Ann. Scient. Éc. Norm. Sup.,
4e série, t. 37, 2004, p. 729 à 757.

ON THE STRUCTURE OF THE CENTRALIZER OF A BRAID

BY JUAN GONZÁLEZ-MENESES [1] AND BERT WIEST

ABSTRACT. – The mixed braid groups are the subgroups of Artin braid groups whose elements preserve a given partition of the base points. We prove that the centralizer of any braid can be expressed in terms of semidirect and direct products of mixed braid groups. Then we construct a generating set of the centralizer of any braid on n strands, which has at most $\frac{k(k+1)}{2}$ elements if $n = 2k$, and at most $\frac{k(k+3)}{2}$ elements if $n = 2k + 1$. These bounds are shown to be sharp, due to work of N.V. Ivanov and of S.J. Lee. Finally, we describe how one can explicitly compute this generating set.

RÉSUMÉ. – Un groupe de tresses mixtes est un sous-groupe d'un groupe de tresses d'Artin dont les éléments préservent une partition donnée des points de base. On démontre qu'on peut exprimer le centralisateur de toute tresse en termes de produits directs et semidirects de groupes de tresses mixtes. Ensuite, on construit une partie génératrice du centralisateur d'une tresse quelconque à n brins. Cette partie a au plus $\frac{k(k+1)}{2}$ éléments si $n = 2k$, et au plus $\frac{k(k+3)}{2}$ éléments si $n = 2k + 1$. On sait que ces bornes sont optimales, grâce à des travaux de N.V. Ivanov et de S.J. Lee. Enfin, on explique comment on peut calculer explicitement cette partie génératrice.

1. Introduction and statement of the results

In 1971, Makanin [26] gave an algorithm for computing a generating set of the centralizer $Z(\beta)$ of any given element β of the n-string braid group B_n. His method, however, tends to yield very large, and highly redundant generating sets. One hint that much smaller generating sets could be found came from the experimental results of González-Meneses and Franco, which were obtained with a radically improved version of Makanin's algorithm, based on new theoretical work [17]. Also, it has probably been clear to specialists for a long time that Nielsen–Thurston theory could be used to improve upon Makanin's results. However, there seems to be no such result in the literature, and the aim of the present paper is to fill this gap.

Although our main interest was to compute, for any given $\beta \in B_n$, a small generating set of $Z(\beta)$, we succeed in describing this centralizer in terms of semidirect and direct products of *mixed braid groups* (see [27,28]). These groups are defined as follows: let $X = \{P_1, \ldots, P_n\}$ be the base points of the braids in B_n. Given a partition $\mathcal{P}$ of X, the mixed braid group $B_{\mathcal{P}}$ consists of those braids whose associated permutation preserves each coset of $\mathcal{P}$.

The well known classification of mapping classes of a punctured surface into periodic, reducible and pseudo-Anosov ones, yields an analogous classification for braids. If β is reducible,

[1] Partially supported by MCYT, BFM2001-3207 and FEDER.

0012-9593/05/© 2004 Published by Elsevier SAS.

then one can decompose it, in a certain sense, into a *tubular braid* $\hat{\beta}$, and some *interior braids* $\beta_{[1]}, \ldots, \beta_{[t]}$, all of them having less than n stands. The main result of this paper is the following:

THEOREM 1.1. – *Let $\beta \in B_n$. One has*:
1. *If β is pseudo-Anosov , then $Z(\beta) \simeq \mathbb{Z}^2$.*
2. *If β is periodic, then $Z(\beta)$ is either B_n or isomorphic to a braid group on an annulus.*
3. *If β is reducible, then there exists a split exact sequence:*

$$1 \longrightarrow Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}) \longrightarrow Z(\beta) \longrightarrow Z_0(\hat{\beta}) \longrightarrow 1,$$

where $Z_0(\hat{\beta})$ is a subgroup of $Z(\hat{\beta})$, isomorphic either to $\mathbb{Z}^2$ or to a mixed braid group.

Notice that $\mathbb{Z} \simeq B_2 = B_{\{\{1,2\}\}}$, also $B_n = B_{\{\{1,\ldots,n\}\}}$, and finally the braid group over an annulus on k strands is isomorphic to $B_{\{\{1,\ldots,k\},\{k+1\}\}} \subset B_{k+1}$. Hence all these groups can be seen as mixed braid groups. Then, by recurrence on the number of strands we deduce the following:

COROLLARY 1.2. – *For every $\beta \in B_n$, the centralizer $Z(\beta)$ can be expressed in terms of semidirect and direct products of mixed braid groups.*

Using the above structure we shall construct, for any braid $\beta \in B_n$, a generating set of $Z(\beta)$ having very few elements. More precisely, we obtain:

THEOREM 1.3. – *If $\beta \in B_n$, then the centralizer $Z(\beta)$ can be generated by at most $\frac{k(k+1)}{2}$ elements if $n = 2k$, and at most $\frac{k(k+3)}{2}$ elements if $n = 2k+1$.*

We will present an example, communicated to us by S. J. Lee, showing that the above bound is sharp. That is, we will define, for every positive integer n, a braid in B_n whose centralizer cannot be generated by less than $\frac{k(k+1)}{2}$ elements if $n = 2k$, or less than $\frac{k(k+3)}{2}$ elements if $n = 2k+1$. (The first to observe that the number of generators of the centralizer may grow quadratically with the number of strands was N.V. Ivanov [22].)

However, the above bound refers to the worst case, and one could be interested in the minimal number of generators of a particular braid. We shall give a generating set which is in some sense the smallest "natural" generating set for the centralizer of a braid. However, we shall also give an example that illustrates the difficulty of finding the absolutely minimum possible number of generators.

Let us mention that, for the special case of reducible braids conjugated to a generator σ_i, its centralizer has already been described in [15]. Moreover, a different special case, namely the case of braids with only one moving string (and $n-1$ strictly vertical strings) was treated by Burde [10], who calculated the intersection of the centralizer of such a braid with the pure braid group. In fact, from his results one can extract a generating set of the centralizer whose size grows polynomially with the number of strings. Burde's article is remarkable for geometric approach.

The plan of the paper is as follows: in Section 2 we set up notation and some standard machinery, and give the mentioned example by S.J. Lee. In Section 3 we study $Z(\beta)$ in the case where β is periodic, Section 4 deals with the pseudo-Anosov case, and Section 5 the reducible one, which is the most involved. In Section 6 we define a generating set which is no larger than the stated upper bound. In Section 7 we describe a generating set which is as small as possible while still reflecting the geometric structure of the Nielsen–Thurston decomposition. We also give an example to show that by algebraic trickery, even smaller sets can be obtained. Finally in Section 8 we discuss how the generating set that we defined can be found algorithmically.

2. Prerequisites from Nielsen–Thurston theory

We denote by D the closed disk of radius 2 centered at 0 in the complex plane. For any $n \in \mathbb{N}$, the disk D, together with any choice of n distinct points in its interior, is denoted D_n, and the distinguished points are called the *punctures*. We shall use different choices for the exact position of the punctures at different times – they may be lined up on the real axis, or regularly distributed on a circle of radius 1, or again one of them may be in the centre while the remaining $n-1$ are distributed over the circle of radius 1. In most instances, the position of the punctures is irrelevant, and we shall leave it unspecified.

We recall that the braid group B_n is the group of isotopy classes of homeomorphisms fixing (pointwise) the boundary and permuting the punctures of D_n. Here the isotopies must fix pointwise the boundary and the punctures. Alternatively, B_n could be defined as the group of isotopy classes of disjoint movements of the punctures, starting and ending with the configuration of D_n. Yet another definition of B_n is as the set of isotopy classes of braids with n strings in the cylinder $D \times [0,1]$, where the start and end points of the strings are exactly the puncture points in $D_n \times \{0\}$ and $D_n \times \{1\}$. We shall use all three points of view.

We shall often work with a certain quotient of the group B_n, rather than with B_n itself. We recall that the center of B_n is isomorphic to the integers, and generated by the full twist Δ^2 (where Δ is Garside's half twist). Geometrically, the group projection $B_n \to B_n/\langle\Delta^2\rangle$ is given by smashing the boundary curve of D_n to a puncture, so that $B_n/\langle\Delta^2\rangle$ is naturally a subgroup of the mapping class group of the sphere with $n+1$ punctures. In order to keep notation manageable, we shall use the same letters for elements of the braid group B_n and for their image in the quotient $B_n/\langle\Delta^2\rangle$. This abuse of notation should not cause confusion.

We say that an element $\beta \in B_n$ is *periodic* if the element of $B_n/\langle\Delta^2\rangle$ represented by β is of finite order. Equivalently, β is periodic if there exists a $k \in \mathbb{N}$ such that in B_n we have that β^k is equal to some power of Δ^2.

We say an element β of B_n is *reducible* if there exists a nonempty multicurve C in D_n (i.e. a system of disjoint simple closed curves in D_n, none of them isotopic to the boundary or enclosing a single puncture) which is stabilized by β, i.e. such that $\beta(C)$ is isotopic to C. Note that β may permute different components of the multicurve C.

The following definition is taken from [8] (see also [21]). To every reducible braid $\beta \in B_n$ one can associate a canonical invariant multicurve: its *canonical reduction system*, which by definition is the collection of all isotopy classes c of simple closed curves which have the following two properties: firstly, c must be stabilized by some power of β, and secondly any simple closed curve which has non-zero geometric intersection number with c must *not* be stabilized by any power of β. For instance, let us consider the punctured disk D_6, where the 6 punctures are arranged uniformly on the circle of radius 1 around 0. Then the rotation of the punctures around the circle by an angle of $\frac{2\pi}{3}$ is a periodic element of B_6 (of period 3), it is also reducible (e.g. the three simple closed curves encircling punctures 1 and 2, 3 and 4, and 5 and 6 respectively form an invariant multicurve), but its canonical reduction system is empty. This example, however, is somewhat untypical: if a *non-periodic* braid is reducible, then its canonical reduction system is nonempty (see [21]).

If C is an invariant multicurve of a reducible braid β, then we define the *tubular braid* induced by β and C to be the braid on fewer strings obtained from β by removing from D_n all the disks bounded by outermost curves of C, and collapsing each outermost curve of C to a puncture point. It should be stressed that this braid is only defined up to conjugacy.

An alternative way to look at the same definition is the following: let us consider again β as an isotopy class of n disjoint strings in $D \times [0,1]$ with extremal points at the puncture points of $D_n \times \{0\}$ and $D_n \times \{1\}$, such that each disk $D \times \{t\}$ intersects each string exactly once. Now

our picture can be completed by embedded cylinders in $D \times [0,1]$ which are disjoint from each other and from the strings of the braid, each of which intersects each disk $D \times \{t\}$ in exactly one circle, and whose boundary components are exactly the outermost curves of C in $D \times \{0\}$ and $D \times \{1\}$. We can interpret the solid cylinders bounded by these cylinders as "fat strings", and the resulting braid with some fat strings is exactly the tubular braid defined above.

The *interior* braids induced by β and C are the braids on fewer strings induced by β at the interior of the discs bounded by the outermost curves of C. They can be thought of as the braids 'inside' the tubes of the tubular braid. Therefore, for every reducible braid β, and every invariant multicurve C, we can decompose β into one tubular braid and some interior braids – as many as the number of outermost curves in C.

Finally, we have the notion of a *pseudo-Anosov* element of B_n, for which we refer to [14] or [21]. Roughly speaking, $\beta \in B_n$ is pseudo-Anosov if it is represented by a homeomorphism of D_n which preserves two transverse measured foliations on D_n (called the "stable" and the "unstable" foliation), while scaling the measure of the unstable one by some factor λ which is greater than 1, and the measure of the stable one by $\frac{1}{\lambda}$.

Thurston's theorem [33,14] states that every irreducible element of B_n is either periodic or pseudo-Anosov.

We end this section with the promised example, due to S.J. Lee, that should be helpful for understanding the relationship between the Nielsen–Thurston decomposition and the centralizer subgroup of a braid $\beta \in B_n$. This example was also found independently by N.V. Ivanov and H. Hamidi-Tehrani [23].

Example 2.1. – Suppose that $n = 2m$, and denote by σ_i the standard generator of B_n, in which the ith and the $(i+1)$st punctures permute their positions in a clockwise sense. We define $\beta = \sigma_1 \sigma_3^2 \sigma_5^3 \cdots \sigma_{2m-1}^m$.

The canonical reduction system of β consists of m circles, the ith one enclosing the punctures $2i-1$ and $2i$. The corresponding tubular braid is the trivial braid of B_m, and the interior braids are, respectively, σ_1, σ_1^2, …, σ_1^m (notice that all of them are non-conjugate, since conjugate braids have the same exponent sum).

Let $D_{(1)}, \ldots, D_{(m)}$ be the disks bounded by the above circles. As we shall see, any braid that commutes with β has to send each disk $D_{(i)}$ to itself (since the interior braids are non-conjugate). A generating set of the centralizer subgroup of β is given by

(i) for each $i \in \{1, \ldots, m\}$, the braid σ_{2i-1}, whose support is contained in $D_{(i)}$,

(ii) any generating set for the pure braid group on m strings P_m – all the generators here act as the identity on $D_{(1)} \cup \cdots \cup D_{(m)}$, and can be seen as a pure tubular braid on m strings (tubes), where the ith tube starts and ends at $D_{(i)}$.

It can be easily shown that, in this case, $Z(\beta) \simeq \mathbb{Z}^m \times P_m$. The essential observation now is the following: it can be deduced by the presentation given in [6], that the abelianization of P_m is isomorphic to $\mathbb{Z}^{m(m-1)/2}$ (see also [1]). Hence, the abelianization of $Z(\beta)$ is isomorphic to $\mathbb{Z}^m \times \mathbb{Z}^{m(m-1)/2}$. Therefore, at least $m + \frac{m(m-1)}{2} = \frac{m(m+1)}{2}$ generators are needed for the centralizer of the braid β.

The case when $n = 2m+1$ is analogous. The braid proposed by S.J. Lee is: $\beta = \sigma_2 \sigma_4^2 \sigma_6^3 \cdots \sigma_{2m}^m$. This time the first strand is not enclosed by any curve of the canonical reduction system of β, and one has: $Z(\beta) \simeq \mathbb{Z}^m \times P_{m+1}$. Hence, in this case the minimal possible number of generators is $m + \frac{m(m+1)}{2} = \frac{m(m+3)}{2}$.

By proving Theorem 1.3, we will show that the above examples are the worst one can find.

3. The periodic case

We have to start by describing the periodic elements of B_n. In order to state this classification result, which is classical, we need to define two braids.

If D_n is the disk with n punctures arranged regularly on the circle of radius 1, then the braid which we shall call $\delta_{(n)}$ is represented by a counterclockwise movement of all punctures on this circle by an angle $\frac{2\pi}{n}$. If no confusion is possible, we shall simply write δ, without indicating the number of strands (note that this braid is the Garside element of the Birman–Ko–Lee structure of B_n [7]).

Similarly, if we think of D_n as having one puncture in the centre, and $n-1$ punctures arranged circularly around it, then we define $\gamma_{(n)} \in B_n$ to be the braid given by a circular movement of the $n-1$ punctures by an angle of $\frac{2\pi}{n-1}$, while leaving the central puncture fixed. Again, for simplicity we shall often only write γ instead of $\gamma_{(n)}$.

