, y)$  a  $\{x, y\}$  es claramente un recubrimiento de dos hojas. Sean  $d_0$  y  $d'_0$  dos puntos de  $\partial\mathbb{D}_n$  lo bastante cercanos entre sí como para que no se crucen las hojas del recubridor. Tomamos  $c_0 = \{d_0, d'_0\}$  como punto base de  $C$ .

Sea  $\alpha : [0, 1] \rightarrow C$  un camino basado  $c_0$ . Este camino se puede levantar relativamente a  $(d_0, d'_0)$  como un par de caminos de la forma  $(\alpha_1, \alpha_2)$ , con  $\alpha_1, \alpha_2 : [0, 1] \rightarrow \mathbb{D}_n$ , el primero basado en  $d_0$  y el segundo en  $d'_0$ . Denotemos pues  $\alpha(t) = \{\alpha_1(t), \alpha_2(t)\}$ . Nótese que si  $\alpha$  es un lazo entonces  $\{\alpha_1(0), \alpha_2(0)\} = \{\alpha_1(1), \alpha_2(1)\} = \{d_0, d'_0\}$ . Por lo tanto, o bien  $\alpha_1$  y  $\alpha_2$  son ambos lazos o bien su concatenación forma un lazo. Ambos casos se observan en la Figura 5.3.

Si  $\alpha_1$  y  $\alpha_2$  son caminos en  $\mathbb{D}_n$  con  $\alpha_1(t) \neq \alpha_2(t)$  para todo  $t \in [0, 1]$ , entonces  $(\alpha_1, \alpha_2)$  es un camino en  $M_2(\mathbb{D}_n)$ . La imagen de este camino mediante la proyección  $M_2(\mathbb{D}_n) \rightarrow C$  se denota  $\{\alpha_1, \alpha_2\}$ .

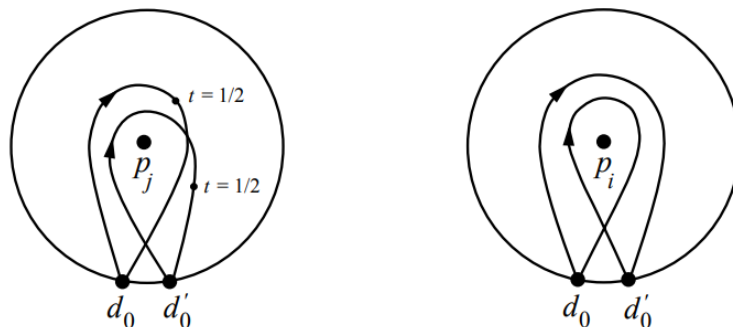


Figura 5.3: A la izquierda, un lazo en  $C$  que surge cuando los dos caminos originales son lazos (el parámetro  $t$  muestra cómo está parametrizado el lazo). A la derecha, la concatenación de los dos lazos originales da lugar a un lazo en  $C$ .

Sea  $\alpha : [0, 1] \rightarrow C$  un representante de un elemento en  $\pi_1(C)$ . Se definen las aplicaciones  $a, b : \pi_1(C) \rightarrow \mathbb{Z}$  como sigue: si  $\alpha_1$  y  $\alpha_2$  son ambos lazos, entonces  $a(\alpha)$  es la suma de los índices totales de  $\alpha_1$  y  $\alpha_2$ . Si no son ambos lazos, entonces  $a(\alpha)$  es el índice total del lazo  $\alpha_1\alpha_2$ . La aplicación  $b$  está definida en primer lugar componiendo  $[0, 1] \ni t \mapsto \frac{(\alpha_1(t) - \alpha_2(t))}{|\alpha_1(t) - \alpha_2(t)|} \in S^1$  con la proyección  $S^1 \rightarrow \mathbb{R}P^1$  para obtener un lazo en  $\mathbb{R}P^1$ . El correspondiente elemento de  $H_1(\mathbb{R}P^1) \cong \mathbb{Z}$  es  $b(\alpha)$ . Por tanto,  $a$  mide la cantidad de veces que los lazos  $\alpha_1$  y  $\alpha_2$  envuelven a los agujeros, mientras que  $b$  mide las veces que un lazo envuelve al otro.

Sea  $\langle q, t \rangle$  el grupo libre abeliano generado por  $q$  y  $t$ . Se define la aplicación  $\phi : \pi_1(C) \rightarrow \langle q, t \rangle$  mediante  $\alpha \mapsto q^{a(\alpha)}t^{b(\alpha)}$ . Por ejemplo, si en la Figura 5.3 denotamos al lazo de la izquierda  $\gamma_1$  y al de la derecha  $\gamma_2$ , tenemos  $\phi(\gamma_1) = q^2$  y  $\phi(\gamma_2) = tq^2$ .

Sea  $\tilde{C} \rightarrow C$  el espacio recubridor correspondiente a  $\ker \phi$  y elijamos un levantamiento  $\tilde{c}_0 \in \tilde{C}$  de  $c_0$ . El grupo de homología  $H_2(\tilde{C})$  se puede considerar como un  $\mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$ -módulo, donde el grupo  $\langle t, q \rangle$  actúa sobre  $\tilde{C}$  como transformaciones recubridoras [5].

