ACTAS DEL VIII CONGRESO
DR. ANTONIO A. R. MONTEIRO
(2005), Páginas 49–56

UNA FORMA NORMAL EN GRUPOS DE TRENZAS DE TIPO B_n

SEBASTIÁN FREYRE

RESUMEN. Presentaremos primero algunas definiciones y propiedades de los grupos de trenzas de tipo A_n (o clásicos), usaremos la forma normal presentada en [BKL] y una relación entre éstos y los grupos de trenzas de tipo B_n para recuperar una forma normal en los últimos. Destacamos que nuestra solución puede implementarse algorítmicamente en tiempo $\mathcal{O}(n|W|^2)$.

1. INTRODUCCIÓN

Este trabajo está relacionado con algunos algoritmos criptográficos sobre grupos no abelianos cuya implementación fue estudiada extensivamente con el grupo de trenzas. Cabe mencionar que para posibilitar tales implementaciones es necesario resolver el problema de la forma normal, que permite traducir los elementos del grupo a código, como también que el problema de la conjugación no pueda resolverse en tiempo polinomial.

Así como a cada diagrama de Dynkin se le asocia un grupo de Coxeter, también se le asocian grupos de trenzas generalizados. Este trabajo consiste en resolver el problema de la forma normal en los grupos de trenzas asociados a diagramas de tipo B_n.

Si bien este problema fue resuelto en un contexto más general en [BS], no está estudiada la complejidad en el caso general. Por otro lado, en el caso de tipo A_n, la complejidad es del orden $\mathcal{O}(n^2|W|^2)$, mientras que una solución alternativa fue estudiada en [BKL], donde se presenta un algoritmo que reduce la complejidad a $\mathcal{O}(n|W|^2)$.

En [B] se presentan herramientas para resolver el problema de la forma normal en el caso general que, en los grupos de tipo A_n, coincide con la presentada en [BKL]. No obstante, no sólo no se da una solución explícita sino que tampoco se estudia la complejidad. Si bien no vamos a presentar un algoritmo para la forma normal que proponemos, éste puede entenderse fácilmente del algoritmo presentado en [BKL] y de este trabajo. También se encuentra de manera completa en [F], donde además estudiamos la complejidad, que resulta ser de $\mathcal{O}(n|W|^2)$.

Con respecto a las aplicaciones criptográficas observamos que como estos grupos están identificados explícitamente con un subgrupo de los grupos de trenzas de tipo A_n, la implementación de éstos no mejora a la que usa los grupos de trenzas clásicos.

2. PRELIMINARES

Presentaremos ahora los grupos de trenzas de tipo A_{n-1} y B_{n-1}, a los que llamaremos β_n y $\hat{\beta}_n$ respectivamente.

2.1. **El grupo de trenzas clásico.** La presentación de Artin del grupo de trenzas (de tipo A_n) [A] está dada por generadores y relaciones y permite entender al grupo simétrico como un cociente del mismo.

Este grupo se puede definir por medio de $n-1$ generadores $\sigma_1, \sigma_2, \ldots \sigma_{n-1}$ y las siguientes relaciones:

$$(1)\ \sigma_i.\sigma_j.\sigma_i = \sigma_j.\sigma_i.\sigma_j \quad \text{si } |i-j| = 1,$$
$$(2)\ \sigma_i.\sigma_j = \sigma_j.\sigma_i \quad \text{si } |i-j| > 1.$$

En esta presentación se puede pensar que los σ_i son levantados de las trasposiciones elementales por la proyección canónica del grupo de trenzas en el grupo simétrico.

Una presentación más reciente [BKL] considera un conjunto de generadores que contiene a los generadores de Artin. Estos consisten en levantar todas las trasposiciones sobre el grupo de trenzas.

Definimos ahora para cada (t,s), con $1 \leq s < t \leq n-1$, el elemento de β_n

$$a_{ts} = (\sigma_{t-1}\sigma_{t-2} \ \ldots \ \sigma_{s+1})\sigma_s(\sigma_{t-1}\sigma_{t-2} \ \ldots \ \sigma_{s+1})^{-1}.$$

Estos elementos se denominan *bandas generadoras*.