The result that classifies periodic braids, which is due to Eilenberg [12] and de Kerékjártó [24] (see [11] for a modern exposition) is:

LEMMA 3.1. – *Every periodic braid in B_n is conjugate to a power of $\delta_{(n)}$ or $\gamma_{(n)}$.*

Thus we only need to consider the centralizer subgroups of $\delta_{(n)}^k$ and $\gamma_{(n)}^k$ for all $n, k \in \mathbb{Z}$, since the centralizers of conjugate elements are isomorphic by an inner automorphism of B_n. This problem has been solved by Bessis, Digne and Michel [4], on the wider context of complex reflexion groups. We shall explain their result in the particular case of braid groups:

We suppose first that $\beta = \delta_{(n)}^k$ where, without loss of generality, $k \geqslant 0$. Let $d = \gcd(n, k)$. For $u = 1, \ldots, n$, we will denote $P_u = e^{i2\pi u/n}$ the punctures of D_n, so $\beta = \delta_{(n)}^k$ sends P_u to P_{u+k} for every u (the indices are taken modulo n). Hence the permutation induced by β has d orbits (cycles) of length $r = \frac{n}{d}$, that we denote by $\mathcal{C}_1, \ldots, \mathcal{C}_d$. See in Fig. 1 an example where $n = 12$, $k = 9$, $d = 3$ and $r = 4$: the braid $\delta_{(12)}$ and the three orbits of $\delta_{(12)}^9$.

If $r > 1$ (that is if $d < n$), consider the once punctured disc $D^* = D \backslash \{0\}$, and the r-sheeted covering $\theta = \theta_r : D^* \to D^*$ defined by $\theta(ae^{it}) = ae^{itr} = ae^{itn/d}$. The orbits $\mathcal{C}_1, \ldots, \mathcal{C}_d$ are sent by θ to the points $Q_1, \ldots, Q_d$, where $Q_u = e^{i2\pi u/d}$. If we consider the half-line $L = \{ae^{i\pi/d}, a \in]0, 2]\}$ (notice that L passes between Q_d and Q_1), then $D^* \backslash L$ is a fundamental region for θ (see Fig. 2).

Now notice that every braid in $B_d(D^*)$ can be lifted, by θ^{-1}, to a braid in B_n in a natural way. The resulting braid is a $\frac{2\pi d}{n}$-symmetric braid, that is, it is invariant under a rotation by an angle of $\frac{2\pi d}{n}$. But then it is also invariant under a rotation of angle $\frac{2\pi k}{n}$; in other words, the resulting braid commutes with β. Hence we have a natural homomorphism: $\theta^* : B_d(D^*) \to B_n$ whose image is contained in $Z(\beta)$. Then one has

THEOREM 3.2 [4]. – *The natural homomorphism $\theta^* : B_d(D^*) \to Z(\delta_{(n)}^k)$ is an isomorphism.*

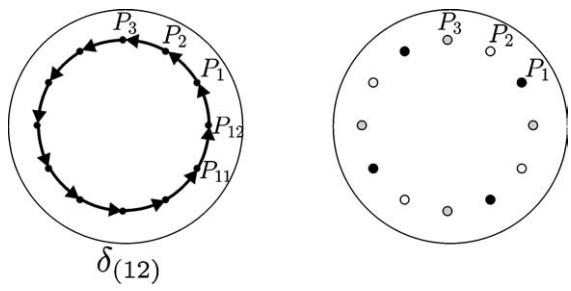

Fig. 1. The braid $\delta \in B_{12}$, and the three orbits of δ^9 (in black, white and grey).

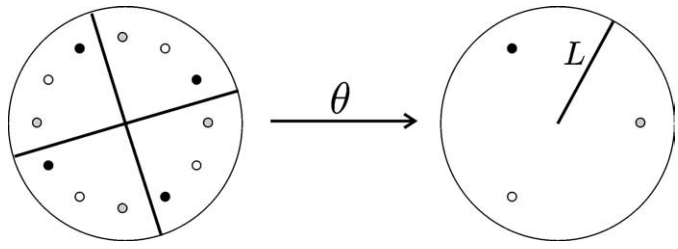

Fig. 2. The covering map $\theta = \theta_4$ associated to $\delta_{(12)}^9$.

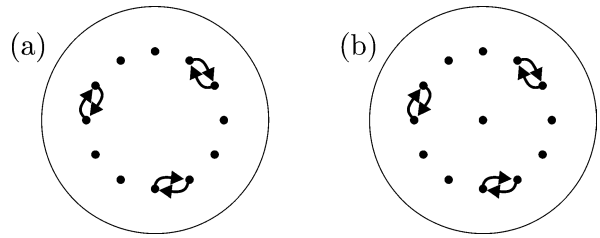

Fig. 3. Generators $\theta_3^*(\sigma_1)$ and $\bar{\theta}_3^*(\sigma_1)$ of the centralizers of $\delta_{(12)}^4$ and $\gamma_{(13)}^4$.

In other words, every element in the centralizer of $\beta = \delta_{(n)}^k$ can be seen (via θ) as a braid on a once punctured disc, that is, a braid on an annulus. Notice that if $r = 1$ (that is, if k is a multiple of n), then β is a power of $\delta_{(n)}^n = \Delta_{(n)}^2$. In this case θ is the identity map, and the fundamental region is the whole D_n. Hence the centralizer of β is the whole B_n, as one should expect.

Since we are interested in minimising the set of generators, we observe that if $d = n$ (thus $r = 1$), then $Z(\beta) = B_n$ is generated by two elements, namely Artin's σ_1 and Birman–Ko–Lee's δ. In a similar way, if $1 < d < n$, then the braid group $B_d(D^*)$ is generated by just two elements, namely $\delta_{(n)} = \theta^*(\delta_{(d)})$ and the braid $\theta^*(\sigma_1)$ shown in Fig. 3(a). Notice that this case contains the above one, where θ^* is the identity. Finally, if $d = 1$ then $B_1(D^*)$ is cyclic. Thus we have:

PROPOSITION 3.3. – *If k and n are coprime, then $Z(\delta_{(n)}^k)$ is generated by a single element, namely $\delta_{(n)}$. If, by contrast, $gcd(k, n) \geqslant 2$, then $Z(\delta_{(n)}^k)$ is generated by two elements: $\delta_{(n)}$ and the braid $\theta^*(\sigma_1)$.*

It is clear that the generating set given by Proposition 3.3 is indeed minimal. Next we study the centralizer of $\beta = \gamma_{(n)}^k$, still following the work in [4]. This time we call $d = \gcd(n-1, k)$, and $r = (n-1)/d$. If $d < n-1$, the above map θ induces a natural homomorphism $\bar{\theta}^* = \bar{\theta}_r^* : B_d(D^*) \to B_n$, where this time the central point of D is considered as a puncture. Hence, the central strand of every braid coming from $B_d(D^*)$ is trivial. We observe that the image of this homomorphism is contained in $Z(\beta)$, and in fact one has:

THEOREM 3.4 [4]. – *The natural homomorphism $\bar{\theta}_r^* : B_d(D^*) \to Z(\gamma_{(n)}^k)$ is an isomorphism.*

By contrast, if $d = n-1$, then β is a power of $\gamma^{n-1} = \Delta^2$, so $\overline{\theta}_r^* = 1$, $Z(\beta) = B_n$ and everything works as above. Hence we have

PROPOSITION 3.5. – *If k and $n-1$ are coprime, then $Z(\gamma_{(n)}^k)$ is generated by a single element, namely $\gamma_{(n)}$. If, by contrast, $gcd(k, n-1) = d \geqslant 2$, then $Z(\gamma_{(n)}^k)$ is generated by two elements: $\gamma_{(n)} = \bar{\theta}^*(\delta_{(d)})$ and the braid $\bar{\theta}^*(\sigma_1)$.*

See Fig. 3(b) for an illustration of the braid $\bar{\theta}^*(\sigma_1)$. We summarize all the results in this section as follows:

COROLLARY 3.6. – *The centralizer of any periodic braid in B_n either equals B_n or is isomorphic to $B_d(D^*)$, for some $d < n$. In particular, it can be generated by at most two elements.*

We end with a result that will be helpful later:

COROLLARY 3.7. – *If k is not a multiple of n, then $Z(\delta_{(n)}^k) \cong Z(\gamma_{(n+1)}^k)$.*

Proof. – Both groups are isomorphic to $B_d(D^*)$, where $d = \gcd(n, k)$. An actual isomorphism can be defined as follows: take any element $\alpha \in Z(\delta_{(n)}^k)$, isotope it to make it $\frac{2\pi k}{n}$-symmetric, and then add a trivial strand based at the central point of D_n. □

4. The pseudo-Anosov case

PROPOSITION 4.1. – *If $\beta \in B_n$ is pseudo-Anosov, then the centralizer of B_n is free abelian and generated by two elements*: *some pseudo-Anosov α which has the same stable and unstable projective measured foliation as β* (*possibly β itself*), *and one periodic braid ρ* (*a root of Δ^2, possibly Δ^2 itself*).

We stress that the generating set promised by Proposition 4.1 is obviously minimal. For proving this result, it is more convenient to think about the quotient group $B_n/\langle\Delta^2\rangle$. Since $\langle\Delta^2\rangle$ is the center of B_n, it is contained in the centralizer of any element. Hence the centralizer of an element in B_n is just the preimage of the centralizer of its corresponding mapping class in $B_n/\langle\Delta^2\rangle$. Thus, for the rest of this section, we shall work in this quotient $B_n/\langle\Delta^2\rangle$; we shall prove the following result, from which Proposition 4.1 will then be deduced:

PROPOSITION 4.2. – *If $\beta \in B_n/\langle\Delta^2\rangle$ is pseudo-Anosov, then the centralizer of β is abelian, and is generated by some pseudo-Anosov α which has the same stable and unstable projective measured foliation as β, and possibly one element ρ of finite order.*

Proof of Proposition 4.2. – We start by observing that the pseudo-Anosov element β cannot commute with any reducible element $a \in B_n/\langle\Delta^2\rangle$, except possibly with periodic ones – thus all elements of $Z(\beta) \subset B_n/\langle\Delta^2\rangle$ are either pseudo-Anosov or periodic. To see this, let us assume that the canonical reduction system C of a is non-empty. Then the canonical reduction system of $\beta^{-1}a\beta$ is $\beta(C)$. If it were true that $\beta^{-1}a\beta = a$, then we would have $\beta(C) = C$, which is impossible since it is well known that pseudo-Anosov homeomorphisms do not stabilise any curves or multicurves. (This result is also a special case of Corollary 7.13 of [21].)

Our next claim is that all pseudo-Anosov elements in $Z(\beta)$ have the same stable and unstable projective measured foliations. In order to prove this, we can apply Corollaries 7.15 and 8.4 of [21]: since the centralizer subgroup of β is infinite and irreducible, it follows that $Z(\beta)$ contains an infinite cyclic group as a subgroup of finite index. It follows that if a is any pseudo-Anosov element in the centralizer of β, then there exist $k, k' \in \mathbb{N}$ such that $a^k = \beta^{k'}$. Since all powers of a pseudo-Anosov element have the same stable and unstable projective measured foliation, it follows that a has the same stable and unstable projective measured foliations as β, and so do all pseudo-Anosov elements of $Z(\beta) \subseteq B_n/\langle\Delta^2\rangle$.

Next we make an essential observation which only works for braid groups, and does not generalize to mapping class groups of surfaces with no boundary, or with more than two boundary components: all elements of $B_n/\langle\Delta^2\rangle$, regarded as a subgroup of the mapping class group of the $n+1$ times punctured sphere, fix the puncture which came from collapsing the boundary

of D_n. Moreover, there are singular leaves of the stable and unstable foliation of β emanating from this puncture, at least one of each (like for every other puncture). In the cyclic ordering around the puncture, singular leaves of the stable and unstable foliation alternate. If an element a of $B_n/\langle\Delta^2\rangle$ commutes with β, then the action of a has to preserve the projective stable and unstable foliations. Thus in the cyclic ordering around our preferred puncture, the action of a can only induce a cyclic (possibly trivial) permutation of the singular leaves (sending stable to stable, and unstable to unstable leaves, nevertheless).

Now we see that an element a of $Z(\beta) \subseteq B_n/\langle\Delta^2\rangle$ is uniquely determined by just two data: firstly the stretch factor λ by which its action on the unstable measured foliation of β multiplies the measure of that foliation. (This factor λ equals 1 if a is periodic, and belongs to the set $\mathbb{R}_+ \setminus \{1\}$ if a is pseudo-Anosov.) And secondly by the cyclic permutation of the leaves of the stable projective foliation emanating from the distinguished puncture of the $n+1$ times punctured sphere. Indeed, if a and b share both data, then ab^{-1} has stretch factor 1 (so it is periodic), and preserves the singular leaves. Hence it is the identity in $B_n/\langle\Delta^2\rangle$, so $a = b$.

This implies that the set of periodic elements of $Z(\beta)$ forms a subgroup of $Z(\beta)$ which is either trivial or isomorphic to $\mathbb{Z}/k\mathbb{Z}$, where k is a divisor of the number of singular leaves of the stable foliation emanating from the preferred puncture. Any generator of this subgroup can play the rôle of our desired generator ρ of $Z(\beta) \subseteq B_n/\langle\Delta^2\rangle$.

Now ρ commutes with any other element in $Z(\beta)$, because their commutator has stretch factor 1 and induces the trivial permutation of the prongs around the preferred singularity.

Now notice that the stretch factor yields a multiplicative map from $Z(\beta)$ to $\mathbb{R}^+$. But it is known that the set of possible stretch factors for a given foliation is discrete (see [21]), so the image of $Z(\beta)$ under this map must be a cyclic subgroup of $\mathbb{R}^+$. Take an element α whose stretch factor λ generates this group. Then α is pseudo-Anosov and the stretch factor of any element in $Z(\beta)$ must be a power of λ.

We now have that α and ρ generate $Z(\beta) \in B_n/\langle\Delta^2\rangle$, because any element in $Z(\beta)$ can be multiplied by some power of α so as to obtain an element with stretch factor 1, i.e. a power of ρ.

It follows that $Z(\beta) \subset B_n/\langle\Delta^2\rangle$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, with generators α and ρ. This completes the proof of Proposition 4.2. □

Proof of Proposition 4.1. – By Proposition 4.2, $Z(\beta) \subset B_n/\langle\Delta^2\rangle$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, with generators α and ρ. But then $Z(\beta) \subset B_n$ is just the preimage of $Z(\beta) \subset B_n/\langle\Delta^2\rangle$ under the natural projection. Consider the subgroup $\langle\rho\rangle \subset Z(\beta) \subset B_n/\langle\Delta^2\rangle$. Its preimage is an infinite cyclic group in B_n that contains $\langle\Delta^2\rangle$. We can suppose (up to choosing an appropriate ρ), that the generator of this cyclic group projects to ρ, so we call it ρ as well. Notice that ρ is a root of Δ^2, since Δ^2 belongs to $\langle\rho\rangle$. Then we choose an element in B_n that projects to α, and we also call it α. We must prove that in B_n we still have $Z(\beta) = \langle\alpha\rangle \times \langle\rho\rangle$.

But every element in $Z(\beta) \subset B_n$ can be written as $\alpha^k\rho^l\Delta^{2m}$. Since Δ^2 is a power of ρ, then $\{\alpha, \rho\}$ is a set of generators of $Z(\beta)$. On the other hand, the commutator of α and ρ projects to the trivial mapping class, hence it equals Δ^{2k} for some k. But the algebraic number of crossings of the braid Δ^{2k} is $kn(n-1)$, while for the commutator of any two elements this number is zero. Hence $k = 0$, so α and ρ commute. Finally, it is well known that B_n is torsion-free, so $Z(\beta)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, as we wanted to show. □

5. The reducible case

It remains to study the centralizer of a non-periodic reducible braid β. Recall that for every braid γ one has $Z(\gamma^{-1}\beta\gamma) = \gamma^{-1}Z(\beta)\gamma$. Hence, in general we will not study $Z(\beta)$, but the

centralizer of a suitable conjugate of β, which will be easier to describe. Throughout this section we shall think of the punctures of the disk D_n as being lined up on the real axis.