Sea  $h$  un automorfismo de  $\mathbb{D}_n$  que fije el borde punto a punto. Entonces  $h$  induce un automorfismo denotado igual  $h : C \rightarrow C$  dado por  $h(\{x, y\}) = \{h(x), h(y)\}$ . Es claro que  $h(c_0) = c_0$ . Por tanto, este homeomorfismo se levanta de forma única a una equivalencia de homotopía  $\tilde{h} : \tilde{C} \rightarrow \tilde{C}$  que fija  $\tilde{c}_0$ . Por tanto,  $\tilde{h}$  induce un isomorfismo de  $\mathbb{Z}[q^{\pm 1}, t^{\pm 1}]$ -módulos  $\tilde{h}_* : H_2(\tilde{C}) \rightarrow H_2(\tilde{C})$ .

**Definición 5.2.2.** La representación  $\kappa : B_n \rightarrow \text{Aut}(H_2(\tilde{C}))$  inducida por  $h \mapsto \tilde{h}_*$  se llama *representación de Bigelow*.

**Teorema 5.2.3.** La representación de Bigelow  $\kappa : B_n \rightarrow \text{Aut}(H_2(\tilde{C}))$  es fiel para todo  $n \geq 1$ .

Este resultado se prueba en [6]. También por [6] podemos tomar una base  $\{v_{i,j} \in H_2(\tilde{C})\}_{(i,j) \in \text{Ref}}$ . Con esto, podemos establecer la equivalencia [31] entre esta representación y la representación 5.1 como sigue:

$$v_{i,j} = x_{i,j} + (1 - q) \sum_{i < k < j} x_{k,j}, \quad x_{i,j} = v_{i,j} + (q - 1) \sum_{i < k < j} q^{k-i-1} v_{k,j}.$$

### 5.3. Solución al problema de la palabra

Los resultados anteriores demuestran que los grupos de trenzas son grupos lineales. Una vez obtenida una representación lineal fiel, es inmediato resolver el problema de la palabra a partir de la expresión matricial: basta hacer el producto de las matrices

que representan las letras de la palabra. Si el resultado de dicho producto es la matriz identidad, entonces la palabra representa el elemento trivial y recíprocamente.

Dado que el producto de matrices se puede calcular en tiempo polinomial sobre la dimensión de la matriz, este algoritmo puede ser bastante rápido, pero la aparición de polinomios en  $t$  y  $t^{-1}$  de tamaño y coeficientes arbitrarios en las entradas de las matrices puede ralentizarlo significativamente, especialmente para trenzas de longitud larga.

**Ejemplo 5.3.1.** Vamos a ver un ejemplo de resolver el problema de la palabra con la representación de Burau reducida para  $n = 3$ , caso para el que sabemos que la representación es fiel. Para cualquier otra representación la mecánica es la misma. Consideremos la palabra  $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$ . En este caso, tenemos las matrices

$$\psi_r(\sigma_1) = \begin{pmatrix} -t & 1 \\ 0 & 1 \end{pmatrix}, \quad \psi_r(\sigma_2) = \begin{pmatrix} 1 & 0 \\ t & -t \end{pmatrix}.$$

Para este caso necesitaremos también las inversas

$$\psi_r(\sigma_1^{-1}) = \psi_r(\sigma_1)^{-1} = \begin{pmatrix} -t^{-1} & t^{-1} \\ 0 & 1 \end{pmatrix}, \quad \psi_r(\sigma_2^{-1}) = \psi_r(\sigma_2)^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & -t^{-1} \end{pmatrix}.$$

Ahora, basta realizar el producto matricial

$$\begin{pmatrix} -t & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & -t \end{pmatrix} \begin{pmatrix} -t^{-1} & t^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & -t^{-1} \end{pmatrix} = \begin{pmatrix} -t & 1 \\ -t & -t^{-1} + 1 \end{pmatrix}.$$

Como la matriz no es la identidad, la palabra no representaba el elemento neutro.