Proposición 2.1.1. *El grupo β_n admite una presentación dada por el conjunto de generadores $\{a_{ts} \in \beta_n \ / \ 1 \leq s < t \leq n\}$ y las relaciones:*

$$(*)\ \ a_{ts}a_{rq} = a_{rq}a_{ts} \quad si\ (t-r)(t-q)(s-r)(s-q) > 0,$$
$$(**)\ \ a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr} \quad para\ todos\ t,s,r\ con\ 1 \leq r < s < t \leq n.$$

Se puede ver una prueba en [BKL, F].

2.2. **El grupo de trenzas de tipo B_n.** El grupo de trenzas asociado a diagramas de Dynkin de tipo B_{n-1}, que llamamos $\hat{\beta}_n$, está definido como grupo de Artin por generadores $\hat{\sigma}_1,\ \hat{\sigma}_2,\ \ldots \hat{\sigma_{n-1}}$ y las siguientes relaciones:

$$(1)\quad \hat{\sigma}_i.\hat{\sigma}_j = \hat{\sigma}_j.\hat{\sigma}_i \ \ si\ |i-j| > 1,$$

$$(2)\quad \hat{\sigma}_i.\hat{\sigma_{i+1}}.\hat{\sigma}_i = \hat{\sigma_{i+1}}.\hat{\sigma}_i.\hat{\sigma_{i+1}}\ si\ 1 \leq i \leq n-3,$$

$$(3)\quad \hat{\sigma_{n-2}}.\hat{\sigma_{n-1}}.\hat{\sigma_{n-2}}.\hat{\sigma_{n-1}} = \hat{\sigma_{n-1}}.\hat{\sigma_{n-2}}.\hat{\sigma_{n-1}}.\hat{\sigma_{n-2}}.$$

Observamos que existe un morfismo Ψ de grupos de $\hat{\beta}_n$ en el subgrupo de β_n generado por $\sigma_1, \sigma_2, \ldots, \sigma_{n-1},\ \sigma_{n-1}^2$, que manda $\hat{\sigma}_i$ en σ_i, para $i = 1, 2, \ldots, n-2$ y $\hat{\sigma_{n-2}}$ en σ_{n-1}^2.

Proposición 2.2.1. *El morfismo Ψ está bien definido y es inyectivo.*

Con esto identificamos al grupo de trenzas de tipo B_n con el subgrupo

$$H_n = \langle \sigma_1; \sigma_2; \ldots; \sigma_{n-2}; \sigma_{n-1}^2 \rangle.$$

Para ver una prueba se pueden revisar [D, DG].

2.3. **El semigrupo de palabras positivas.**

Definición 2.3.1. *Se llama* palabra positiva en las bandas generadoras, *W, a una representación de un elemento de β_n como producto de las bandas generadoras en la que no aparecen inversos de las mismas. Llamamos* longitud *de W al número de generadores que aparecen en su escritura.*

Para referirnos a la longitud de una palabra positiva W usamos la notación $|W|$. Notar que esta longitud es menor o igual que la dada por los generadores σ_i.

Definición 2.3.2. *Decimos que dos palabras positivas V y W son* positivamente equivalentes *si se puede transformar una en la otra por medio de aplicaciones directas de las relaciones $(*)$ y $(**)$. En tal caso notamos $V \doteq W$.*

Definición 2.3.3. *Decimos que un elemento* W *de β_n* pertenece al semigrupo de palabras positivas, *β_n^+, si admite una representación por medio de una palabra positiva.*

Se define β_n^+ como el conjunto de palabras positivas módulo equivalencia positiva.

Teorema 2.3.4 (Teorema de inmersión)**.** *El mapa natural de β_n^+ en β_n es inyectivo. Dicho de otro modo, dos palabras positivas son positivamente equivalentes si y sólo si definen el mismo elemento de β_n.*

Para ver una prueba, revisar [CP].

2.4. **La forma normal en los grupos de tipo A_n.** Introduzcamos una palabra importante para el desarrollo de las formas normales. Llamamos *palabra fundamental* a la palabra representada por:

$$\delta = a_{n(n-1)}a_{(n-1)(n-2)}\dots a_{21}.$$

Definición 2.4.1. *Definimos el* automorfismo fundamental *de β_n como el automorfismo $\tau : \beta_n \to \beta_n$ correspondiente a conjugar por δ. Más precisamente, $\tau(W) = \delta^{-1}W\delta$.*

Definiremos y estudiaremos ahora una clase de trenzas invariantes por el automorfismo fundamental.