5.1. Reducible braids in regular form

As we saw in Section 2, if β is a non-periodic reducible element, then its canonical reduction system is nonempty. We denote by $R'(\beta)$ the set of outermost curves in the canonical reduction system of β. It is determined by β up to isotopy fixing the punctures. Since we can study any conjugate of β, we can suppose that $R'(\beta)$ is a family of disjoint circles centered at the real axis, with disjoint interiors, each one enclosing more than one and less than n punctures.

Notice that there could be punctures in D_n not enclosed by any circle in $R'(\beta)$. In order to simplify the notations below, we define the system of curves $R(\beta)$ to contain exactly the curves of $R'(\beta)$, plus one circle around each such puncture of D_n. These new circles are called the degenerate circles of $R(\beta)$. We now have that every puncture in D_n is enclosed by exactly one circle in $R(\beta)$.

Notice that β preserves $R(\beta)$, but it could permute the circles. We will suppose that this permutation has t orbits (or cycles) $\mathcal{C}_1, \dots, \mathcal{C}_t$. That is, $\mathcal{C}_i$ is a family of circles $\{C_{i,1}, \dots, C_{i,r_i}\} \subset R(\beta)$ such that β sends $C_{i,k}$ to $C_{i,k+1}$ (here the second index is taken modulo r_i). Then one has $R(\beta) = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_t = \{C_{1,1}, \dots, C_{1,r_1}\} \cup \cdots \cup \{C_{t,1}, \dots, C_{t,r_t}\}$. If m_i is the number of punctures inside $C_{i,k}$, for any k, then $1 \leqslant m_i < n$ and $m_1 r_1 + \cdots + m_t r_t = n$.

Let $\hat{\beta}$ be the tubular braid induced by β and $R(\beta)$. Then $\hat{\beta} \in B_m$, where $m = r_1 + \cdots + r_t$. For $i = 1, \dots, t$ and $k = 1, \dots, r_i$, let $\beta_{i,k}$ be the braid induced by β in the interior of $C_{i,k}$. In other words, $\beta_{i,k}$ is the braid inside the tube of $\hat{\beta}$ which starts at $C_{i,k}$ and ends at $C_{i,k+1}$. We will call the braids $\beta_{i,k}$ the *interior braids* of β. Notice that the interior braids of each degenerate circle is just a trivial braid on one string.

In Fig. 4 we can see an example of a reducible braid $\beta \in B_{13}$, and its corresponding tubular braid $\hat{\beta} \in B_6$. In this example we have three orbits, and the following data: $r_1 = 3$, $r_2 = 2$, $r_3 = 1$; $m_1 = 2$, $m_2 = 3$, $m_3 = 1$, $\beta_{1,1} = \sigma_1^2$, $\beta_{1,2} = \sigma_1^{-1}$, $\beta_{1,3} = 1$, $\beta_{2,1} = \sigma_1\sigma_2$, $\beta_{2,2} = \sigma_1^{-1}\sigma_2$, $\beta_{3,1} = 1$ and $\hat{\beta} = \sigma_3^2\sigma_2\sigma_1\sigma_5^2\sigma_4$.

It would be desirable for β to have its interior braids as simple as possible, in order to study its centralizer. We propose the following:

DEFINITION 5.1. – Let $\beta \in B_n$ be a non-periodic reducible braid. Then β will be said to be in *regular form* if (using the notation introduced above) it satisfies the following conditions:

1. The only non-trivial interior braids in β are $\beta_{1,r_1}, \beta_{2,r_2}, \dots, \beta_{t,r_t}$ – we shall denote these braids by $\beta_{[1]}, \beta_{[2]}, \dots, \beta_{[t]}$.
2. For $i, j \in \{1, \dots, t\}$, if $\beta_{[i]}$ and $\beta_{[j]}$ are conjugate, then $\beta_{[i]} = \beta_{[j]}$.

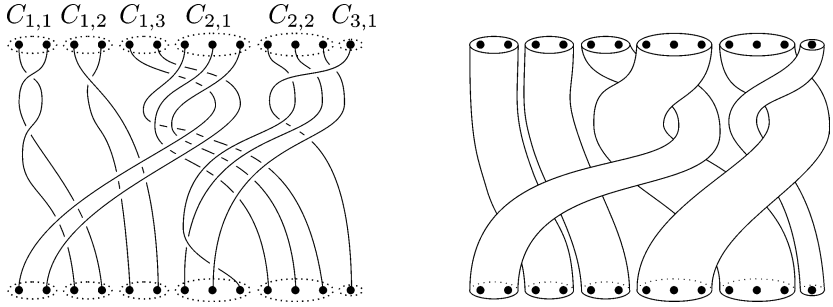

Fig. 4. Example of a reducible braid β, and its corresponding tubular braid $\hat{\beta}$.

Hence, if β is in regular form, there is at most one non-trivial interior braid for each orbit, and any two interior braids are either equal or non-conjugate. Fortunately, one can conjugate every non-periodic reducible braid β to another one in regular form, as we are going to see.

First, consider the subgroup $B_{R(\beta)} \subset B_n$ consisting of those braids preserving $R(\beta)$. For $\alpha \in B_{R(\beta)}$, we can consider the tubular braid $\hat{\alpha}$ induced by α and $R(\beta)$. Every $\alpha \in B_{R(\beta)}$ is completely determined by $\hat{\alpha}$ and its interior braids $\alpha_{i,k}$, for $i = 1, \dots t$ and $k = 1, \dots, r_i$.

Now consider, in β, an orbit $\mathcal{C}_i = \{C_{i,1}, \dots, C_{i,r_i}\}$ and the interior braids $\beta_{i,1}, \dots, \beta_{i,r_i} \in B_{m_i}$. We define $\alpha \in B_{R(\beta)}$ as follows: $\hat{\alpha}$ is trivial, $\alpha_{j,k} = 1$ if $j \neq i$, and $\alpha_{i,k} = \beta_{i,k}\beta_{i,k+1} \cdots \beta_{i,r_i}$. If we conjugate β by α, we obtain $\beta' = \alpha^{-1}\beta\alpha$, which has the following properties:

- $\hat{\beta}' = \hat{\beta}$.
- $\beta'_{j,k} = \beta_{j,k}$, for $j \neq i$.
- $\beta'_{i,k} = (\alpha_{i,k})^{-1}\beta_{i,k}\alpha_{i,k+1} = (\beta_{i,r_i}^{-1} \cdots \beta_{i,k}^{-1})(\beta_{i,k} \cdots \beta_{i,r_i}) = 1$, for $k \neq r_i$.
- $\beta'_{i,r_i} = (\alpha_{i,r_i})^{-1}\beta_{i,r_i}\alpha_{i,1} = \beta_{i,r_i}^{-1}\beta_{i,r_i}(\beta_{i,1} \cdots \beta_{i,r_i}) = \beta_{i,1} \cdots \beta_{i,r_i}$.

In other words, if we conjugate β by α we 'transfuse' all the interior braids in $\mathcal{C}_i$ to the last tube C_{i,r_i}, so β'_{i,r_i} becomes the only nontrivial interior braid in $\mathcal{C}_i$. In Fig. 5 we can see an example of such a conjugation, where $\beta_{[i]}$ denotes the product $\beta_{i,1} \cdots \beta_{i,r_i}$. We can now do the same for every $i = 1, \dots, t$. Therefore, since we are interested in β up to conjugacy, we can suppose that $\beta_{i,k} = 1$ if $k \neq r_i$ and denote $\beta_{[i]} = \beta_{i,r_i}$, for every $i = 1, \dots, t$.

Now suppose that some $\beta_{[i]}$ is conjugate to some $\beta_{[j]}$, and let $h_{i,j}$ be a conjugating braid, that is, $h_{i,j}^{-1}\beta_{[i]}h_{i,j} = \beta_{[j]}$. Consider the braid $\alpha \in B_{R(\beta)}$ such that $\hat{\alpha} = 1$, $\alpha_{j,k} = 1$ for $j \neq i$ and $\alpha_{i,k} = h_{i,j}$ for every k. As we can see in Fig. 6, if we conjugate β by α, then $\beta_{[i]}$ is replaced by

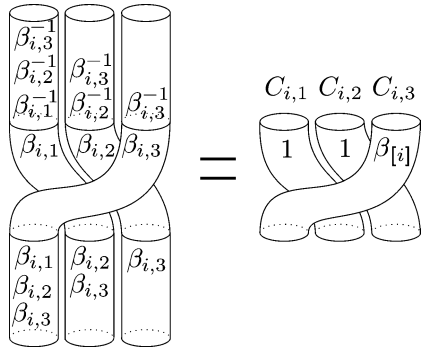

Fig. 5. How to conjugate β to simplify interior braids.

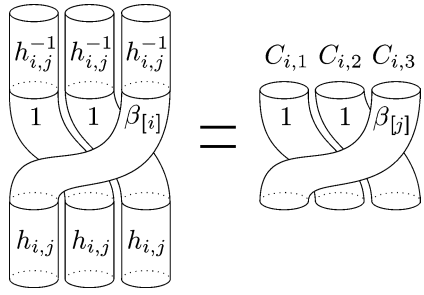

Fig. 6. How to replace $\beta_{[i]}$ by $\beta_{[j]}$ if they are conjugate.

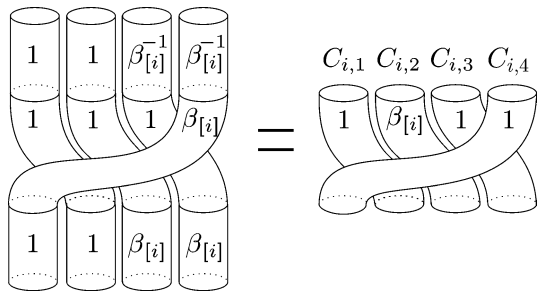

Fig. 7. How to move $\beta_{[i]}$ from $C_{i,4}$ to $C_{i,2}$, when $r_i = 4$.

$\beta_{[j]}$. Therefore, we can assume that for $i, j \in \{1, \dots, t\}$, either $\beta_{[i]} = \beta_{[j]}$ or $\beta_{[i]}$ and $\beta_{[j]}$ are not conjugate, and therefore we can suppose that β is in regular form.

Notice that we have chosen to put $\beta_{[i]}$ into the tube starting at C_{i,r_i}. But we can move it to any other tube of $\mathcal{C}_i$ if we wish, by a suitable conjugation, and later on we will need to use this. Hence we define, for $i \in \{1, \dots, t\}$ and $k \in \{1, \dots, r_i - 1\}$, a braid $\mu = \mu(i, k)$ that will 'move' the interior braid $\beta_{[i]}$ to the tube $C_{i,k}$. This braid is defined as follows: the tubular braid $\hat{\mu}$ is trivial, and the interior braids are all trivial except $\mu_{i,k+1} = \mu_{i,k+2} = \cdots = \mu_{i,r_i} = \beta_{[i]}$. We can see in Fig. 7 how this works.

5.2. Centralizer of a braid in regular form

We will now study the centralizer of β, assuming that β is in regular form. Recall that the only non-trivial interior braids of β are denoted $\beta_{[1]}, \dots, \beta_{[t]}$, and that $\hat{\beta}$ is the tubular braid associated to β and $R(\beta)$. In this section we will show that there is an exact sequence:

$$1 \to Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}) \xrightarrow{g} Z(\beta) \xrightarrow{p} Z_0(\hat{\beta}) \to 1,$$

where $Z_0(\hat{\beta})$ is a subgroup of $Z(\hat{\beta})$. Later on we will see that this sequence splits.

For $i \in \{1, \dots, t\}$, consider the centralizer $Z(\beta_{[i]})$ in B_{m_i}. We define a map

$$g_i : Z(\beta_{[i]}) \to B_{R(\beta)}$$

as follows: given $\gamma \in Z(\beta_{[i]})$, $g_i(\gamma)$ is the braid $\alpha \in B_{R(\beta)}$ satisfying $\hat{\alpha} = 1$, $\alpha_{j,k} = 1$ for $j \neq i$, and $\alpha_{i,k} = \gamma$ for $k = 1, \dots, r_i$. We need to show the following:

PROPOSITION 5.2. – *The map g_i defined above is an injective homomorphism, and its image is contained in $Z(\beta)$.*

Proof. – The map g_i is given by the diagonal homomorphism $Z(\beta_{[i]}) \to Z(\beta_{[i]}) \times \cdots \times Z(\beta_{[i]})$ (r_i factors), followed by the homomorphism induced by an inclusion of r_i copies of an m_i-times punctured disk into r_i disjoint subdisks (each containing m_i punctures) of D_n. By the results of [29] we can deduce that g_i is indeed an injective homomorphism.

It remains to show that for every $\gamma \in Z(\beta_{[i]})$ one has $\alpha = g_i(\gamma) \in Z(\beta)$. Since $\hat{\alpha}$ is trivial, $\widehat{\alpha^{-1}\beta\alpha} = \hat{\alpha}^{-1}\hat{\beta}\hat{\alpha} = \hat{\beta}$. So we just need to show that the interior braids of $\alpha^{-1}\beta\alpha$ and β coincide. For $j \neq i$, the braids $\alpha_{j,k}$ are trivial for every k, so $(\alpha^{-1}\beta\alpha)_{j,k} = \beta_{j,k}$. Now, for $k \neq r_i$, one has $(\alpha^{-1}\beta\alpha)_{i,k} = \alpha_{i,k}^{-1}\beta_{i,k}\alpha_{i,k+1} = \gamma^{-1}1\gamma = 1 = \beta_{i,k}$. Finally, since γ commutes with $\beta_{[i]}$, one has $(\alpha^{-1}\beta\alpha)_{i,r_i} = \alpha_{i,r_i}^{-1}\beta_{i,r_i}\alpha_{i,1} = \gamma^{-1}\beta_{[i]}\gamma = \beta_{[i]} = \beta_{i,r_i}$. Therefore $\alpha^{-1}\beta\alpha = \beta$, so the image of g_i is contained in $Z(\beta)$. □

PROPOSITION 5.3. – *The map $g : Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}) \longrightarrow Z(\beta)$ defined by $g(\gamma_1, \ldots, \gamma_t) = g_1(\gamma_1) \cdots g_t(\gamma_t)$ is an injective homomorphism.*

Proof. – Given $\gamma \in Z(\beta_{[i]})$, the only nontrivial strands in $g_i(\gamma)$ are those inside the tubes $C_{i,1}, \ldots, C_{i,r_i}$. Hence if $i \neq j$, $\gamma \in Z(\beta_{[i]})$ and $\delta \in Z(\beta_{[j]})$, then $g_i(\gamma)$ and $g_j(\delta)$ commute. Since every g_i is a homomorphism, this shows that g is also a homomorphism. But we know by the previous proposition that g_i is injective for $i = 1, \ldots, t$. Using an argument similar to the proof of Proposition 5.2, one can deduce that g is also injective. □

Now we will relate $Z(\beta)$ and $Z(\hat{\beta})$. Every braid in $Z(\beta)$ preserves the canonical reduction system of β (see [21]), so it must preserve $R(\beta)$. That is, $Z(\beta) \subset B_{R(\beta)}$. Let $p : B_{R(\beta)} \to B_m$ be the homomorphism which sends α to $\hat{\alpha}$, the tubular braid induced by α and $R(\beta)$. If we take $\alpha \in Z(\beta)$ then $\beta = \alpha^{-1}\beta\alpha$, so $p(\beta) = p(\alpha^{-1}\beta\alpha) = p(\alpha)^{-1}p(\beta)p(\alpha)$. Hence $p(\alpha)$ commutes with $p(\beta) = \hat{\beta}$. Therefore, if we restrict p to $Z(\beta)$ we get $p : Z(\beta) \to Z(\hat{\beta})$.