# Bibliografía

- [1] J. W. Alexander. *On the deformation of an  $n$ -cell*. Proc. of the Nat. Acad. of Sci. of the USA., 9 (12):406–407, 1923. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1085470/pdf/pnas01885-0010.pdf>
- [2] E. Artin. *Theorie der Zöpfe*. Abh. Math. Sem. Hamburgischen Univ., 4:47–72, 1925.
- [3] E. Artin. *The theory of braids*. Annals of Math., 48:101–126, 1947. <http://www.maths.ed.ac.uk/~aar/papers/artinbraids.pdf>
- [4] M.A. Berger. *Topological invariants in braid theory*. Letters in Mathematical Physics (2001) 55: 181. <https://doi.org/10.1023/A:1010979823190>
- [5] S.J. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. 14 (2001), no. 2, 471–486. <https://arxiv.org/pdf/math/0005038.pdf>
- [6] S. Bigelow. *The Burau representation is not faithful for  $n = 5$* . Geom. Topol. 3 (1999), no. 1, 397–404. doi:10.2140/gt.1999.3.397. <https://arxiv.org/pdf/math/9904100.pdf>
- [7] J. S. Birman. *Braids, links and mapping class groups*. Annals of Mathematics Studies, No. 82. Princeton University Press, Princeton, N.J., 1974.
- [8] Burau, Werner (1936). *Über Zopfgruppen und gleichsinnig verdrillte Verkettungen*. Abh. Math. Sem. Univ. Hamburg. 11: 179–186. doi:10.1007/bf02940722
- [9] A. H. Clifford and G.B. Preston. *The algebraic theory of semigroups*. AMS Math. Surveys, vol. 7, 1967. MR0218472 (36:1558)
- [10] M. Dehn. *Transformation der Kurven auf zweiseitigen Flächen*. Mathematische Annalen (1912), 72 (3): 413–421
- [11] M. Dehn. *Über unendliche diskontinuierliche Gruppen*. Mathematische Annalen (1911), 71 (1): 116–144.
- [12] P. Dehornoy. *Groupes de Garside*. Annales scientifiques de l'École Normale Supérieure, Série 4 : Tome 35 (2002) no. 2 , p. 267-306 <https://arxiv.org/pdf/math/0111157.pdf>
- [13] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest. *Ordering Braids*. Mathematical Surveys and Monographs Volume: 148; 2008; 323 pp; ISBN: 978-0-8218-4431-1.

- [14] E. A. El-Rifai, H. R. Morton. *Algorithms for positive braids*. Quart. J. Math. Oxford Ser. (2), 45 (180):479–497, 1994.
- [15] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, W. P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.
- [16] E. Fadell, L. Neuwirth. *Configuration spaces*. Math. Scand., 10:111–118, 1962. <http://www.msccand.dk/article/download/10517/8538>
- [17] F. A. Garside. *The braid group and other groups*. Quart. J. Math. Oxford Ser. (2), 20:235–254, 1969. <http://www.maths.ed.ac.uk/~aar/papers/garside.pdf>
- [18] J. González-Meneses. *Basic results on braid groups*. Annales mathématiques, Blaise Pascal Working version – October 5, 2010. <https://arxiv.org/abs/1010.0321v1>
- [19] J. González-Meneses, M. Silvero. *Polynomial braid combing*. December 5, 2017. <https://arxiv.org/abs/1712.01552>
- [20] A. Hatcher, *Algebraic Topology*. Cambridge University Press, 2002. <https://www.math.cornell.edu/~hatcher/AT/AT.pdf>
- [21] A. Hurwitz. *Über Riemannsche Flächen mit gegebenen Verzweigungspunkten*. Math. Ann., 39 (1):1–60, 1891.
- [22] C. H. Jackson, *Braid group representations*. The Ohio State University 2001. <http://go.owu.edu/~chjackso/Papers/thesis.pdf>
- [23] D. Krammer, *Braid groups are linear*, Ann. of Math. (2) 155 (2002), no. 1, 131–156. <https://arxiv.org/pdf/math/0405198.pdf>
- [24] W. Magnus. *Über Automorphismen von Fundamentalgruppen berandeter Flächen*. Math. Ann., 109:617–646, 1934.
- [25] A. Markov. *Foundations of the algebraic theory of tresses*. (russian). Trav. Inst. Math. Stekloff, 16:53 pp., 1945. <http://www.mathnet.ru/links/f1a9f74975a0ed7e11860df5c4a69c58/tm911.pdf>
- [26] P. S. Novikov. *On the algorithmic unsolvability of the word problem in group theory*, Proceedings of the Steklov Institute of Mathematics (in Russian), 44: 1–143 (1955).



- [27] O. Ore. *Linear equations in non-commutative fields*. Ann. of Math. (2), 32 (3):463–477, 1931.
- [28] L. Paris. *Braid groups and Artin groups*. Institut de Mathématiques de Bourgogne – November 15, 2007. <https://arxiv.org/abs/0711.2372v1>
- [29] D. D. Long, M. Paton. *The Burau representation is not faithful for  $n \geq 6$* . Topology, Volume 32, Issue 2, 1993, Pages 439-447, ISSN 0040-9383. [http://web.math.ucsb.edu/~long/pubpdf/Burau\\_n6.pdf](http://web.math.ucsb.edu/~long/pubpdf/Burau_n6.pdf)
- [30] V. Shpilrain. *Search and witness problem in group theory*. October 3, 2010. <https://arxiv.org/abs/1010.0382>
- [31] V. Turaev. *Faithful linear representations of the braid groups*. Séminaire N. Bourbaki, 1999-2000, exp. n° 878, p.389-409. [http://www.numdam.org/article/SB\\_1999-2000\\_\\_42\\_\\_389\\_0.pdf](http://www.numdam.org/article/SB_1999-2000__42__389_0.pdf)
- [32] O. Zariski. *On the Poincaré group of rational plane curves*. Amer. J. of Math., 58 (3):607–619, 1936.