Definición 2.4.2. *Llamamos* factor canónico *a toda palabra positiva A para la que existe otra palabra positiva B tal que $\delta = AB$.*

Definición 2.4.3. *Se llama* ciclo descendente *a todo ciclo de Σ_n de la forma $(n_l\, n_{l-1}\dots n_1)$, con $1 \le n_i < n_{i+1} \le n$ para todo $1 \le i \le l$.*

Definición 2.4.4. *Decimos que dos ciclos descendentes $\pi = (n_k\, n_{k-1}\dots n_1)$ y $\pi' = (m_l\, m_{l-1}\dots m_1)$ son* paralelos *si $(m_{i+1} - n_{j+1})(m_{i+1} - n_j)(m_i - n_{j+1})(m_i - n_j) > 0$ para todos $i,\ j$ tales que $1 \le i < l$ y $1 \le j < k$.*

Decimos que una permutación π es un producto de ciclos paralelos descendentes *si $\pi = \pi_1\pi_2\dots\pi_k$ y, para todo par $i,\ j$ de subíndices distintos, π_i y π_j son paralelos.*

Observación 2.4.5. *Sea $\pi = (n_l\, n_{l-1}\dots n_1)$ un ciclo descendente, asociamos a π el elemento de β_n:*

$$\delta_\pi = a_{n_l n_{l-1}}a_{n_{l-1}n_{l-2}}\dots a_{n_1 n_2}.$$

Si $\pi = \pi_1\pi_2\dots\pi_k$ es un producto de ciclos paralelos descendentes le asociamos la trenza $\delta_\pi = \delta_{\pi_1}\delta_{\pi_2}\dots\delta_{\pi_k}$.

Teorema 2.4.6. *Sea A un elemento de β_n^+. Las siguientes afirmaciones son equivalentes:*

(I) A es un factor canónico, es decir $A \le \delta$.

(II) $A = \delta_\pi$ para alguna permutación π producto de ciclos paralelos descendentes en Σ_n.

Una prueba de esta proposición puede verse en [BKL, F].

Definición 2.4.7. *Sea P una palabra positiva y A un factor canónico, decimos que el par (A,P) es* cargado a izquierda *si para toda descomposición de la forma $AP = A'P'$, en la que A' es un factor canónico y P' una palabra positiva, se tiene que $|A| \leq |A'|$. En tal caso notamos $A\lceil P$.*

Observación 2.4.8. *Se puede probar que el automorfismo fundamental manda palabras positivas en palabras positivas y factores canónicos en factores canónicos. Más aún, que $\tau(a_{ts}) = a_{(t+1)(s+1)}$, donde los subíndices deben interpretarse módulo n. Esto permite probar que el automorfismo fundamental manda pares de factores canónicos cargados a izquierda en pares de factores canónicos también cargados a izquierda.*

Una prueba de estos hechos puede encontrarse en [F].

Teorema 2.4.9 (de la forma normal)**.** *Todo elemento W de β_n admite una representación única de la forma:*

$$W = \delta^k A_1 A_2 A_3 \dots A_r,$$

donde k es algún entero, r algún entero no negativo y los A_i, con $1 \leq i \leq r$, son factores canónicos tales que $A_1 \neq \delta$ y cada par $A_i A_{i+1}$ es cargado a la izquierda.

Se puede ver una prueba en [BKL, F].

3. La forma normal en grupos de tipo B_n

Ahora nos abocaremos a recuperar una forma normal para representar a los elementos de los grupos de trenzas de tipo B_n. Al igual que en la forma normal de trenzas de tipo A_n tendremos una palabra que jugará un rol central, definimos la *trenza fundamental* de $\hat{\beta}_n$ como sigue:

$$\hat{\delta} = a_{n(n-1)}^2 a_{(n-1)(n-2)} \dots a_{21}.$$

3.1. **Dos lemas centrales.**

Lema 3.1.1. *Las palabras δ y $\hat{\delta}$ satisfacen la siguiente identidad: $\delta^n = \hat{\delta}^{n-1}$.*