Unfortunately, neither $p : B_{R(\beta)} \to B_m$ nor its restriction $p : Z(\beta) \to Z(\hat{\beta})$ are surjective, but we shall see that the elements in the image of p in either case can be easily characterised by the permutation they induce. Notice that p induces a bijection $\tilde{p}$ from $R(\beta)$ to $\{P_1, \ldots, P_m\}$, the punctures of D_m. We denote by τ the inverse of $\tilde{p}$.

DEFINITION 5.4. – Let $\eta \in B_m$, and let π_η be the permutation induced by η on the punctures of D_m. We say that π_η is *consistent with* $R(\beta)$ if, for $i = 1, \ldots, m$, $\tau(P_i)$ and $\tau(\pi_\eta(P_i))$ enclose the same number of punctures.

PROPOSITION 5.5. – *An element $\eta \in B_m$ is in the image of $p : B_{R(\beta)} \to B_m$ if and only if π_η is consistent with $R(\beta)$.*

Proof. – If η is in the image of p, let $\alpha \in B_{R(\beta)}$ with $p(\alpha) = \eta$. Then, for every $i = 1, \ldots, m$, $\tau(P_i)$ and $\tau(\pi_\eta(P_i))$ are the top and bottom circles of a tube determined by α. Hence they must enclose the same number of punctures (the number of strands inside the tube).

Conversely, suppose that π_η is consistent with $R(\beta)$. Take $i \in \{1, \ldots, m\}$ and suppose that $\tau(P_i) = C_{j,k}$. Then take the ith strand of η and consider it as a tube, enclosing the trivial braid on m_j strands. Do this for every $i = 1, \ldots, m$. The resulting braid, $\psi(\eta)$, is well defined since π_η is consistent with $R(\beta)$, and it belongs to $B_{R(\beta)}$. Moreover, $p(\psi(\eta)) = \eta$ by construction. □

The homomorphism ψ introduced in this proof will play a prominent rôle in what follows: if $\eta \in B_m$, then $\psi(\eta)$ is the braid in $B_{R(\beta)}$ whose tubular braid equals η, and whose interior braids are all trivial.

All the elements in B_m that shall be considered from now on will have permutations consistent with $R(\beta)$. Hence, by abuse of notation, we will identify $C_{i,k} = \tilde{p}(C_{i,k})$ and $\mathcal{C}_i = \tilde{p}(\mathcal{C}_i)$ if it does not lead to confusion.

We still need to characterise the elements in the image of $p : Z(\beta) \to Z(\hat{\beta})$. We just know that their permutations must be consistent with $R(\beta)$, but this is not sufficient. Recall that the permutation induced by β on the components of $R(\beta)$ has t orbits, $\mathcal{C}_1, \ldots \mathcal{C}_t$. The key observation now is that every element $\alpha \in Z(\beta)$ preserves these orbits setwise, though it could permute them. Therefore, for $i = 1, \ldots, t$, one has $\alpha(\mathcal{C}_i) = \mathcal{C}_j$ for some j. In the same way, for any $\eta \in Z(\hat{\beta})$ one has $\alpha(\mathcal{C}_i) = \mathcal{C}_j$ for some j.

LEMMA 5.6. – *Let $\alpha \in Z(\beta)$. If $\alpha(\mathcal{C}_i) = \mathcal{C}_j$ for some $i, j \in \{1, \ldots, t\}$, then $\beta_{[i]} = \beta_{[j]}$.*

Proof. – Since $\alpha(\mathcal{C}_i) = \mathcal{C}_j$, the two orbits have the same length, which we shall denote r; thus $r = r_i = r_j$. Now β^r is a braid that preserves $C_{i,k}$ and $C_{j,k}$ for every k, and is such that $(\beta^r)_{i,k} = \beta_{[i]}$ and $(\beta^r)_{j,k} = \beta_{[j]}$. Now since α commutes with β, then it also commutes with β^r.

Suppose that α sends $C_{i,1}$ to $C_{j,k}$. Then

$$\beta_{[j]} = (\beta^r)_{j,k} = (\alpha^{-1}\beta^r\alpha)_{j,k} = (\alpha_{i,1})^{-1}(\beta^r)_{i,1}\alpha_{i,1} = (\alpha_{i,1})^{-1}\beta_{[i]}\alpha_{i,1}.$$

Therefore $\beta_{[i]}$ and $\beta_{[j]}$ are conjugate, and since β is in regular form, $\beta_{[i]} = \beta_{[j]}$, as we wanted to prove. □

Lemma 5.6 imposes another condition for a braid in $Z(\hat{\beta})$ to be in $p(Z(\beta))$:

DEFINITION 5.7. – Let $\eta \in Z(\hat{\beta})$. We say that π_η is *consistent with* β if it is consistent with $R(\beta)$ and, furthermore, for every $i, j \in \{1, \ldots, t\}$ such that $\eta(\mathcal{C}_i) = \mathcal{C}_j$, one has $\beta_{[i]} = \beta_{[j]}$.

DEFINITION 5.8. – $Z_0(\hat{\beta})$ is the subgroup of $Z(\hat{\beta})$ consisting of those elements whose permutation is consistent with β.

Then Lemma 5.6 can be restated as follows: If $\alpha \in Z(\beta)$ then $p(\alpha) \in Z_0(\hat{\beta})$. Moreover, we can prove the following:

PROPOSITION 5.9. – *The homomorphism $p : Z(\beta) \longrightarrow Z_0(\hat{\beta})$ is surjective.*

Proof. – Let $\eta \in Z_0(\hat{\beta})$. We shall construct a preimage of η under p in two steps. Since π_η is consistent with β (thus with $R(\beta)$), we can, as a first step, consider the braid $\psi(\eta) \in B_n$. We then have $p(\psi(\eta)) = \eta$; but $\psi(\eta)$ does not necessarily commute with β, since the interior braids of $\psi(\eta)^{-1}\beta\psi(\eta)$ could differ from those of β. Actually, since the interior braids of $\psi(\eta)$ are all trivial, conjugating β by $\psi(\eta)$ just permutes the interior braids of β. More precisely, the braid $\psi(\eta)^{-1}\beta\psi(\eta)$ equals β, except that, for each $i \in \{1, \ldots, t\}$, it may not be the tube C_{i,r_i} which contains the nontrivial interior braid $\beta_{[i]}$, but some other tube from the family $\mathcal{C}_i$. Our aim in the second step is thus to fill the tubes of $\psi(\eta)$ with more suitable interior braids, in order to obtain a braid that commutes with β.

For every $i \in \{1, \ldots, t\}$, we know that $\psi(\eta)$ sends $\mathcal{C}_i$ to some $\mathcal{C}_j$. Let $k_i \in \{1, \ldots, r_i\}$ be such that $\psi(\eta)$ sends C_{i,k_i} to C_{j,r_j}, and consider the braid $\mu(i, k_i)$ defined at the end of Section 5.1. If we conjugate β by $\mu(i, k_i)$ we move $\beta_{[i]}$ from C_{i,r_i} to C_{i,k_i}. If we further conjugate by $\psi(\eta)$, then $\beta_{[i]}$ goes to C_{j,r_j}. But η is consistent with β, so $\beta_{[i]} = \beta_{[j]}$. Hence, the interior braids in $\mathcal{C}_j$ are preserved. We can do this for $i = 1, \ldots, t$, so we obtain that the braid

$$\left(\prod_{i=1}^{t} \mu(i, k_i)\right)\psi(\eta)$$

commutes with β and its tubular braid is η, so it is in $p^{-1}(\eta) \cap Z(\beta)$. This shows the result. □

We can finally bring together all the results in this section to state the following:

THEOREM 5.10. – *Let $\beta \in B_n$ be a non-periodic reducible braid in regular form. Then the sequence*

$$1 \to Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}) \xrightarrow{g} Z(\beta) \xrightarrow{p} Z_0(\hat{\beta}) \to 1$$

is exact.

Proof. – By Proposition 5.3 g is injective, and by Proposition 5.9 p is surjective. It just remains to show that $\mathrm{im}(g) = \ker(p)$.

By construction, every element in the image of g induces a trivial tubular braid, so $\mathrm{im}(g) \subset \ker(p)$. Let then $\alpha \in \ker(p)$, that is, $\hat{\alpha} = 1$. Since $\alpha \in Z(\beta)$, we have $\alpha^{-1}\beta\alpha = \beta$, and since

$\beta_{i,k}=1$ for $k\neq r_i$, we must have $\alpha_{i,k}^{-1}1\alpha_{i,k+1}=1$, so $\alpha_{i,k}=\alpha_{i,k+1}$ for $k=1,\dots,r_i-1$. Hence $\alpha_{i,1}=\alpha_{i,2}=\cdots=\alpha_{i,r_i}$ for every i. Moreover, we have

$$\beta_{[i]}=\beta_{i,r_i}=\alpha_{i,r_i}^{-1}\beta_{i,r_i}\alpha_{i,1}=\alpha_{i,1}^{-1}\beta_{[i]}\alpha_{i,1},$$

so $\alpha_{i,1}\in Z(\beta_{[i]})$. Therefore, $\alpha=g_1(\alpha_{1,1})g_2(\alpha_{2,1})\cdots g_t(\alpha_{t,1})=g(\alpha_{1,1},\alpha_{2,1},\dots,\alpha_{t,1})$. That is, $\ker(p)\subset\operatorname{im}(g)$. □

5.3. Finding a section for p

In this subsection we will prove that the exact sequence of Theorem 5.10 splits. We recall that $\hat\beta$ is obtained from β by collapsing the disks bounded by outermost curves in the canonical reduction system of β to single punctures. In particular, the canonical reduction system of $\hat\beta$ must be empty. Hence, $\hat\beta$ is either periodic or pseudo-Anosov. We will distinguish these two cases, to define a multiplicative section for p, but first we will show an easy particular case. Recall that a braid is pure if it induces the trivial permutation of its base points.

PROPOSITION 5.11. – *If $\hat\beta$ is pure, there is a homomorphism $h:Z_0(\hat\beta)\to Z(\beta)$ such that $p\circ h=1$.*

Proof. – We shall prove that in this case, the homomorphism ψ constructed in the proof of Proposition 5.5 is such a section. Let $\eta\in Z_0(\hat\beta)$. Since $\hat\beta$ is pure, $\mathcal{C}_i=\{C_{i,1}\}$ for all i. Hence, if η sends $\mathcal{C}_i$ to $\mathcal{C}_j$ then it sends the tube $C_{i,1}$ (containing $\beta_{[i]}$) to the tube $C_{j,1}$ (containing $\beta_{[j]}=\beta_{[i]}$, since β is in regular form). Therefore, filling every tube in η with the trivial braid, that is, defining $h(\eta)=\psi(\eta)$, yields indeed an element of $Z(\beta)$. □

Next we study the general case, depending whether $\hat\beta$ is periodic or pseudo-Anosov.

PROPOSITION 5.12. – *If $\hat\beta$ is periodic, there is a homomorphism $h:Z_0(\hat\beta)\to Z(\beta)$ such that $p\circ h=1$.*

Proof. – Recall that we are studying β up to conjugacy. This implies that we can also study $\hat\beta$ up to conjugacy since, for every $\xi\in B_m$, if we conjugate β by $\psi(\xi)$ we are conjugating $\hat\beta$ by ξ. Moreover, after conjugating by $\psi(\xi)$, β continues to be in regular form (up to renaming the circles in $R(\beta)$). Therefore we can suppose, up to conjugacy, that $\hat\beta$ is a rigid rotation of the disc, that is, a power of $\delta_{(m)}$ or $\gamma_{(m)}$.

Suppose first that $\hat\beta=\delta_{(m)}^k$ for some k. We can suppose that k is not a multiple of m, since in that case $\hat\beta$ would be a power of $\Delta^2_{(m)}$, thus it would be pure, and this case has already been studied in Proposition 5.11. Recall the analysis of periodic braids in Section 3: the base points $Q_1,\dots,Q_m$ of $\hat\beta$ will be evenly distributed along a circle of radius 1 around 0. Let $d=\gcd(m,k)<m$ and $r=m/d$. Then $\hat\beta$ sends Q_i to Q_{i+k}, and there are d orbits $\mathcal{C}_1,\dots,\mathcal{C}_d$ of length r. The orbit $\mathcal{C}_i$ will contain the points Q_u where $u\equiv i\pmod d$. Since we can choose which tubes of β contain the interior braids, we will suppose that these are the tubes starting at $Q_{m-d+1},Q_{m-d+2},\dots,Q_m$, that is, the last d points of D_m.

We will consider now some line segments in D which separate the points $Q_1,\dots,Q_m$ into r sets of d points. Let L be the line segment joining the origin with the border of D, passing between the points Q_{m-d} and Q_{m-d+1}, and let L' be the segment passing between Q_m and Q_1. Notice that L and L' determine a sector which contains the points $Q_{m-d+1},\dots,Q_m$, corresponding to the tubes of β with nontrivial interior braids. Let $\phi:\mathbb{C}\to\mathbb{C}$ be the rotation around the origin by an angle of $2\pi k/m$ (the angle induced by $\hat\beta$), and denote $L_i=\phi^i(L)$. Since $\gcd(m,k)=d$, the segments $L_0,\dots,L_{r-1}$ divide D into $m/d=r$ sectors, each one of angle

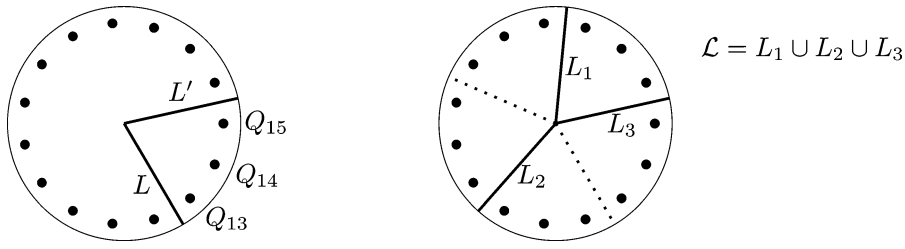

Fig. 8. The segments L, L', and the union of segments $\mathcal{L}$, for $\hat{\beta} = \delta^6 \in B_{15}$.

$2\pi/r$ and containing the points $Q_{id+1}, \ldots, Q_{id+d}$ for some i. Take the smallest integer $e > 0$ such that $\phi^e(L) = L'$. Then one has $L_0 = L$ and $L_e = L'$. We are interested in the union of segments $\mathcal{L} = L_1 \cup L_2 \cup \cdots \cup L_e$ (see Fig. 8 for an example).

Let then $\eta \in Z_0(\hat{\beta})$. In order to define $h(\eta)$, it suffices to define its interior braids. This is done as follows: recall that, since η commutes with $\hat{\beta}$, it can be isotoped to a symmetric braid (with respect to the rotation ϕ), so we take a symmetric representative of η. For every base point Q_i of $\hat{\beta}$ (corresponding to a circle $C_{j,u}$), consider the strand of η starting at Q_i (the ith strand of η). Then we define the interior braid $h(\eta)_{j,u} = (\beta_{[j]})^{L(\eta,i)}$, where $L(\eta, i) \in \mathbb{Z}$ is the algebraic number of times that the ith strand of η crosses $\mathcal{L}$. This is well defined by Theorem 3.2 (if you take two distinct representatives of η as a symmetric braid, they are isotopic through symmetric braids, so the strands never touch the origin and the intersection number $L(\eta, i)$ is preserved).

In other words, we define $h(\eta)$ as follows: we start with trivial interior braids, and we follow the movement of the strands of η. Each time a strand crosses a segment of $\mathcal{L}$ in the positive sense, we multiply its interior braid by $\beta_{[j]}$ (where j is the index of the orbit $\mathcal{C}_j$ of that strand). And every time a strand crosses $\mathcal{L}$ in the negative sense, we multiply its interior braid by $\beta_{[j]}^{-1}$.

We have thus defined a map $h : Z_0(\hat{\beta}) \to B_{R(\beta)}$. To show that h is a homomorphism, it suffices to see that the interior braids of $\eta\xi$ are the product of those of η and ξ, for $\eta, \xi \in Z_0(\hat{\beta})$. Suppose that the ith strand of η goes from Q_i (corresponding to $C_{j,u}$) to $Q_{i'}$ (corresponding to $C_{j',u'}$). Hence η sends $\mathcal{C}_j$ to $\mathcal{C}_{j'}$, and since $\eta \in Z_0(\hat{\beta})$, it follows that $\beta_{[j]} = \beta_{[j']}$. One also has, by definition, $L(\eta\xi, i) = L(\eta, i) + L(\xi, i')$. Therefore $(\eta\xi)_{j,u} = (\beta_{[j]})^{L(\eta\xi,i)} = (\beta_{[j]})^{L(\eta,i)}(\beta_{[j]})^{L(\xi,i')} = \eta_{j,u}\xi_{j',u'}$, so h is a homomorphism.

We must finally show that, with this definition, $h(\eta) \in Z(\beta)$, for every $\eta \in Z_0(\hat{\beta})$. We will define first some special braids. For every $i, j \in \{1, \ldots, d\}$ such that $i < j$ and $\beta_{[i]} = \beta_{[j]}$, define the symmetric braid $S_{i,j} = S_{j,i} = \theta_r^*(\sigma_i \cdots \sigma_{j-2}\sigma_{j-1}\sigma_{j-2} \cdots \sigma_i)$ (see Fig. 3 in Section 3 to recall the definition of θ_r^*, and Fig. 9 here for an example). The braid $S_{i,j}$ commutes with $\hat{\beta}$ (since it is symmetric), and it permutes the orbits $\mathcal{C}_i$ and $\mathcal{C}_j$, preserving the others. Hence $S_{i,j} \in Z_0(\hat{\beta})$.

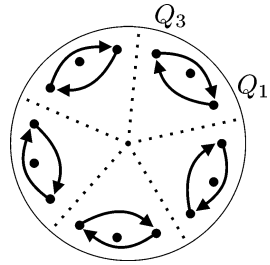

Fig. 9. The braid $S_{1,3}$, for $\hat{\beta} = \delta^6 \in B_{15}$ (assuming that $\beta_{[1]} = \beta_{[3]}$).

Moreover, its strands do not cross $\mathcal{L}$, so by definition of h one has $h(S_{i,j}) = \psi(S_{i,j})$ (the interior braids are trivial).

But $h(S_{i,j})$ commutes with β, since the only tubes it permutes are those of the orbits $\mathcal{C}_i$ and $\mathcal{C}_j$; among these tubes, the only two with non-trivial interior braids are exchanged, and their corresponding interior braids are equal ($\beta_{[i]} = \beta_{[j]}$). Hence the interior braids of β are preserved by $\psi(S_{i,j}) = h(S_{i,j})$, so $h(S_{i,j}) \in Z(\beta)$.

Take then an arbitrary $\eta \in Z_0(\hat{\beta})$. We must show that $h(\eta) \in Z(\beta)$. Suppose that η sends $\mathcal{C}_i$ to $\mathcal{C}_j$ for some i, j. Then $\beta_{[i]} = \beta_{[j]}$, so $S_{i,j}$ is defined, and the braid $\eta S_{i,j}$ preserves the orbit $\mathcal{C}_i$. We can continue this way, until we obtain a braid $\eta S_{i_1,j_1} \cdots S_{i_k,j_k}$ that commutes with $\hat{\beta}$ and preserves every orbit $\mathcal{C}_i$, for $i = 1, \ldots, d$. Since $h(S_{i,j}) \in Z(\beta)$ for every i, j, and h is a homomorphism, in order to show that $h(\eta) \in Z(\beta)$ it suffices to show that $h(\eta S_{i_1,j_1} \cdots S_{i_k,j_k}) \in Z(\beta)$. Therefore, we can suppose that η preserves every orbit $\mathcal{C}_i$.

Denote $\alpha = h(\eta)$. We need to show that the interior braids of $\alpha^{-1}\beta\alpha$ coincide with those of β. Since η preserves all orbits, we will consider just the tubes of $\mathcal{C}_1$, the other ones being analogous. Suppose that α sends the circle $C_{1,u}$ to $C_{1,r}$. Then it must send $C_{1,v}$ to $C_{1,v-u}$ for every v (the indices are taken modulo r).

We will identify the points $Q_1, \ldots, Q_m$ with their corresponding circles $C_{i,v}$. For every $v = 1, \ldots, r$, let b_v be the strand of η starting at $C_{1,v}$. Since η is symmetric, we have $\phi(b_v) = b_{v+1}$. Suppose that b_v crosses t times the segment L_i, where $i \in \{0, \ldots, r-1\}$. Then b_{v+1} will cross t times the segment $\phi(L_i) = L_{i+1}$. Therefore, if b_v crosses l times $\mathcal{L}$, and if it crosses l_0 times L_0 and l_e times L_e, then b_{v+1} crosses $l - l_e + l_0$ times $\mathcal{L}$.

If $v \neq r$ and $v \neq u$, then b_v neither starts nor ends at $C_{1,r}$. Then it crosses L_0 and L_e the same number of times. Hence, b_v and b_{v+1} cross $\mathcal{L}$ the same number of times, say l. Therefore, if $v \neq r, u$, one has

$$(\alpha^{-1}\beta\alpha)_{1,v-u} = (\alpha_{1,v})^{-1}\beta_{1,v}\alpha_{1,v+1} = \beta_{[1]}^{-l}1\beta_{[1]}^{l} = 1 = \beta_{1,v-u}.$$

If $u = v = r$, then b_v starts at ends at $C_{1,r}$. Hence, as above, it crosses L_0 and L_e the same number of times, so $b_v = b_r$ and $b_{v+1} = b_1$ cross $\mathcal{L}$ the same number of times, say l. We then have $(\alpha^{-1}\beta\alpha)_{1,v-u} = (\alpha^{-1}\beta\alpha)_{1,r} = (\alpha_{1,r})^{-1}\beta_{1,r}\alpha_{1,1} = \beta_{[1]}^{-l}\beta_{[1]}\beta_{[1]}^{l} = \beta_{[1]} = \beta_{1,r} = \beta_{1,v-u}$. Hence, if $u = r$, we have already seen all the possible cases. We will then suppose that $u \neq r$.

If $v = r$, then b_v starts (but does not end) at $C_{1,r}$. Hence, it crosses L_e one more time (in the positive sense) than it crosses L_0. Therefore, if $b_v = b_r$ crosses l times $\mathcal{L}$, then $b_{v+1} = b_1$ crosses it $l - 1$ times. One has:

$$(\alpha^{-1}\beta\alpha)_{1,v-u} = (\alpha^{-1}\beta\alpha)_{1,r-u} = (\alpha_{1,r})^{-1}\beta_{1,r}\alpha_{1,1} = \beta_{[1]}^{-l}\beta_{[1]}\beta_{[1]}^{l-1} = 1 = \beta_{1,r-u} = \beta_{1,v-u}.$$

Finally, if $v = u$ then b_v ends (but does not start) at $C_{1,r}$. In this case, it crosses L_e one less time (in the positive sense) than it crosses L_0. Hence, if $b_v = b_u$ crosses l times $\mathcal{L}$, then $b_{v+1} = b_{u+1}$ crosses it $l + 1$ times. One then has:

$$(\alpha^{-1}\beta\alpha)_{1,v-u} = (\alpha^{-1}\beta\alpha)_{1,r} = (\alpha_{1,u})^{-1}\beta_{1,u}\alpha_{1,u+1} = \beta_{[1]}^{-l}1\beta_{[1]}^{l+1} = \beta_{[1]} = \beta_{1,r} = \beta_{1,v-u}.$$

Therefore, in every possible case we have $(\alpha^{-1}\beta\alpha)_{1,v-u} = \beta_{1,v-u}$, for every v. This means that the interior braids of $(\alpha^{-1}\beta\alpha)$ and of β coincide, that is, $\alpha = h(\eta)$ commutes with β, as we wanted to show.

This completes the proof of Proposition 5.12 in the case $\hat{\beta} = \delta_{(m)}^{k}$, and it only remains to deal with the case when $\hat{\beta} = \gamma_{(m)}^{k}$. As above, we can suppose that k is not a multiple of $m - 1$, since

in that case $\hat{\beta}$ would be pure, and this case has already been treated in Proposition 5.11. Hence, the only fixed point in the permutation induced by $\hat{\beta}$ is the origin. Therefore, every η commuting with $\hat{\beta}$ must fix the origin. This means that, for every $\eta \in Z_0(\hat{\beta})$, we can fill its central tube with the trivial braid, and the other tubes in the same way as above (defining $\mathcal{L}$, and counting the number of times each strand crosses $\mathcal{L}$). This defines a homomorphism $h : Z_0(\hat{\beta}) \to Z(\beta)$ which is a section of p. The proof is the same as above. □

It remains to study the case when $\hat{\beta}$ is pseudo-Anosov.

PROPOSITION 5.13. – *If $\hat{\beta}$ is pseudo-Anosov, then there is a homomorphism*

$$h : Z_0(\hat{\beta}) \to Z(\beta)$$

such that $p \circ h = 1$.

Proof. – In this case, we know that $Z(\hat{\beta})$ is a free abelian group of rank 2, generated by a pseudo-Anosov and a periodic braid. Hence, $Z_0(\hat{\beta})$ is an abelian group of rank one or two. Notice that $\Delta^2_{(m)} \in Z_0(\hat{\beta})$, because this braid commutes with $\hat{\beta}$ and because π_{Δ^2} is trivial, and thus consistent with β. Hence $Z_0(\hat{\beta})$ contains at least one periodic element. On the other hand, $\hat{\beta}$ belongs itself to $Z_0(\hat{\beta})$, since $\pi_{\hat{\beta}}$ is clearly consistent with β. Hence in $Z_0(\hat{\beta})$ there are also pseudo-Anosov braids. Since all powers of a periodic braid are periodic, and all powers of a pseudo-Anosov braid are pseudo-Anosov, it follows that $Z_0(\hat{\beta})$ has in fact rank two. More precisely, $Z_0(\hat{\beta}) = \langle\eta\rangle \times \langle\rho\rangle$, where η is pseudo-Anosov and ρ is periodic. In particular, we have $\hat{\beta} \in \langle\eta\rangle \times \langle\rho\rangle$, and the three braids $\hat{\beta}$, η and ρ are mutually commuting.

Our aim is to define two commuting braids $h(\rho)$ and $h(\eta)$ in $Z(\beta)$ which are preimages of ρ respectively η under p. The definition of $h(\rho)$ is very simple: we take an arbitrary preimage of ρ under p – this is possible since p is surjective by Proposition 5.9. It remains to construct $h(\eta)$.

LEMMA 5.14. – *Suppose $\alpha \in B_{R(\beta)}$, that is, the braid α preserves the set of outermost curves in the canonical reduction system of β. Suppose also that $\mu, \nu \in Z(\hat{\alpha})$. Suppose that $\iota_\mu \in B_{R(\beta)}$ is a braid with trivial tubes (i.e. $\hat{\iota}_\mu = 1$) such that $\psi(\mu) \cdot \iota_\mu \in Z(\alpha)$. Finally, suppose that μ and ν induce the same permutation. Then we have as well that $\psi(\nu) \cdot \iota_\mu \in Z(\alpha)$.*

In other words, if two tubular braids commute with $\hat{\alpha}$, if they induce the same permutation, and if some "filling" of one of them commutes even with α, then the same filling of the other will also commute with α.

Proof of Lemma 5.14. – Conjugating α by $\psi(\nu) \cdot \iota_\mu \in Z(\alpha)$ yields a certain braid α'; we have to check that $\alpha' = \alpha$. Firstly, we have an equality of tubular braids $\hat{\alpha}' = \hat{\alpha}$, because ν, the tubular braid of $\psi(\nu) \cdot \iota_\mu$, commutes with $\hat{\alpha}$. Moreover, since μ and ν induce the same permutations, we have for $i = 1, \ldots, m$ that the ith tube of α' contains the same braid as the ith tube of $(\psi(\mu) \cdot \iota_\mu)^{-1} \cdot \alpha \cdot (\psi(\mu) \cdot \iota_\mu)$. Since $\psi(\mu) \cdot \iota_\mu$ commutes with α, this is in turn the same as the ith tube of α. In summary, α and α' have the same tubular braids, and corresponding tubes contain the same interior braids, which implies that $\alpha = \alpha'$. □

Next we have to think in detail about the orbit structure of $\hat{\beta}$. Let us choose arbitrarily a puncture P of the disk D_m (on which $\hat{\beta}$ acts), and let $O(\hat{\beta}, \rho)$ be the orbit of that puncture under the action of the subgroup $\langle\hat{\beta}\rangle \times \langle\rho\rangle$ of $Z_0(\hat{\beta})$. Let $O(\hat{\beta}, \rho, \eta)$ be the orbit of P under the action of the group $\langle\rho\rangle \times \langle\eta\rangle$ (note that this group is also isomorphic to $\mathbb{Z}^2$, and contains $\hat{\beta}$).

We are going to suppose without loss of generality that $O(\hat{\beta}, \rho, \eta)$ contains *all* punctures of D_m, and we shall specify how the tubes of η corresponding to this orbit shall be filled – indeed, if there are other orbits, then these can be treated in same way, independently.

Special case: Let us start by considering the simpler special case that $O(\hat{\beta},\rho,\eta)=O(\hat{\beta},\rho)$, i.e. that the action of η preserves the $(\hat{\beta},\rho)$-orbit. In this case we have

LEMMA 5.15. – *There exist integers k and l such that η and $\hat{\beta}^k\cdot\rho^l$ induce the same permutations on $O(\hat{\beta},\rho)$.*

Proof of Lemma 5.15. – One can choose k and l such that $\hat{\beta}^k\rho^l(P)=\eta(P)$, simply because $\eta(P)$ is in the orbit of P under the action of $\hat{\beta}$ and ρ. Now if P' is another point in the orbit, then $P'=\hat{\beta}^\kappa\rho^\lambda(P)$ for some $\kappa,\lambda\in\mathbb{Z}$. Since $\hat{\beta},\rho$, and η are mutually commuting, we get $\hat{\beta}^k\rho^l(P')=\hat{\beta}^k\rho^l(\hat{\beta}^\kappa\rho^\lambda(P))=\hat{\beta}^\kappa\rho^\lambda(\hat{\beta}^k\rho^l(P))=\hat{\beta}^\kappa\rho^\lambda(\eta(P))=\eta(\hat{\beta}^\kappa\rho^\lambda(P))=\eta(P')$. □

We already know a nice preimage of $\hat{\beta}^k\cdot\rho^l$ under p: the braid $\beta^k\cdot h(\rho)^l$ belongs to $Z(\beta)$, because both β and $h(\rho)$ do. This braid can be reexpressed as $\psi(\hat{\beta}^k\rho^l)\cdot\iota$, where ι is some braid in $B_{R(\beta)}$ with $\hat{\iota}=1$. (That is, we define ι to consist of the interior braids of the tubes of $\beta^k\cdot h(\rho)^l$).