Demostración. Es una consecuencia inmediata de la observación 2.4.8 vía un argumento inductivo. Una prueba completa puede verse en [F]. ∎

Lema 3.1.2. *Sea π en Σ_n un producto de ciclos paralelos descendentes. Entonces existe un único k entero, con $0 \leq k \leq n-1$, tal que $\Psi^{-1}(\delta^k \delta_\pi)$ admite una representación por medio de una palabra positiva en las bandas generadoras de $\hat{\beta}_n$, donde Ψ es el isomorfismo que identifica H_n con $\hat{\beta}_n$.*

Demostración. Nos permitimos abusar de la notación en el siguiente sentido: si un elemento de β_n pertenece a H_n, diremos indistintamente que el mismo pertenece a $\hat{\beta}_n$.

Observemos primero que si $\pi(n) = n$, entonces δ_π es una palabra positiva en las bandas generadoras de $\hat{\beta}_n$. Es decir, $\delta^0 \delta_\pi$ admite una representación en las bandas generadoras de $\hat{\beta}_n$.

Supongamos ahora que $\pi(n) \neq n$, tenemos entonces que $\pi = \pi_1\pi_2 \dots \pi_l$, con π_1; π_2; $\dots \pi_l$ ciclos paralelos descendentes y $\pi_1 = (n\, t_j\, t_{j-1} \dots t_1)$, donde $t_i < t_{i+1} < n$, para todo i con $1 \leq i < j$.

Probaremos que $\delta^{t_j}\delta_\pi$ pertenece a $\hat{\beta}_n^+$ por inducción en t_j.

Observemos que el hecho de que los ciclos π_i sean paralelos y que $\pi_1(n) \neq n$ implica que $\delta'_\pi = \delta_{\pi_2}\delta_{\pi_3} \dots \delta_{\pi_j}$ es una palabra positiva en las bandas generadoras de $\hat{\beta}_n$.

Si $t_j = 1$ entonces $\delta_{\pi_1} = a_{n1}$ y, por la observación 2.4.8 se tiene que

$$\delta\delta_{\pi_1} = \delta a_{n1} = a_{n(n-1)}\delta = \hat{a}_{n(n-1)}\hat{a}_{(n-1)(n-2)} \dots \hat{a}_{21} = \hat{\delta},$$

de lo que deducimos que

$$\delta\delta_\pi = \delta\delta_{\pi_1}\delta_{\pi'} = \hat{\delta}\delta_{\pi'}$$

y, por lo tanto, que $\delta\delta_\pi$ admite una representación por medio de una palabra positiva en $\hat{\beta}_n$.

Supongamos ahora que, si $t_j = m$, entonces $\delta^{t_j}\delta_\pi$ pertenece a $\hat{\beta}_n^+$.

Sea π tal que $t_j = m+1$. Por la observación 2.4.8 tenemos que

$$\begin{aligned}
\delta^{t_j}\delta_\pi &= \delta^{t_{j-1}}\delta\delta_\pi \\
&= \delta^{t_{j-1}}\delta\delta_{\pi_1}\delta_{\pi'} \\
&= \delta^{t_{j-1}}\delta(a_{nt_j}a_{t_jt_{j-1}} \dots a_{t_2t_1})\delta_{\pi'} \\
&= \delta^{t_{j-1}}a_{(n-1)(t_j-1)}\delta(a_{t_jt_{j-1}}a_{t_{j-1}t_{j-2}} \dots a_{t_2t_1})\delta_{\pi'}.
\end{aligned}$$

Para alivianar la notación llamemos $W_R = (a_{t_jt_{j-1}}a_{t_{j-1}t_{j-2}} \dots a_{t_2t_1})\delta_{\pi'}$. Usando nuevamente el lema de la palabra fundamental, tenemos que