Now we define our filling of η by $h(\eta):=\psi(\eta)\cdot\iota$. By Lemma 5.14 we have that indeed $\psi(\eta)\cdot\iota\in Z(\beta)$. In order to see that $\psi(\eta)\cdot\iota$ lies also in the centralizer of $h(\rho)$ one can use a very similar argument. Explicitly, both η and $\hat{\beta}^k\rho^l$ lie in the centralizer of ρ, and they induce the same permutation of the punctures. Moreover, $\psi(\hat{\beta}^k\rho^l)\cdot\iota=\beta^k h(\rho)^l\in Z(h(\rho))$. By Lemma 5.14 we conclude again that $\psi(\eta)\cdot\iota\in Z(h(\rho))$, also.

General case: In the case where η does not preserve $O(\hat{\beta},\rho)$, the strategy is to work not with β itself but with a certain conjugate of β. The details are as follows. We have a finite number of disjoint $(\hat{\beta},\rho)$-orbits in $O(\hat{\beta},\rho,\eta)$, and since η commutes with $\hat{\beta}$ and ρ, the action of η permutes these orbits cyclically:

$$O(\hat{\beta},\rho)\xrightarrow{\eta\text{-action}}\eta(O(\hat{\beta},\rho))\xrightarrow{\eta\text{-action}}\cdots\xrightarrow{\eta\text{-action}}\eta^s(O(\hat{\beta},\rho))=O(\hat{\beta},\rho).$$

Let us denote $\hat{\beta}_*,\rho_*$ and η_*^s the braids which are obtained from $\hat{\beta},\rho$ and η^s by retaining only the strands corresponding to $O(\hat{\beta},\rho)$, and forgetting the strands corresponding to all other $(\hat{\beta},\rho)$-orbits. Similarly, let β_* be the corresponding restriction of β. Our first aim is to fill the tubes of ρ_* and η_*^s so as to obtain commuting braids in $Z(\beta_*)$. This can be done as in the "special case": for ρ_* we choose any filling in $Z(\beta_*)$, and for η_*^s there exists a braid ι_* with trivial tubes such that $\psi(\eta_*^s)\cdot\iota_*$ commutes with β_* and the filling of ρ_*.

We have succeeded in finding a filling of certain tubes of η^s, but not yet of η itself. Also, we have so far only filled the tubes of ρ which correspond to $O(\hat{\beta},\rho)$, but not yet those in the η-translates of this orbit. We first notice that the η-action sends $\hat{\beta}$-orbits to $\hat{\beta}$-orbits, and that in each $\hat{\beta}$-orbit there is exactly one tube whose preimage in β contains a nontrivial braid (the same for all $\hat{\beta}$-orbits), and all other tubes are filled with a trivial braid. Thus, up to cyclically changing the numbering of the orbits of each tube of $\hat{\beta}$, we may assume that the η-action sends each tube of $\hat{\beta}$ in $O(\hat{\beta},\rho)$ to a tube of $\hat{\beta}$ in $\eta(O(\hat{\beta},\rho))$ which is filled with the nontrivial braid if and only if the tube of $O(\hat{\beta},\rho)$ is. Similarly, for $i=1,\dots,s-1$ we may assume that η^i sends each $\hat{\beta}$-tube in $O(\hat{\beta},\rho)$ to a $\hat{\beta}$-tube in $\eta^i(O(\hat{\beta},\rho))$ which has the same filling in β.

Now we can use the same property as a construction recipe for $h(\rho)$: a tube of ρ in $\eta^i(O(\hat{\beta},\rho))$ (where $i=1,\dots,s$) is filled in the same way as its preimage under η^i. With this definition, $h(\rho)$ commutes with β. Finally we are ready to define $h(\eta)$: we take the braid $\psi(\eta)$, but modify the braids in the tubes that terminate at positions corresponding to $O(\hat{\beta},\rho)$ by multiplying them on the right by ι_*. In other words, the braid $h(\eta)$ is obtained from η as follows: we fill those tubes of η which connect points in $\eta^i(O(\hat{\beta},\rho))$ to points in $\eta^{i+1}(O(\hat{\beta},\rho))$ (with $i=0,\dots,s-2$) with the trivial braid, and we fill the tubes that start in $\eta^{s-1}(O(\hat{\beta},\rho))$ and terminate in $O(\hat{\beta},\rho)$ with

the interior braids of ι_*. By construction, this braid $h(\eta)$ commutes with both β and $h(\rho)$. This concludes the proof of Proposition 5.13. □

COROLLARY 5.16. – *Suppose that β is a non-periodic reducible braid in regular form. Then the exact sequence*

$$1 \longrightarrow Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}) \xrightarrow{g} Z(\beta) \xrightarrow{p} Z_0(\hat{\beta}) \longrightarrow 1$$

splits. That is, $Z(\beta) \cong (Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]})) \rtimes Z_0(\hat{\beta})$.

Proof. – Since $\hat{\beta}$ cannot be reducible, the result is a direct consequence of Propositions 5.11, 5.12 and 5.13. □

5.4. Structure of $Z_0(\hat{\beta})$

The proof of Theorem 1.1 is now completed by the following result.

PROPOSITION 5.17. – *Suppose that β is a non-periodic reducible braid, and that its tubular braid $\hat{\beta}$ has m strands. Then $Z_0(\hat{\beta})$ is isomorphic either to $\mathbb{Z}^2$ or to a mixed braid group on k strands, where $k \leqslant m$.*

Proof. – As usual, there are three subcases, depending whether $\hat{\beta}$ is trivial, periodic or pseudo-Anosov. Recall that we are assuming that β is in regular form.

Suppose first that $\hat{\beta} = 1$. In this case, $Z(\hat{\beta}) = B_m$. Hence $Z_0(\hat{\beta})$ contains any braid whose permutation is consistent with β. Denote by $\mathcal{P}$ the following partition of $\{P_1, \ldots, P_m\} = \{C_{1,1}, \ldots, C_{m,1}\}$: we say that P_i and P_j belong to the same coset of $\mathcal{P}$ if and only if $\beta_{[i]} = \beta_{[j]}$. By definition, a braid's permutation is consistent with β if and only if it preserves $\mathcal{P}$. Therefore, $Z_0(\hat{\beta}) = B_{\mathcal{P}}$, and we are done. (In this case, we have $k = m$.)

If $\hat{\beta}$ is pseudo-Anosov, it is shown in proposition 5.13 that $Z_0(\hat{\beta}) \simeq \mathbb{Z}^2$, so this case is already known.

Finally, suppose that $\hat{\beta}$ is periodic. If it is a power of Δ^2, then its centralizer is the whole B_m, and its corresponding permutation is trivial, so this case is equivalent to the first one.

If $\hat{\beta}$ is periodic but not a power of Δ^2, then we know by Theorems 3.2 and 3.4 that $Z(\hat{\beta}) \simeq B_d(D_*)$, for some $d \geqslant 1$, where D^* is the once punctured disk. But every base point Q_i in D^* corresponds to an orbit $\mathcal{C}_i$ of $\hat{\beta}$ (see Fig. 2 in Section 3), so we can define the following partition $\mathcal{P}'$ of $\{Q_1, \ldots, Q_d\}$: Q_i and Q_j belong to the same coset if and only if $\beta_{[i]} = \beta_{[j]}$. This partition lifts by θ^{-1} to a partition of $\{P_1, \ldots, P_m\}$, in such a way that any braid in $B_d(D_*)$ preserves $\mathcal{P}'$ if and only if its corresponding permutation in $Z(\hat{\beta})$ is consistent with β. Therefore, $Z_0(\hat{\beta}) \simeq B_{\mathcal{P}'}(D^*)$. Now it suffices to consider the central puncture of D^* as another base point, Q_{d+1}, and to notice that $B_{\mathcal{P}'}(D^*) \cong B_{\mathcal{P}}$, where $\mathcal{P} = \mathcal{P}' \cup \{\{Q_{d+1}\}\}$. To summarize, in this case we have $Z_0(\hat{\beta}) \cong B_{\mathcal{P}'}(D^*) \cong B_{\mathcal{P}}$, and the partition $\mathcal{P}$ has $k = d + 1$ cosets. Since d must be a proper divisor of m, we get that $k = d + 1 < m$, and the result follows. □

In particular, $Z_0(\hat{\beta})$ is isomorphic either to $\mathbb{Z}^2$ or to a mixed braid group. Theorem 1.1 is thus proven.

6. An upper bound for the number of generators

Once decomposed $Z(\beta)$, if β is reducible, as a semi-direct product of $(Z(\beta_{[1]}) \times \cdots \times Z(\beta_{[t]}))$ and $Z_0(\hat{\beta}) \subset Z(\hat{\beta})$, we will define a small set of generators for $Z(\beta)$. We will proceed by

induction on the number of strings, but we need to define first a generating set for $Z_0(\hat{\beta})$. We do it as follows:

PROPOSITION 6.1. – *Let $\beta \in B_n$ be a non-periodic reducible braid, and let $\hat{\beta} \in B_m$ be its corresponding tubular braid. Then $Z_0(\hat{\beta})$ can be generated by at most $\frac{m(m-1)}{2}$ elements.*

Proof. – If $m = 2$ then $Z_0(\hat{\beta})$ is cyclic, so let us assume that $m \geqslant 3$. We know by Section 5.4 that $Z_0(\hat{\beta})$ is either isomorphic to $\mathbb{Z}^2$ or to a mixed braid group. The case $\mathbb{Z}^2$ satisfies our result, so we will assume that $Z_0(\hat{\beta})$ is isomorphic to a mixed braid group on k strings.

Mixed braid groups have been studied in [27], where a presentation in terms of generators and relations is given. Since we are mainly interested in the generators, we will extract from those in [27] a small generating set: Let $\mathcal{P}$ be a partition of the set $\{1, \ldots, k\}$, having d cosets of length m_i (for $i = 1, \ldots, d$). A generating set for $B_{\mathcal{P}}$ is given by the following:

1. For $i = 1, \ldots, d$, a generating set for B_{m_i} (if $m_i > 1$).
2. A generating set for the pure braid group P_d.

It is clear that the first kind of generators corresponds to the movements of the points inside a coset, while the second one corresponds to the movement of the points of a coset with respect to those of the others. For instance, if $k = 6$ and $\mathcal{P} = \{\{1\}, \{2, 3\}, \{4, 5, 6\}\}$, then one possible generating set would be:

$$\{\sigma_2\} \cup \{\sigma_4, \sigma_5\} \cup \{\sigma_1^2, \sigma_1\sigma_2\sigma_3^2\sigma_2^{-1}\sigma_1^{-1}, \sigma_3^2\}.$$

In order to minimise these generators we recall that B_2 is cyclic and, if $m > 2$, then B_m can be generated by two elements. Hence, if we denote $e_i = m_i - 1$ if $m_i < 3$ and $e_i = 2$ otherwise, then e_i is a minimal number of generators for B_{m_i}. On the other hand, a minimal number of generators for P_d is $\frac{d(d-1)}{2}$. Therefore, the minimal number of generators for $B_{\mathcal{P}}$ is:

$$\begin{aligned} g_{\mathcal{P}} &= \left(\sum_{i=1}^{d} e_i\right) + \frac{d(d-1)}{2} \leqslant \left(\sum_{i=1}^{d} (m_i - 1)\right) + \frac{d(d-1)}{2} \\ &= k - d + \frac{d(d-1)}{2} = k + \frac{d(d-3)}{2} \leqslant k + \frac{k(k-3)}{2} = \frac{k(k-1)}{2}. \end{aligned}$$

Notice that if $\mathcal{P} = \{\{1\}, \{2\}, \ldots, \{k\}\}$ (so $d = k$), then $g_{\mathcal{P}} = \frac{k(k-1)}{2}$, and this is the worst possibility by the above formula.

Finally we recall from Proposition 5.17 that $k \leqslant m$, so that $g_{\mathcal{P}} \leqslant \frac{m(m-1)}{2}$. □

The first generating set G' of $Z(\beta)$ that we will present is the following: if β is periodic or pseudo-Anosov, we have already defined in Sections 3 and 4 a minimal generating set of $Z(\beta)$, having one or two elements. So suppose that β is reducible. Then, by induction on the number of strings, and by proposition 6.1, we can suppose that we have defined $G_1, \ldots, G_t$ and G_0, generating sets for $Z(\beta_{[1]}), \ldots, Z(\beta_{[t]})$ and $Z_0(\hat{\beta})$ respectively (if some $\beta_{[i]}$ has one string, then $G_i = \emptyset$). Then we define $G' = g_1(G_1) \cup \cdots \cup g_t(G_t) \cup h(G_0)$, which is clearly a generating set for $Z(\beta)$.

Proof of Theorem 1.3. – Denote $p(n)$ the upper bound proposed in Theorem 1.3, that is, $p(n) = \frac{k(k+1)}{2}$ if $n = 2k$ or $p(n) = \frac{k(k+3)}{2}$ if $n = 2k + 1$. We will show that the generating set G' defined above has at most $p(n)$ elements. The case $n = 2$ is trivial, so we can suppose that $n > 2$ and that the result is true for any smaller number of strings. We can also assume that β is non-periodic and reducible.

The strategy now is to successively replace β by different braids, in such a way that during each replacement step the number of generators of its centralizer, as given by the above construction, increases.

The first modification of β will be to replace the tubular braid $\hat{\beta}$ by the trivial braid. At the same time, we shall modify the interior braids, with the aim of rendering them pairwise non-conjugate. More precisely, we notice that, for any braid α with at least two strings, the number of generators of $Z(\alpha)$ and $Z(\Delta^{2p}\alpha)$ is the same, while $\Delta^{2p}\alpha$ and $\Delta^{2q}\alpha$ are conjugate if and only if $p=q$. Thus after multiplying each interior braid $\beta_{[i]}$ by a suitable power of twists $\Delta^2_{(m_i)}$, we can assume that all the interior braids with at least two strings are pairwise non-conjugate, so that $t=m$. As seen in the proof of Proposition 6.1, this first replacement has increased (or left unchanged) the number of generators of G_0, according to our construction.

Suppose, without loss of generality, that $m_1=m_2=\cdots=m_d=1$, that $m_i=2s_i$ for $i=d+1,\ldots,d+u$, and that $m_i=2s_i+1$, for $i=d+u+1,\ldots,d+u+v$, where $d+u+v=m$. Hence u is the number of interior braids with an even number of strings, and v is the number of interior braids with an odd (but greater than one) number of strings. If $d\geqslant 2$, then we shall make further modifications to the braid β, with the aim of lowering d. More precisely, if $d\leqslant 2$, then we can decrease d by multiplying β by σ_1^p for some p, where p is chosen in such a way that no other interior braid of β equals σ_1^p. This replacement increases u by one, and decreases d by two. Thus the number of generators in G_0 decreases by one (if $d=2$) or increases (if $d>2$). But we would have a new interior braid, σ_1^p, yielding one new generator. Hence, the total number of elements in $|G'|$ will not decrease. In other words, without decreasing the number of elements of $|G'|$ we can replace β by a braid with $d\leqslant 1$.

Denote $a=s_{d+1}+\cdots+s_{d+u}$, $b=s_{d+u+1}+\cdots+s_m$ and $S=a+b$. Then one has $n=d+2S+v$. By induction on the number of strings, we have the following bound on the number of elements in G':

$$\begin{aligned}
|G'| &\leqslant \sum_{i=d+1}^{m} p(m_i)+\frac{m(m-1)}{2}\\
&= \sum_{i=d+1}^{d+u}\frac{s_i(s_i+1)}{2}+\sum_{i=d+u+1}^{m}\frac{s_i(s_i+3)}{2}+\binom{m}{2}\\
&= \sum_{i=d+1}^{m}\binom{s_i+1}{2}+\sum_{i=d+u+1}^{m}s_i+\binom{m}{2}\\
&= \sum_{i=d+1}^{m}\binom{s_i+1}{2}+b+\binom{m}{2}
\end{aligned}$$

where $s_i\geqslant 1$ for $i=d+1,\ldots,m$.

Given two positive integers x and y, one has:

$$\binom{x+1}{2}+\binom{y+1}{2}=\binom{x+y+1}{2}-xy.$$

This yields:

$$|G'|\leqslant\binom{S+1}{2}-\Bigg(\sum_{d+1\leqslant i<j\leqslant m}s_is_j\Bigg)+b+\binom{m}{2}.$$

Now we distinguish two cases. If $d=0$, then $m=u+v$ and $n=2S+v$. Also,

$$|G'| \leqslant \binom{S+1}{2} - \Bigg(\sum_{1\leqslant i<j\leqslant m} s_i s_j\Bigg) + b + \binom{m}{2}$$
$$\leqslant \binom{S+1}{2} - \binom{m}{2} + b + \binom{m}{2} = \frac{S(S+1)}{2} + b.$$

If $v=0$ one has $b=0$, so $S=a$ and $|G'| \leqslant \frac{S(S+1)}{2} = \frac{a(a+1)}{2}$; but also $n=2k=2a$, so $p(n)=\frac{a(a+1)}{2}$ and we are done.

If $v=1$ then $n=2S+1$, hence $k=S$ and $p(n)=\frac{S(S+3)}{2}$. But in this case

$$|G'| \leqslant \frac{S(S+1)}{2} + b \leqslant \frac{S(S+1)}{2} + S = \frac{S(S+3)}{2} = p(n).$$

If $v \geqslant 2$, since $n=2S+v$ one has $k \geqslant S+1$. Then

$$|G'| \leqslant \frac{S(S+1)}{2} + b < \frac{S(S+1)}{2} + (S+1) = \frac{(S+2)(S+1)}{2} \leqslant \frac{k(k+1)}{2} \leqslant p(n).$$

Therefore, the result is true if $d=0$. Suppose now that $d=1$. In this case $m=u+v+1$ and $n=2S+v+1$. Then one has:

$$|G'| \leqslant \binom{S+1}{2} - \Bigg(\sum_{2\leqslant i<j\leqslant m} s_i s_j\Bigg) + b + \binom{m}{2}$$
$$\leqslant \binom{S+1}{2} - \binom{m-1}{2} + b + \binom{m}{2}$$
$$= \frac{S(S+1)}{2} + b + m - 1 = \frac{S(S+1)}{2} + b + u + v$$
$$\leqslant \frac{S(S+1)}{2} + S + v = \frac{S(S+3)}{2} + v.$$

If $v=0$ then $b=0$ and $k=S$, so $|G'| \leqslant \frac{S(S+3)}{2} = p(n)$.

If $v=1$ then $n=2S+2$ and $k=S+1$. Then

$$|G'| \leqslant \frac{S(S+3)}{2} + 1 = \frac{(S+1)(S+2)}{2} = p(n).$$

If $v=2$ then $n=2S+3$ and $k=S+1$. Then

$$|G'| \leqslant \frac{S(S+3)}{2} + 2 = \frac{S^2+3S+4}{2} < \frac{(S+1)(S+4)}{2} = p(n).$$

Finally, if $v \geqslant 3$ then $n=2S+v+1$ so $k \geqslant S+v/2$. Hence

$$p(n) \geqslant \frac{(S+v/2)(S+v/2+1)}{2} = \frac{S^2+(v+1)S+v(v+2)/4}{2}$$
$$\geqslant \frac{S(S+3)}{2} + S/2 + v/2 > \frac{S(S+3)}{2} + v \geqslant |G'|.$$

Therefore, in every case $|G'| \leqslant p(n)$, and Theorem 1.3 is proved. □

Recall that, in Example 2.1, we defined braids of any number of strands whose centralizer could not be generated by less than $p(n)$ elements. Therefore, the bound given by Theorem 1.3 is the best possible one.

7. Small generating sets

We saw in the previous section an upper bound for the number of generators of the centralizer of a braid β, in terms of its number of strings. But one could obtain a better bound if more information about β is given. In this section we will define a new generating set G for $Z(\beta)$, which is in most cases smaller than the set G' defined before. It is also the smallest possible "natural" generating set, in the sense that each generator belongs to one of the $t+1$ factors in the semidirect product decomposition in Theorem 1.1(c). Thus in a philosophical sense, G is the "right" generating set, even though it is not in general the smallest possible one, as we shall see at the end of this section.

If β is periodic or pseudo-Anosov, we already know a minimal generating set, with at most two elements. We also know a minimal generating set for any mixed braid group (see the proof of Proposition 6.1). Hence we can define G by induction on the number of strands, when β is a reducible, non-periodic braid. We can also suppose that β is in regular form. We recall that the interior braids are denoted $\beta_{[1]}, \dots, \beta_{[t]}$, and the tubular braid $\hat{\beta}$.

DEFINITION 7.1. – We will say that $i, j \in \{1, \dots, t\}$ are *permutable* if there exists some $\eta \in Z_0(\hat{\beta})$ such that $\eta(\mathcal{C}_i) = \mathcal{C}_j$.

Remark that permutability is an equivalence relation, and the definition of $Z_0(\hat{\beta})$ says that if i and j are permutable then $\beta_{[i]} = \beta_{[j]}$.

Let then $\{i_1, \dots, i_r\} \subset \{1, \dots, t\}$ be coset representatives for permutability. Let G_{i_k} be a minimal set of generators for $Z(\beta_{[i_k]})$, and G_0 be a minimal set of generators for $Z_0(\hat{\beta})$. Then we define $G = g_{i_1}(G_{i_1}) \cup \dots \cup g_{i_r}(G_{i_r}) \cup h(G_H)$. Notice that $G \subset G'$, and they coincide if and only if there is no pair of permutable indices.

PROPOSITION 7.2. – *G is a generating set of $Z(\beta)$.*

Proof. – From the exact sequence of Theorem 5.10 it follows that, if G_i is a set of generators for $Z(\beta_{[i]})$, then a set of generators for $Z(\beta)$ is $G' = g_1(G_1) \cup \dots \cup g_t(G_t) \cup h(G_0)$. Hence, we just need to show that if $j \in \{1, \dots, t\} \backslash \{i_1, \dots, i_r\}$, then every element in $g_j(G_j)$ can be written as a product of elements in G.

Take then j as above. There must be some i_k permutable with j, so $\beta_{[j]} = \beta_{[i_k]}$ and there is some $\eta \in Z_0(\hat{\beta})$ such that $\eta(\mathcal{C}_{i_k}) = \mathcal{C}_j$. Notice that G_j is a set of generators for $Z(\beta_{[j]}) = Z(\beta_{[i_k]})$, so every $\gamma \in G_j$ can be written as a product of elements in G_{i_k}. Hence the braid $\alpha = h(\eta)^{-1} g_{i_k}(\gamma) h(\eta)$ can be written as a product of elements in G. Moreover, one has $\hat{\alpha} = \widehat{h(\eta)}^{-1} 1 \widehat{h(\eta)} = 1$, and the only nontrivial interior braids in α are those corresponding to $\mathcal{C}_j$. Since the interior braids $h(\eta)_{i_k,l}$ for every l are just powers of $\beta_{[i_k]} = \beta_{[j]}$, and γ commutes with $\beta_{[j]}$, it follows that for every l, $\alpha_{j,l} = \gamma$. Therefore $\alpha = g_j(\gamma)$, so every element in $g_j(G_j)$ can be written as a product of elements in G, thus G is a generating set for $Z(\beta)$. □

The generating set we have just defined is, unfortunately, not always the smallest possible one:

Example 7.3. – Consider the five string braid $\beta = \sigma_3\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_2\sigma_3\sigma_4\sigma_1\sigma_2\sigma_3$ – the canonical reduction system of this braid has two round circles, one containing punctures number 1, 2 and 3, the other punctures number 4 and 5; the tubular braid is just a full twist of the two fat strings: $\hat{\beta} = \sigma_1^2$. Moreover, the interior braids of each tube are trivial. According to Theorem 1.1, the centralizer of this braid is

$$Z(\beta) \cong (B_3 \times B_2) \rtimes PB_2 \cong (B_3 \times \mathbb{Z}) \rtimes \mathbb{Z}$$

and the generating set constructed in this section has four elements: two for B_3, and one for each factor $\mathbb{Z}$. We now claim that this generating set is not as small as possible.

Indeed, $B_3 \times \mathbb{Z}$ can be generated by only two elements (and thus $Z(\beta)$ can be generated by three elements). To see this, recall that the 3-string braid group is isomorphic to the group of the $(2,3)$-torus knot. Thus B_3 has a presentation $\langle y, z \mid y^3 z^{-2} = 1 \rangle$ (with $y = \sigma_1\sigma_2$ and $z = \sigma_1\sigma_2\sigma_1$). Moreover, the factor $\mathbb{Z}$ is generated by σ_4. Now the two generators (y, σ_4) and (z, σ_4) generate $B_3 \times \mathbb{Z}$, because $(1, \sigma_4)$ can be written as $(y, \sigma_4)^3 (z, \sigma_4)^{-2}$.

8. Some algorithmic aspects

The aim of this section is to present the essential ingredients for an algorithm which, for any given braid, finds a generating set of its centralizer subgroup that matches the description of the previous sections. Since, for any braid β and any $k \in \mathbb{Z}$, the centralizer subgroups of β and $\beta\Delta^{2k}$ coincide, we can always assume that β is positive.

We start by mentioning that algorithms that perform the Nielsen–Thurston classification, and give the invariant folitations in the pseudo-Anosov case (in the form of train tracks), are available – notably, there are Bestvina–Haendel's [5] and of Los' [25] algorithms; and computer implementations are available on the web [9,20].

We recall briefly the idea of the two automatic structures on braid groups that are relevant for us: for the first one, given by Garside [18] and Thurston [34] (and refined by El-Rifai and Morton [13]), we think of D_n has having the n punctures lined up on the real line in the disk D. For the second one, given by Birman, Ko, and Lee [7], we think of B_n as having the n punctures regularly spaced on the circle of radius 1. Apart from that, the structures are exactly analogue. In the Garside–Thurston structure, there is a canonical way to write β as a product of divisors of Δ, namely by pushing each crossing between two strings into a factor as far to the left as possible. This normal form is called the *left greedy normal form*. For instance, in this normal form all factors which are *equal* to Δ (not just divisors of it) are grouped together at the very left of the product decomposition. Analogously, Birman–Ko–Lee write each braid as a product of divisors of δ in a left-greedy way. If β is a positive braid, then its *super summit set* is the subset of all elements α of its conjugacy class which satisfy the following conditions:

(i) α is positive,
(ii) the writing of α in left greedy normal form has as few factors as possible among all elements satisfying (i),
(iii) the writing of α in left greedy normal form has as many factors on the left as possible equal to Δ (or δ), among all elements satisfying (i) and (ii).

Two positive elements of B_n are conjugate if and only if their super summit sets coincide. Given $\beta \in B_n$ there is an algorithm, given in [16] (which is an improvement of the algorithm in [13]), to compute its super summit set. It is as follows: first we repeatedly *cycle* β (i.e. move the first factor different from Δ, respectively δ, to the end and calculate the left greedy form of the resulting braid), until this process runs into a loop. At this point we are guaranteed to have achieved condition (ii) above. Then we repeatedly *decycle* (i.e. move the last factor to the front and calculate the left greedy form of the resulting braid) until we run into a loop. Then all elements of this loop belong to the super summit set. Afterwards, all other elements of the super summit set can be found recursively by conjugating already known elements by (suitable) divisors of Δ (respectively δ), and retaining the result if it belongs to the super summit set.

This algorithm for computing the super summit set is necessary for our purposes. Now suppose we are given a braid $\beta \in B_n$ and we want to compute its centralizer. First we need to determine if β is periodic, reducible or pseudo-Anosov, and then we can use the results in this paper.

Remark 8.1. – Very recently, V. Gebhardt [19] presented a better algorithm for the conjugacy problem in braid groups. He defined the *ultra summit set*, which is in general much smaller than the super summit set described here.

8.1. Periodic elements

Deciding whether a given element β of B_n is periodic is very easy: one calculates the $(n-1)$st and the nth power of β. Then β is periodic if and only if one of the two results is a power of Δ^2.

If $\beta^{n-1} = \Delta^{2k}$ for some $k \in \mathbb{N}$, then β is conjugate to $\gamma_{(n)}^k$ (as can be easily seen from Lemma 3.1), and a conjugating element can be found explicitly using either of the two standard algorithms. Similarly, if $\beta^n = \Delta^{2k}$, then β is conjugate to $\delta_{(n)}^k$, and either algorithm yields an explicit conjugating element. In either case, one can find explicitly a generating set of the centralizer subgroup with only two elements, using Propositions 3.3 or 3.5.

8.2. Finding reducing curves of reducible elements

After establishing that an element β of B_n is not periodic, we need to check whether it is reducible, and if it is, we want to find explicitly an invariant multicurve. This is, in fact, a standard part of Bestvina–Haendel's [5] and of Los' [25] algorithms.

We want to point out one particularly elegant alternative, which is due to Benardete, Gutierrez and Nitecki [3] (see also [2]). We think of D_n as having the n punctures lined up horizontally, and we look at Garside–Thurston's left greedy normal form. The key observation from [3] is the following: suppose that C is an invariant multicurve of a braid β, and that the normal form of β is $\beta = \beta_1 \cdots \beta_k$, where $\beta_1, \ldots, \beta_k \in B_n$ are divisors of Δ. Moreover, suppose that all components of C are *round* (i.e. actual geometric circles in D_n). Then we have not only that $\beta_1 \cdots \beta_n(C) = C$, but also that all components of all the multicurves $\beta_1 \cdots \beta_i(C)$ are round for $i = 1, \ldots, k$.

As remarked in [3] this implies as a corollary that invariant multicurves are visible as round curves in the super summit set of β, and in particular the reducibility of a braid is easily detectable from the super summit set. To prove the corollary we note that β has a conjugate in which all components of the curve system C are round; moreover, β and its conjugate have the same super summit set. Now cycling and decycling this conjugate does not change the fact that there is a *round* invariant curve system, by the key observation above. At the end of the cycling/decycling procedure we have found elements of the super summit set which contain the desired round invariant curves.

Now it is shown in [3] how to determine if a given braid preserves a system of disjoint round curves. And there is a finite number of these systems. Moreover, since for each element of the super summit set we know how it can be conjugated to obtain β, we can find explicitly all curves that belong to a reduction system for β. We can then easily determine, by its definition, which of these curves belong to the canonical reduction system of β. That is, we can compute the canonical reduction system of β.

By the results in this paper, $Z(\beta)$ is then a semi-direct product of two groups that can be computed by induction on the number of strings. Hence, it only remains to study the case when β is pseudo-Anosov.

8.3. Pseudo-Anosov elements: commutation with $\delta_{(n)}^k$

Suppose that our braid β fails the tests of periodicity and reducibility, hence it is known to be pseudo-Anosov. We need to check if it commutes with the periodic braid other than powers of Δ^2.

We shall think of D_n as having its n punctures uniformly distributed over the circle of radius 1, and we consider Birman–Ko–Lee's left-greedy normal form. We want to decide algorithmically whether β is conjugate to a braid α with the property that α commutes with $\delta_{(n)}^k$ for some positive integer $k < n$. If it is, we want to know the conjugating braid explicitly. The following result yields such an algorithm.