$$\begin{aligned}
\delta^{t_j}\delta_\pi &= \delta^{t_{j-1}}a_{(n-1)(t_j-1)}\delta W_R \\
&= \delta^{t_{j-1}}a_{(n-1)(t_j-1)}a_{n(t_j-1)}(a_{n(n-1)}a_{(n-1)(n-2)} \dots a_{(t_j+1)t_j}) \\
&\quad (a_{(t_j-2)(t_j-3)}a_{(t_j-3)(t_j-4)\dots a_{21}})W_R \\
&= \delta^{t_{j-1}}a_{n(t_j-1)}a_{n(n-1)}(a_{n(n-1)}a_{(n-1)(n-2)} \dots a_{(t_j+1)t_j}) \\
&\quad (a_{(t_j-2)(t_j-3)}a_{(t_j-3)(t_j-4)\dots a_{21}})W_R \\
&= (\delta^{t_{j-1}}a_{n(t_j-1)})(a^2_{n(n-1)}a_{(n-1)(n-2)} \dots a_{(t_j+1)t_j}) \\
&\quad (a_{(t_j-2)(t_j-3)}a_{(t_j-3)(t_j-4)\dots a_{21}})W_R.
\end{aligned}$$

Ahora, aplicando la hipótesis inductiva, obtenemos que $W_L = \delta^{t_{j-1}}a_{n(t_j-1)}$ admite una representación positiva en las bandas generadoras de $\hat{\beta}_n$.

Observando que

$$W_C = (a^2_{n(n-1)}a_{(n-1)(n-2)} \dots a_{(t_j+1)t_j})(a_{(t_j-2)(t_j-3)}a_{(t_j-3)(t_j-4)} \dots a_{21})$$

es una palabra positiva en $\hat{\beta}_n$ y que $\delta^{t_j}\delta_\pi = W_LW_CW_R$, concluimos que $\delta^{t_j}\delta_\pi$ admite una representación por medio de una palabra positiva en las bandas generadoras de $\hat{\beta}_n$.

Esto completa el paso inductivo y, por lo tanto, probamos que para todo ciclo descendente π, existe un entero k entre 0 y $n-1$ tal que $\delta^k\delta_\pi$ pertenece a $\hat{\beta}_n^+$.

Probemos ahora que tal entero es único entre 1 y $n-1$.

Supongamos que $\delta^k\delta_\pi$ y $\delta^{k'}\delta_\pi$ petenecen a H_n, donde k y k' son enteros entre 0 y $n-1$ inclusive. Podemos suponer sin pérdida de generalidad que $k \leq k'$. Tenemos entonces que $\delta^{k'-k}$ pertenece a H_n, de lo que deducimos que $k'-k$ es congruente a 0 módulo n, pues $\Pi(\delta^s)(n) = s$, donde Π denota la proyección canónica de β_n en el grupo simétrico Σ_n. Luego, como k y k' están entre 0 y $n-1$, sigue que $k = k'$. ■

3.2. **La forma normal.**

Teorema 3.2.1 (de la forma normal en $\hat{\beta}_n$)**.** *Todo elemento W en $\hat{\beta}_n$ admite una única representación de la forma:*

$$W = \hat{\delta}^{k(n-1)}B_1B_2\dots B_r,$$

donde k es algún entero, para cada i con $1 \leq i \leq$, B_i es una palabra positiva tal que $\Psi(B_i)$ admite una descomposición en β_n de la forma $\Psi(B_i) = \delta^{k_i}A_i$, para algún entero no negativo k_i menor que n y un factor canónico $A_i \neq \delta$, y además $A_i \lceil \tau^{-k_{i+1}}(A_{i+1})$ para todo i entre 1 y $n-1$.

Demostración. Sea W en $\hat{\beta}_n$ y sea $\Psi(W) = \delta^s A_1A_2\dots A_r$ la forma normal de $\Psi(W)$ en β_n. Por el lema anterior, sabemos que existe k_r un entero no negativo tal que $\delta^{k_r}A_r$ admite una representación por medio de una palabra positiva en las bandas generadoras de $\hat{\beta}_n$, B_r. Tenemos entonces que

$$\begin{aligned}
\Psi(W) &= \delta^s A_1A_2\dots A_r \\
&= \delta^s A_1A_2\dots A_{r-1}\delta^{-k_r}\delta^{k_r}A_r \\
&= \delta^s A_1A_2\dots A_{r-1}\delta^{-k_r}B_r \\
&= \delta^s\delta^{-k_r}\tau^{-k_r}(A_1)\tau^{-k_r}(A_2)\dots\tau^{-k_r}(A_{r-1})B_r \\
&= \delta^{s-k_r}\tau^{-k_r}(A_1)\tau^{-k_r}(A_2)\dots\tau^{-k_r}(A_{r-1})B_r.
\end{aligned}$$

Como $\tau^{-k_r}(A_{r-1})$ es un factor canónico en β_n, por la misma razón tenemos ahora que existe k_{r-1}, con $0 \leq k_{r-1} < n$, tal que $\delta^{k_{r-1}}\tau^{-k_r}(A_{r-1})$ admite una representación por medio de una palabra positiva en las bandas generadoras de $\hat{\beta}_n$, B_{r-1}. Entonces

$$\begin{aligned}
\Psi(W) &= \delta^{s-k_r}\tau^{-k_r}(A_1)\tau^{-k_r}(A_2)\dots\tau^{-k_r}(A_{r-1})\delta^{-k_r}B_r \\
&= \delta^{s-k_r}\tau^{-k_r}(A_1)\tau^{-k_r}(A_2)\dots\tau^{-k_r}(A_{r-2})\delta^{-k_{r-1}}\delta^{k_{r-1}}\tau^{-k_r}(A_{r-1})B_r \\
&= \delta^{s-k_r}\tau^{-k_r}(A_1)\tau^{-k_r}(A_2)\dots\tau^{-k_r}(A_{r-2})\delta^{-k_{r-1}}\delta^{k_{r-1}}\tau^{-k_r}(A_{r-1})B_r \\
&= \delta^{s-k_r-kr-1}\tau^{-k_r-k_{r-1}}(A_1)\tau^{-k_r-k_{r-1}}(A_2)\dots\tau^{-k_r-k_{r-1}}(A_{r-2})B_{r-1}B_r.
\end{aligned}$$

Así siguiendo, vemos que existen k_1; k_2; $\dots k_r$ enteros entre 0 y $n-1$ inclusive, tales que $\delta^{k_i}\tau^{-k_{i+1}-k_{i+2}\cdots-k_r}(A_i)$ admite una representación por medio de una palabra positiva en las bandas generadoras de $\hat{\beta}_n$, B_i. Además, para estas palabras se tiene que

$$\Psi(W) = \delta^{s-k_r-k_{r-1}\cdots-k_1}B_1B_2\dots B_r.$$

Como $\Psi(W)$ y $B_1B_2\dots B_r$ pertenecen a H_n, sigue que $\delta^{s-k_r-k_{r-1}\cdots-k_1}$ pertenece a H_n y, por lo tanto, $s-k_r-k_{r-1}\cdots-k_1$ es múltiplo de n. Luego, por el lema 3.1.1, $\delta^{s-k_r-k_{r-1}\cdots-k_1} = \delta^{kn} = \hat{\delta}^{k(n-1)}$.

Por otro lado tenemos que $B_i = \delta^{k_i}\tau^{-k_{i+1}-k_{i+2}\cdots-k_r}(A_i)$. Por lo que, para probar la existencia de una representación como la que se presenta en el teorema, falta ver que

$$\tau^{-k_{i+1}-k_{i+2}\cdots-k_r}(A_i)\lceil\tau^{-k_{i+1}}(\tau^{-k_{i+2}-k_{i+3}\cdots-k_r}(A_{i+1})),$$

que por el lema 2.4.8 se reduce a observar que $A_i\lceil A_{i+1}$.

Luego, vía Ψ^{-1} obtenemos una representación como la que describe el teorema.

Probemos ahora la unicidad de la misma.

Supongamos que W admite dos representaciones de esta forma, es decir que

$$W = \hat{\delta}^{k(n-1)}B_1B_2\ldots B_r = \hat{\delta}^{k'(n-1)}B'_1B'_2\ldots B'_{r'}.$$

Aplicando el morfismo Ψ tenemos que

$$\delta^{kn}\delta^{k_1}A_1\delta^{k_2}A_2\ldots\delta^{k_r}A_r = \delta^{k'n}\delta^{k'_1}A'_1\delta^{k'_2}A'_2\ldots\delta^{k'_{r'}}A'_{r'}.$$

Definamos ahora los factores canónicos

$$\tilde{A}_i = \tau^{k_r+k_{r-1}\cdots+k_{i+1}}(A_i) \quad \text{y} \quad \tilde{A'}_i = \tau^{k'_{r'}+k'_{r'-1}\cdots+k'_{i+1}}(A'_i).$$