PROPOSITION 8.2. – *Suppose that a pseudo-Anosov braid β has a conjugate which commutes with $\delta_{(n)}^k$ for some integer k. Then there exists an element α of the super summit set of β which has the property that α, and in fact every factor of the left greedy normal form of α, commutes with $\delta_{(n)}^k$.*

Proof. – Let β' be a conjugate of β which commutes with $\delta_{(n)}^k$. If $\beta' = \beta'_1 \cdot \ldots \cdot \beta'_r$ is the left-greedy normal form of β', then each factor β'_i is a divisor of $\delta_{(n)}$ which is $\frac{2\pi k}{n}$-symmetric. This follows from the fact that the very definition of the left-greedy normal form is completely rotation symmetric. More precisely, the fact that two consecutive factors $\beta'_i\beta'_{i+1}$ determine a left-greedy normal form is not modified by rotating them. Hence, the product $(\delta_{(n)}^{-k}\beta'_1\delta_{(n)}^k)\cdots(\delta_{(n)}^{-k}\beta'_r\delta_{(n)}^k)$ is in left-greedy normal form. Since this product equals $\delta_{(n)}^{-k}\beta'\delta_{(n)}^k = \beta'$, whose left-greedy normal form is $\beta'_1\cdots\beta'_k$, we obtain that $\delta_{(n)}^{-1}\beta'_i\delta_{(n)} = \beta'_i$, for $i = 1, \ldots, r$.

Using the same argument inductively, we see that the cycling and decycling procedure only ever creates braids in left greedy normal form in which all factors are $\frac{2\pi k}{n}$-symmetric. □

Now we notice that it is very easy to decide if a given divisor of δ (in the Birman–Ko–Lee context) is invariant under a given rotation. Hence one can determine if a braid commutes with an (explicitly computable) conjugate of $\delta_{(n)}^k$ by looking at the elements of its super summit set.

8.4. Pseudo-Anosov elements: commutation with $\gamma_{(n)}^k$

Now we want to determine if a given pseudo-Anosov braid commutes with a conjugate of $\gamma_{(n)}^k$, for a given positive integer $k < n-1$. This is only possible if there is some index $i \in \{1, \ldots, n\}$ such that β preserves P_i, as can be easily seen by looking at the corresponding permutations.

Call $\mathcal{P}_i = \{\{P_i\}, \{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n\}\}$, a partition of $\{P_1, \ldots, P_n\}$. Then β should belong to $B_{\mathcal{P}_i}$. There is a natural map $f_i : B_{\mathcal{P}_i} \to B_{n-1}$ which consists of forgetting the ith string. Notice that, if a braid α commutes with $\gamma_{(n)}^k$ (where P_1 is considered to be the central point of $D_{(n)}$) then $f_1(\alpha)$ commutes with $f_1(\gamma_{(n)}^k) = \delta_{(n-1)}^k$.

Hence we have a necessary condition that must be satisfied. If β preserves a puncture P_i, then we conjugate it to some α that preserves P_1, and we test whether a conjugate of $f_1(\alpha)$ commutes with $\delta_{(n-1)}^k$ for some $k < n-1$. If this does not happen, for $i = 1, \ldots, n$, then no conjugate of β commutes with $\gamma_{(n)}^k$.

This necessary condition is of course not sufficient. A sufficient and testable condition is now given by the following result. Recall that, by Corollary 3.7, there is an isomorphism $\chi = (\bar{\theta}^*)^{-1}\theta^*$ from $Z(\delta_{(n-1)}^k)$ to $Z(\gamma_{(n)}^k)$, given by adding a trivial string at the centre of D_{n-1}. Notice that, if $\zeta \in Z(\gamma_{(n)}^k)$, then $\chi(f_1(\zeta)) = \zeta$. Then one has:

PROPOSITION 8.3. – *Suppose that $\alpha \in B_n$ preserves P_1, and $\tilde{\alpha} = f_1(\alpha)$ commutes with $\delta_{(n-1)}^k$. Then the following two statements are equivalent.*

(i) *α is conjugate to an element ζ of B_n which commutes with $\gamma_{(n)}^k$, and the conjugating homeomorphism preserves P_1.*

(ii) *α is conjugate to $\chi(\tilde{\alpha})$.*

Proof. – The implication (ii) $\Rightarrow$ (i) is immediate, by choosing $\zeta := \chi(\tilde{\alpha})$.

For the implication (i)$\Rightarrow$(ii), we suppose that (i) holds, that is, there is an element $\eta \in B_{\mathcal{P}_1}$ such that $\eta^{-1}\alpha\eta = \zeta$, where $\zeta \in Z(\gamma_{(n)}^k)$. We can apply f_1 to all these elements, denoting $\tilde{\eta} = f_1(\eta)$ and $\tilde{\zeta} = f_1(\zeta)$. This yields $(\tilde{\eta})^{-1}\tilde{\alpha}\tilde{\eta} = \tilde{\zeta}$, where $\tilde{\alpha}, \tilde{\zeta} \in Z(\delta_{(n-1)}^k)$.

If we show that $\tilde{\eta} \in Z(\delta_{(n-1)}^k)$, then we can apply χ to all factors, obtaining

$$\chi(\tilde{\eta})^{-1}\chi(\tilde{\alpha})\chi(\tilde{\eta}) = \chi(\tilde{\zeta}) = \zeta,$$

hence $\chi(\tilde{\alpha})$ is conjugate to ζ which is conjugate to α, and the result follows.

Let us then show that $\tilde{\eta}$ commutes with $\delta_{(n-1)}^k$. Notice that ζ is a pseudo-Anosov braid that commutes with $\gamma_{(n)}^k$. Hence it preserves a projective foliation $\mathcal{F}_\zeta$, which is invariant under a rotation by an angle of $\frac{2\pi k}{n-1}$. But in this case $\tilde{\zeta}$ also preserves $\mathcal{F}_\zeta$, with the same stretch factor, hence it is also pseudo-Anosov. Since $\tilde{\alpha}$ is conjugated to $\tilde{\zeta}$, then it is pseudo-Anosov as well, and we call $\mathcal{F}_{\tilde{\alpha}}$ its corresponding projective foliation (which is also invariant under the same rotation, since $\tilde{\alpha}$ commutes with $\delta_{(n-1)}^k$). Since $(\tilde{\eta})^{-1}\tilde{\alpha}\tilde{\eta} = \tilde{\zeta}$, we have that $\tilde{\eta}$ sends $\mathcal{F}_{\tilde{\alpha}}$ to $\mathcal{F}_\zeta$.

Now consider the braid $d = \tilde{\eta}^{-1}\delta_{(n-1)}^k\tilde{\eta}$. It is conjugate to $\delta_{(n-1)}^k$, and hence periodic. Moreover, it preserves $\mathcal{F}_\zeta$, so it commutes with $\tilde{\zeta}$. But the periodic elements in the centralizer of $\tilde{\zeta}$ form a cyclic group containing $\delta_{(n-1)}^k$, and $\delta_{(n-1)}^k$ is the only element having exponent sum $(n-2)k$. Since d has exactly the same exponent sum, it follows that $d = \delta_{(n-1)}^k$. Hence $\tilde{\eta}$ commutes with $\delta_{(n-1)}$, and the result follows. □

An algorithm for testing whether a braid β is conjugate to a braid which commutes with $\gamma_{(n)}^k$ is now easy to construct: for each of the n punctures test whether the puncture is fixed by β, and whether forgetting this puncture yields a braid which is conjugate to a braid $\tilde{\alpha}$ that commutes with $\delta_{(n)}^k$. (We know how to do this, by the results of the previous subsection). For each puncture that does satisfy this property, test whether $\chi(\tilde{\alpha})$ (which is obtained from $\tilde{\alpha}$ by adding a "trivial" string in the centre), is conjugate to β. If, for one of the punctures, this is the case, then the answer is "yes", otherwise "no".

8.5. Pseudo-Anosov elements: finding roots

It remains to describe a last step for computing a generating set for $Z(\beta)$, when β is pseudo-Anosov. We assume that we have already computed the subgroup $\langle\rho\rangle$ of periodic braids commuting with β. Then we can multiply β by a suitable power of ρ, to obtain a braid b that preserves the singular leaves of the projective foliations corresponding to β. Then we know that $Z(\beta) = \langle\alpha\rangle \times \langle\rho\rangle$, where α is the smallest possible root of b.

The last problem, therefore, is to determine whether a given pseudo-Anosov braid b has a kth root, for given k, and to compute that root. This problem has been solved in [32] (generalised to all Garside groups in [31]). Moreover, since the number of possible values of k is finite (we are assuming that b is positive), we have an algorithm for computing α, thus a generating set for $Z(\beta)$.

Acknowledgements

We are grateful to a number of people for discussions and valuable ideas that greatly contributed to this research. The examples of Nikolai V. Ivanov [22,23], which we learned about through discussions with Mustafa Korkmaz, were an important inspiration and greatly helped us clarify our ideas. It was thus from Ivanov (via Korkmaz) that we learned that the number of

generators may have to grow quadratically with the number of strings, contradicting a conjecture in [17]. We are very grateful to Sang Jin Lee who later, but independently of Ivanov, came up with his examples, conjectured that they represent the worst case, and kindly communicated these ideas to us by email. (Hessam Hamidi-Teherani found the same examples as Lee immediately after listening to Ivanov's talk, but we didn't learn this until very recently.) We also thank David Bessis for useful discussions, and Joan Birman for telling us about Refs. [2] and [3].

REFERENCES

[1] ARNOLD V.I., The cohomology ring of the group of dyed braids, *Mat. Zametki* **5** (1969) 227–231.
[2] BENARDETE D., GUTIERREZ M., NITECKI Z., A combinatorial approach to reducibility of mapping classes, *Contemporary Math.* **150** (1993) 1–31.
[3] BENARDETE D., GUTIERREZ M., NITECKI Z., Braids and the Nielsen–Thurston classification, *J. Knot Theory Ramifications* **4** (1995) 549–618.
[4] BESSIS D., DIGNE F., MICHEL J., Springer theory in braid groups and the Birman–Ko–Lee monoid, *Pacific J. Math.* **205** (2) (2002) 287–309.
[5] BESTVINA M., HAENDEL M., Train-tracks for surface homeomorphisms, *Topology* **34** (1995) 109–140.
[6] BIRMAN J., Braids, Links, and Mapping Class Groups, Annals of Math. Studies, vol. **82**, Princeton University Press, 1975.
[7] BIRMAN J., KO K.H., LEE S.J., A new approach to the word and conjugacy problems in the braid groups, *Adv. Math.* **139** (1998) 322–353.
[8] BIRMAN J., LUBOTZKY A., MCCARTHY J., Abelian and solvable subgroups of the mapping class groups, *Duke Math. J.* **50** (1983) 1107–1120.
[9] BRINKMANN P., An implementation of the Bestvina-Handel algorithm for surface homeomorphisms, *Experiment. Math.* **9** (2000) 235–240, Computer program available at http://www.math.uiuc.edu/~brinkman/software/train/.
[10] BURDE G., Über Normalisatoren der Zopfgruppe, *Abh. Math. Sem. Univ. Hamburg* **27** (1964) 97–115.
[11] CONSTANTIN A., KOLEV B., The theorem of Kerékjártó on periodic homeomorphisms of the disc and the sphere, *Enseign. Math. (2)* **40** (3–4) (1994) 193–204.
[12] EILENBERG S., Sur les transformations périodiques de la surface de sphère, *Fund. Math.* **22** (1934) 28–41.
[13] EL-RIFAI E.A., MORTON H.R., Algorithms for positive braids, *Quart. J. Math. Oxford Ser. (2)* **45** (180) (1994) 479–497.
[14] FATHI A., LAUDENBACH F., POENARU V., Travaux de Thurston sur les surfaces – séminaire Orsay, Astérisque, vols. **66–67**, Société Math. de France, 1991.
[15] FENN R., ROLFSEN D., ZHU J., Centralisers in the braid group and singular braid monoid, *Enseign. Math.* **42** (1996) 75–96.
[16] FRANCO N., GONZÁLEZ-MENESES J., Conjugacy problem for braid groups and Garside groups, *J. Algebra* **266** (2003) 112–132.
[17] FRANCO N., GONZÁLEZ-MENESES J., Computation of centralizers in braid groups and Garside groups, *Rev. Mat. Iberoamericana* **19** (2003) 367–384.
[18] GARSIDE F.A., The braid group and other groups, *Quart. J. Math. Oxford* **20** (1969) 235–254.
[19] GEBHARDT V., A new approach to the conjugacy problem in Garside groups, Preprint, math.GT/0306199, 2003.
[20] HALL T., Computer implementation of Bestvina-Handel algorithm, available at http://www.liv.ac.uk/maths/PURE/MIN_SET/CONTENT/members/T_Hall.html.
[21] IVANOV N.V., Subgroups of Teichmüller Modular Groups, Translations of Mathematical Monographs, vol. **115**, AMS, 1992.
[22] IVANOV N.V., Talk at the special session "Mapping class groups and the geometric theory of Teichmüller spaces" at the 974th meeting of the AMS, Ann Harbour, MI, March 1–3, 2002.
[23] IVANOV N.V., Examples of centralizers in the Artin braid groups, Preprint, math.GT/0306418, 2003.

[24] DE KERÉKJÁRTÓ B., Über die periodischen Transformationen der Kreisscheibe und der Kugelfläche, *Math. Annalen* **80** (1919) 3–7.
[25] LOS J., Pseudo-Anosov maps and invariant train tracks in the disc: a finite algorithm, *Proc. London Math. Soc. (3)* **66** (1993) 400–430.
[26] MAKANIN G.S., On normalizers in the braid group, *Mat. Sb.* **86** (128) (1971) 171–179.
[27] MANFREDINI S., Some subgroups of Artin's braid group. Special issue on braid groups and related topics (Jerusalem, 1995), *Topology Appl.* **78** (1–2) (1997) 123–142.
[28] OREVKOV S.YU., Quasipositivity test via unitary representations of braid groups and its applications to real algebraic curves, *J. Knot Theory Ramifications* **10** (7) (2001) 1005–1023.
[29] PARIS L., ROLFSEN D., Geometric subgroups of surface braid groups, *Ann. Inst. Fourier* **49** (1999) 101–156.
[30] PENNER R.C., HARER J.L., Combinatorics of Train Tracks, Annals of Math., vol. **125**, Princeton University Press, Princeton, NJ, 1992.
[31] SIBERT H., Extraction of roots in Garside groups, *Comm. Algebra* **30** (6) (2002) 2915–2927.
[32] STYŠNEV V.B., *Izv. Akad. Nauk SSSR Ser. Mat.* **42** (5) (1978) 1120–1131, 1183.
[33] THURSTON W.P., On the geometry and dynamics of diffeomorphisms of surfaces, *Bull. Amer. Math. Soc. (N.S.)* **19** (1988) 417–431.
[34] THURSTON W.P., Braid Groups, in: D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson, W.P. Thurston (Eds.), *Word Processing in Groups*, Jones and Bartlett Publishers, Boston, MA, 1992, Chapter 9.

(Manuscrit reçu le 12 septembre 2003 ;
accepté le 28 avril 2004.)

Juan GONZÁLEZ-MENESES
Departamento de Algebra,
Universidad de Sevilla,
Apdo. 1160,
41080 Sevilla, Spain
E-mail: meneses@us.es

Bert WIEST
IRMAR (UMR 6625 du CNRS),
Université de Rennes 1,
Campus de Beaulieu,
35042 Rennes cedex, France
E-mail: bertold.wiest@math.univ-rennes1.fr