Usando la observación 2.4.8 inductivamente podemos ver que

$$\delta^{kn}\delta^{k_1}A_1\delta^{k_2}A_2\ldots\delta^{k_r}A_r = \delta^{kn+k_1+k_2\cdots+k_r}\tilde{A}_1\tilde{A}_2\ldots\tilde{A}_r$$

y que

$$\delta^{k'n}\delta^{k'_1}A'_1\delta^{k'_2}A'_2\ldots\delta^{k'_{r'}}A'_{r'} = \delta^{k'n+k'_1+k'_2\cdots+k'_{r'}}\tilde{A'}_1\tilde{A'}_2\ldots\tilde{A'}_{r'},$$

de lo que deducimos que

$$\text{(I)} \quad \delta^{kn+k_1+k_2\cdots+k_r}\tilde{A}_1\tilde{A}_2\ldots\tilde{A}_r = \delta^{k'n+k'_1+k'_2\cdots+k'_r}\tilde{A'}_1\tilde{A'}_2\ldots\tilde{A'}_r.$$

Observemos ahora que $\tilde{A}_i\lceil\tilde{A}_{i+1}$, pues, como sabemos que $A_i\lceil\tau^{-k_{i+1}}(A_{i+1})$, por la observación 2.4.8, aplicando $\tau^{k_r+k_{r-1}\cdots+k_{i+1}}$, tenemos que

$$\tilde{A}_i = \tau^{k_r+k_{r-1}\cdots+k_{i+1}}(A_i)\lceil\tau^{k_r+k_{r-1}\cdots+k_{i+2}}(A_{i+1}) = \tilde{A}_{i+1}.$$

Análogamente se ve que $\tilde{A'}_i\lceil\tilde{A'}_{i+1}$, por lo que la igualdad (I) es una igualdad de formas normales para $\Psi(W)$ en β_n. Por la unicidad de la misma, tenemos que $r = r'$ y que $\tilde{A}_i = \tilde{A}'_i$ para todo i con $1 \leq i \leq r$.

Ahora bien, como $A_r = \tilde{A}_r$ y $A'_r = \tilde{A'}_r$, sigue que $A_r = A'_r$, de lo que deducimos, por el lema anterior, que $k_r = k'_r$ y que $B_r = B'_r$. De aquí, con un argumento similar se puede ver que $A_{r-1} = A'_{r-1}$ y por ende que $B_{r-1} = B'_{r-1}$ y, así siguiendo, que $B_i = B'_i$ para todo i, con $1 \leq i \leq r$. ∎

Aunque en este artículo no se desarrolle un algoritmo para encontrar formas normales, para el caso de trenzas de tipo A_n pueden encontrarse en [BKL] y, para el caso de las de tipo B_n, en [F].

REFERENCIAS

[A] E. Artin, *Theorie der Zopfe*, Hamburg Abh. **4** (1925), 42–72.

[B] D. Bessis, *The dual braid monoid*, Ann. Sci. École Norm. Sup. (4) **36** (2003), no. 5, 647–683.

[BKL] J. Birman, K. H. Ko y S. J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), no. 2, 322–353.

[BS] E. Brieskorn and K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972), 245–271.

[CP] A. H. Clifford y G. B. Preston, *Algebraic theory of semi-groups, Vol. I*, Amer. Math. Soc. Survey **7** (1961).
[D] T. tom. Dieck, *IV. Knot Algebra, Ch. 2, 3*, Braid groups of type B, 129-139.
[DG] F. Digne y Y. Gomi, *Presentation of pure braid groups*, J. Knot Theory Ramif. **10** (2001), no. 4, 609–623.
[F] S. Freyre, *Una presentación de los grupos de trenzas de tipo A_n y B_n, formas normales y aplicaciones*, Tesis de licenciatura. Departamento de Matemática, FCEyN, Universidad de Buenos Aires (2005).
[S] V. Sergiescu, *Graphes planaires et presentations des groupes de tresses*, Math. Z., **214** (1993).

FACULTAD DE CIENCIAS EXACTAS Y NATURALES, UNIVERSIDAD DE BUENOS AIRES